Release Change Reference, StarOS Release 21.28

First Published: 2022-09-29

Last Modified: 2024-10-25

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

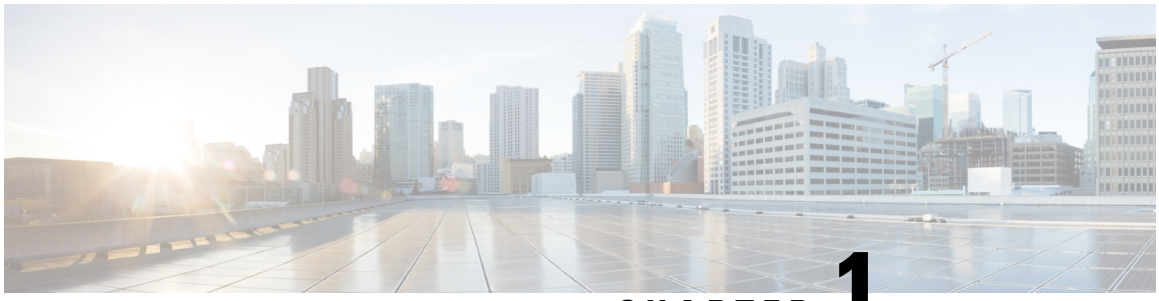
Conventions Used

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

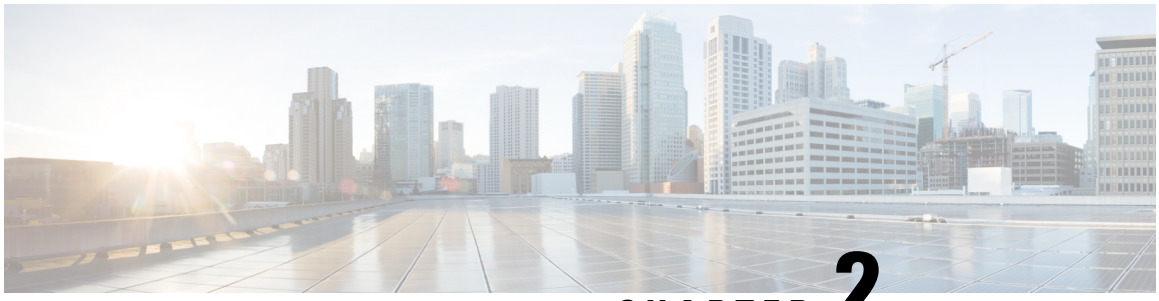
Release 21.28 Features and Changes Quick Reference

Release 21.28 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
5GIWK Active Sessions Count Support in ePDG, on page 37	ePDG	2024.02.0
Adding Abort Except Subscription Withdrawn Statistics as CLR Types, on page 17	MME	21.28.m10
Address Hold Timer Support, on page 19	P-GW	21.28.m14
Bulkstats to Print Summarized PGW Roaming Data Rate, on page 23	P-GW	2024.02.0
Bulk Busyout IP Pools based on VRFs, on page 31	P-GW	2024.03.0
Clear Hold IPs by Moving to Release State , on page 43	P-GW	2024.03.0
Enable Cinder Volume Multi-attach to Multiple VNFs	• P-GW • SAEGW	2024.02.0
Collision Handling of Modify Bearer Request over Modify Bearer Request Drop and Retry, on page 65	• P-GW • SAEGW • S-GW	21.28.m4

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Configuring ACL SRP Checkpoint, on page 69	• ASR5500 • VPC-DI	2024.02.0
Detecting Reuse of TCP Ports , on page 73	P-GW	21.28.m15
Differential Charging with 5G NSA, on page 75	MME	21.28.m0
Dynamic S-GW Selection for Interworking-5GC , on page 97	MME	• 2024.02.0 • 21.28.m7
Encrypt AES-GCM Algorithm , on page 109	IPSec	21.28
Enhanced SGW CDR nodeID Encoding for Larger Instance Numbers Support	SGW	2024.04.0
EPS to 5Gs Mobility Procedure without n1 Mode Support, on page 113	MME	2024.02.0
Fetching the Target eNB based on the Target en-gNB ID without TAC, on page 121	MME	21.28.m5
Handling Simultaneous Gy RARs from Different DRAs with Different RGs, on page 125	P-GW	21.28
Handling Duplicate eNodeB Path, on page 129	MME	21.28.m0
Handling CC-Request-Number AVP during Assume Positive State, on page 123	P-GW	21.28.m7
IMSI Privacy on ePDG, on page 135	ePDG	2024.03.0
Increasing CPU threshold from 30 to 70, on page 145	StarOs	21.28.m0
Handling 5G to 4G TAU when n1-mode is not Supported, on page 147	MME	21.28.m5
IP Source Violation, on page 149	P-GW	21.28
IPv4 and IPV6 Notification Support for IP Address Alignment	ePDG	2024.02.0
IKEV2 VRF Support, on page 131	StarOS	21.28.5
NAT Port Chunk Hold Timer Support, on page 159	P-GW	21.28.m10
Processing APCO IE on Unsupported Container ID, on page 175	ePDG	21.28.m0

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Prioritizing IMEI over MAC Address, on page 173	P-GW	21.28.m22
Public Warning System Failure and Restart Indication Support on SBc Interface, on page 169	MME	21.28
Recording the APN in the EDR Record, on page 179	• SGSN • MME	21.28.m10
Reject Sessions from Blocked APGROUPNAME, on page 181	SaMOG	• 21.28.m5 • 21.28.m1
QCI67 Support, on page 177	MME	21.28
Send 5G User Location Information to SMF+PGW-c, on page 187	ePDG	21.28.m10
Separate Counters for All EAP Type for Success and Failure Events, on page 199	SaMOG	21.28
Subscriber Session Continuation at SaMOG During Wi-Fi Frequency Band Change, on page 231	SaMOG	21.28
Support for DH group 5 Encryption under IKESA and IPSEC Transform Set, on page 229	ePDG IPSec	21.28.m6
TMSI Based NRI Container IE, on page 259	MME	21.28
TEID Collision with ULI Change, on page 263	P-GW	21.28.m4
Security Enhancement, on page 271	StarOS	21.28.1
SMS over NAS Messages on SGd Interface , on page 273	MME LI	21.28.m18
UE-Usage-Type Based P-GW or SMF+PGW-C Selection, on page 277	ePDG	• 21.28.5 • 21.28.6
UE Radio Capability IE Size , on page 305	MME	2024.03.0
Updating TAC ID to S-GW on Delete Session Request in Attach over Attach Case	MME	21.28.Fm0
VLAN-aware VMs, on page 309	P-GW	21.28.m0



CHAPTER 2

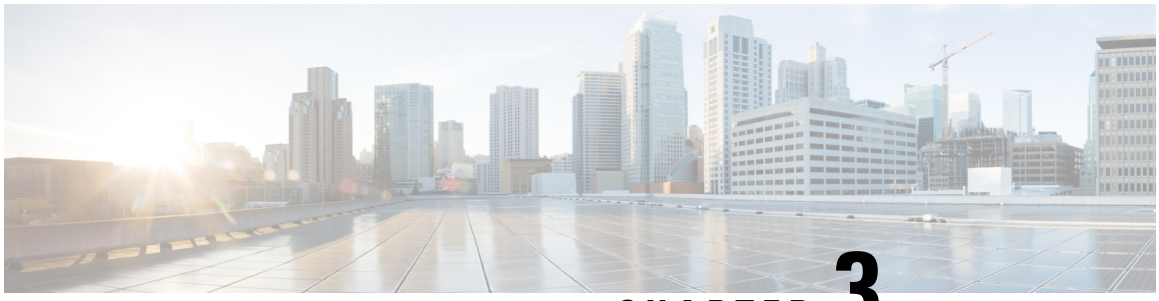
Feature Defaults Quick Reference

Feature Defaults

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

Feature	Default
Address Hold Timer Support	Disabled - Configuration Required
Bulkstats to Print Summarized PGW Roaming Data Rate	Enabled-Always-On
Bulk Busyout IP Pools based on VRFs	Disabled - Configuration Required to Enable
Clear Address Hold Timer for IP Pools	• Disabled - Configuration Required for Thresholds • Not applicable for exec mode Clear CLIs
Collision Handling of Modify Bearer Request over Modify Bearer Request Drop and Retry	Disabled - Configuration Required
Configuring ACL SRP Checkpoint	Disabled - Configuration Required
Differential Charging with 5G NSA	Disabled - Configuration Required
Dynamic S-GW Selection for Interworking-5GC	Disabled - Configuration Required
Encrypt AES-GCM-256 Algorithm	Disabled - Configuration Required
EPS to 5Gs Mobility Procedure without n1 Mode Support	Enabled-Always-On
Fetching the Target eNB based on the Target en-gNB ID without TAC	Enabled - Always-on
Handling CC-Request-Number AVP during Assume Positive State	Disabled - Configuration Required

Feature	Default
Handling Simultaneous Gy RARs from Different DRAs with Different RGs	Disabled - Configuration Required
Handling Duplicate eNodeB Path	Disabled - Configuration Required
Handling of 5G to 4G TAU when n1-mode is not Supported	Disabled - Configuration Required
IMSI Privacy on ePDG	Disabled – Configuration Required
IP Source Violation	Disabled - Configuration Required
NAT Port Chunk Hold Timer	Disabled - Configuration Required
Prioritizing IMEI over MAC Address	Disabled - Configuration Required
Processing APCO IE on Unsupported Container ID	Disabled - Configuration Required
Public Warning System Failure and Restart Indication Support on SBc Interface	Enabled - Configuration Required
QCI67 Support	Enabled - Always-on
Send 5G User Location Information to SMF+PGW-c	Disabled – Configuration Required
Separate Counters for All EAP Type for Success and Failur Events	Enabled - Always-on
Support for DH group 5 Encryption under IKESA and IPSEC Transform Set	Disabled – Configuration Required
Subscriber Session Continuation at SaMOG During Wi-Fi Frequency Band Change	Enabled - Always-on
TMSI Based NRI Container IE	Disabled - Configuration Required
TEID Collision with ULI Change	Disabled - Configuration Required
UE-Usage-Type based P-GW Selection in ePDG	Disabled - License not Required
UE Radio Capability IE Size	Disabled – Configuration Required to Enable
VLAN-aware VMs	Disabled - Configuration Required



CHAPTER 3

Bulk Statistics Changes Quick Reference

New Bulk Statistics

MME Schema

The following bulk statistics are added in the MME schema.

Bulk Statistics Variable	Description
esm-msgtx-brrmod-rej-eps-qos-not-accepted	The total number of times Bearer Modification Reject has occurred with an ESM Cause of 'EPS QoS Not Accepted'.
dcnr-nsa-ipra-count	Shows the total number of IPRA counts.
dcnr-nsa-opra-count	Shows the total number of OPRA count.
emm-msgtx-attach-rej-network-fail-hss-abort-except-subscription-withdrawn	Shows the total number of Attach Reject messages that are sent for an Attach Request, with a cause code Network Failure, when the rejection is due to HSS abort except subscription withdrawn.
emm-msgtx-attach-rej-network-fail-hss-cancel-except-sw	Shows the total number of Attach Reject messages sent for an Attach Request, with a cause code Network Failure, when the rejection is due to HSS CLR, excluding cancellation type of subscription withdrawal.

NAT Realm Schema

The NAT Realm schema provides operational statistics that can be used for monitoring and troubleshooting the NAT Port chunk hold timer feature.

Bulk Statistics Variable	Description
nat-rlm-port-chunks-on-hold	The total number of port chunks on hold, which are collected per context and for each realm

SaMOG Schema

The following bulk statistics are added in the SaMOG schema as part of the Separate Counters for All EAP Type for Success and Failure Events feature

Bulk Statistics Variables	Description
mrme-eap-rxmobile-eap-tls	Total number of EAP TLS received.
mrme-eap-rxmobile-eap-ttls	Total number of EAP TTLS received.
mrme-eap-rxmobile-eap-peap	Total number of EAP PEAP received.
mrme-eap-rxmobile-eap-aka-total-rcvd	Total number of EAP-AKA received.
mrme-eap-rxmobile-eap-aka-success	Total number of EAP-AKA connections succeeded.
mrme-eap-rxmobile-eap-aka-challenge	Total number of EAP-AKA challenges received.
mrme-eap-rxmobile-eap-aka-failure-rcvd	Total number of EAP AKA requests failed.
mrme-eap-rxmobile-eap-aka-msgs-from-svr-discarded	Total number of EAP-AKA messages from server that are discarded.
mrme-eap-rxmobile-eap-aka-prime-total-rcvd	Total number of EAP-AKA' received.
mrme-eap-rxmobile-eap-aka-prime-success	Total number of EAP-AKA' connections succeeded.
mrme-eap-rxmobile-eap-aka-prime-challenge	Total number of EAP-AKA' challenges received.
mrme-eap-rxmobile-eap-aka-prime-failure-rcvd	Total number of EAP AKA' requests failed.
mrme-eap-rxmobile-eap-aka-prime-msgs-from-svr-discarded	Total number of EAP-AKA' messages from server that are discarded.
mrme-eap-rxmobile-eap-sim-total-rcvd	Total number of EAP-SIM received.
mrme-eap-rxmobile-eap-sim-success	Total number of EAP-SIM connections succeeded.
mrme-eap-rxmobile-eap-sim-challenge	Total number of EAP-SIM challenges received.
mrme-eap-rxmobile-eap-sim-failure-rcvd	Total number of EAP SIM requests failed.
mrme-eap-rxmobile-eap-sim-msgs-from-svr-discarded	Total number of EAP-SIM messages from server that are discarded.
mrme-eap-rxmobile-eap-tls-total-rcvd	Total number of EAP-TLS received.
mrme-eap-rxmobile-eap-tls-success	Total number of EAP-TLS connections succeeded.

Bulk Statistics Variables	Description
mrme-eap-rxmobile-eap-tls-challenge	Total number of EAP-TLS challenges received.
mrme-eap-rxmobile-eap-tls-failure-rcvd	Total number of EAP TLS requests failed.
mrme-eap-rxmobile-eap-tls-msgs-from-svr-discarded	Total number of EAP-TLS messages from server that are discarded.
mrme-eap-rxmobile-eap-ttls-total-rcvd	Total number of EAP-TTLS received.
mrme-eap-rxmobile-eap-ttls-success	Total number of EAP-TTLS connections succeeded.
mrme-eap-rxmobile-eap-ttls-challenge	Total number of EAP-TTLS challenges received.
mrme-eap-rxmobile-eap-ttls-failure-rcvd	Total number of EAP TTLS requests failed.
mrme-eap-rxmobile-eap-ttls-msgs-from-svr-discarded	Total number of EAP-TLS messages from server that are discarded.
mrme-eap-rxmobile-eap-peap-total-rcvd	Total number of EAP-PEAP received.
mrme-eap-rxmobile-eap-peap-success	Total number of EAP-PEAP connections succeeded.
mrme-eap-rxmobile-eap-peap-challenge	Total number of EAP-PEAP challenges received.
mrme-eap-rxmobile-eap-peap-failure-rcvd	Total number of EAP PEAP requests failed.
mrme-eap-rxmobile-eap-peap-msgs-from-svr-discarded	Total number of EAP-PEAP messages from server that are discarded.

PGW Schema

The following bulk statistics are added to the PGW schema:

Bulk Statistics Variables	Description
Bulk Statistic Variables in the pgw-only data-rate	
pgw-subs-total	Displays the total number of the subscriber count.
pgw-data-active	Displays the total number of active subscribers.
pgw-data-dormant	Displays the total number of dormant subscribers.
pgw-data-fromuseravg-bps	Displays the average data rate from user in bits per second.
pgw-data-touseravg-bps	Displays the average data rate to user in bits per second.

Bulk Statistics Variables	Description
pgw-data-fromuserpeak-bps	Displays the Peak data rate from user in bits per second.
pgw-data-fromusersust-bps	Displays the mean data rate from user in bits per second.
pgw-data-tousersust-bps	Displays the Sust data rate to user in bits per second
pgw-data-fromuserpeak-pps	Displays the peak data rate from user in packets per second.
pgw-data-touserpeak-pps	Displays the peak data rate to user in packets per second. **Type:** Gauge
pgw-data-fromuseravg-pps	Displays the average data rate from user in packets per second.
pgw-data-touseravg-pps	Displays the average data rate to user in packets per second.
pgw-data-fromusersust-pps	Displays the Sust data rate from user in packets per second
pgw-data-tousersust-pps	Displays the Sust data rate to user in packets per second. **Type:** Gauge
Bulk Statistic Variables in the pgw-only data-rate with plmn-type home	
pgw-subs-total-home	Displays the total number of the home subscriber count.
pgw-data-active-home	Displays the total number of active home subscribers.
pgw-data-dormant-home	Displays the total number of dormant home subscribers.
pgw-data-fromuseravg-bps-home	Displays the average data rate from user in bits per second.
pgw-data-touseravg-bps -home	Displays the average data rate to user in bits per second.
pgw-data-fromuserpeak-bps-home	Displays the peak data rate from user in bits per second.
pgw-data-fromusersust-bps-home	Displays the mean data rate from user in bits per second.

Bulk Statistics Variables	Description
pgw-data-tousersust-bps-home	Displays the sust data rate to user in bits per second
pgw-data-fromuserpeak-pps-home	Displays the peak data rate from user in packets per second.
pgw-data-touserpeak-pps-home	Displays the peak data rate to user in packets per second.
pgw-data-fromuseravg-pps-home	Displays the average data rate from user in packets per second.
pgw-data-touseravg-pps -home	Displays the average data rate to user in packets per second.
pgw-data-fromusersust-pps-home	Displays the sust data rate from user in packets per second. **Type:** Gauge
pgw-data-tousersust-pps-home	Displays the sust data rate to user in packets per second.
Bulk Statistic Variables in the pgw-only data-rate with plmn-type roaming	
pgw-subs-total-roaming	Displays the total number of the roaming subscriber count.
pgw-data-active-roaming	Displays the total number of active roaming subscribers.
pgw-data-dormant-roaming	Displays the total number of dormant roaming subscribers.
pgw-data-fromuseravg-bps-roaming	Displays the average data rate from user in bits per second. **Type:** Gauge
pgw-data-touseravg-bps-roaming	The average data rate to user in bits per second.
pgw-data-fromuserpeak-bps-roaming	The peak data rate from user in bits per second.
pgw-data-fromusersust-bps-roaming	The mean data rate from user in bits per second.
pgw-data-tousersust-bps-roaming	The sust data rate to user in bits per second
pgw-data-fromuserpeak-pps-roaming	The peak data rate from user in packets per second.

Bulk Statistics Variables	Description
pgw-data-touserpeak-pps-roaming	The peak data rate to user in packets per second.
pgw-data-fromuseravg-pps-roaming	The average data rate from user in packets per second.
pgw-data-touseravg-pps -roaming	The average data rate to user in packets per second.
pgw-data-fromusersust-pps-roaming	The sust data rate from user in packets per second.
pgw-data-tousersust-pps-roaming	The sust data rate to user in packets per second.
Bulk Statistic Variables in the pgw-only data-rate with plmn-type visiting	
pgw-subs-total-visiting	Displays the total number of the visiting subscriber count.
pgw-subs-total-visiting	Displays the total number of the visiting subscriber count.
pgw-data-dormant-visiting	Displays the total number of dormant visiting subscribers.
pgw-data-fromuseravg-bps-visiting	Displays the average data rate from user in bits per second.
pgw-data-touseravg-bps -visiting	The average data rate to user in bits per second.
pgw-data-fromuserpeak-bps-visiting	Displays the peak data rate from user in bits per second.
pgw-data-fromusersust-bps-visiting	Displays the mean data rate from user in bits per second.
pgw-data-tousersust-bps-visiting	Displays the sust data rate to user in bits per second
pgw-data-fromuserpeak-pps-visiting	Displays the peak data rate from user in packets per second.
pgw-data-touserpeak-pps-visiting	Displays the peak data rate to user in packets per second.
pgw-data-fromuseravg-pps-visiting	Displays the average data rate from user in packets per second.
pgw-data-touseravg-pps -visiting	Displays the average data rate to user in packets per second.

Bulk Statistics Variables	Description
pgw-data-fromusersust-pps-visiting	Displays the sust data rate from user in packets per second.
pgw-data-tousersust-pps-visiting	Displays the sust data rate to user in packets per second.

System Schema

The following bulk statistics are added to the system schema:

Bulk Statistics Variable	Description
ikev2-notifpaysent-pdntype-ipv4	Total number of sessions with IPv4 PDN type.
ikev2-notifpaysent-pdntype-ipv6	Total number of sessions with IPv6 PDN type.

Modified Bulk Statistics

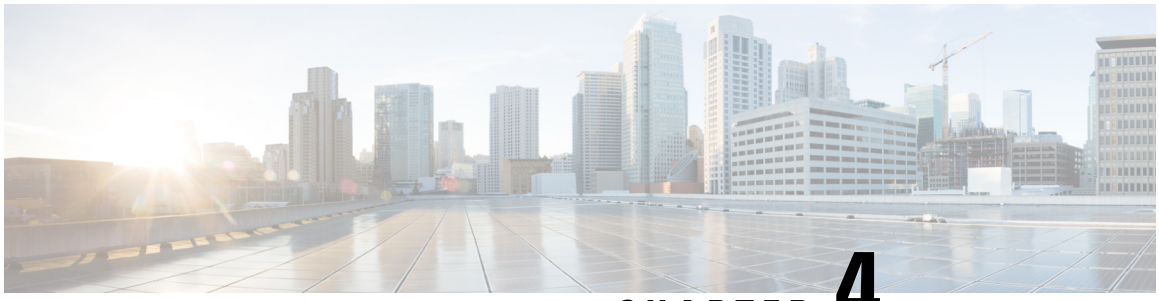
MME Schema

The following bulk statistics are modified in the MME schema.

Bulk Statistics Variable	Description
emm-msgtx-attach-rej-network-fail-smgr-resource-unavailable	Shows the total number of Attach Reject messages sent for an Attach Request with a cause code Network Failure, when the rejection is due to Session Manager resources is unavailable.
emm-msgtx-attach-rej-nw-fail-hssabort-ex-sub-withdrawn	Shows total number of Attach procedure not completing due to HSS CLR, excluding cancellation type of subscription withdrawal. This includes scenario of attach reject with network failure and also attach abort, where CLR abort happens after attach accept is sent and before attach complete is received.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.28

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.28 software release.

SNMP MIB Alarm Changes for 21.28

This section provides information on SNMP MIB alarm changes in release 21.28.

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

New SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.28.

- starPreThreshIPPoolUsable
- starPreThreshClearIPPoolUsable
- starFinalThreshIPPoolUsable
- starFinalThreshClearIPPoolUsable
- starS8HRLMISFSigConfNotFound
- starSxMonitorDown
- starSxMonitorUp
- starSessMgrAAAMgrGrStateUpdateFailure
- starRMDemuxUnavailable
- starRMDemuxUnavailable
- starUserPasswordExpiryInd

SNMP MIB Conformance Changes for 21.28

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

SNMP MIB Object Changes for 21.28

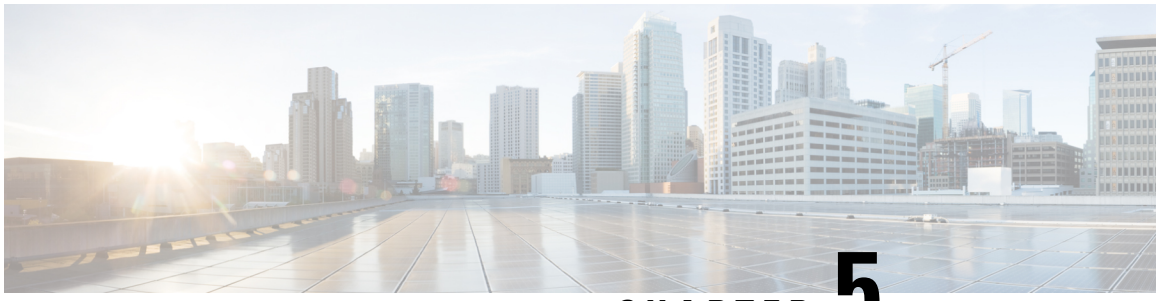
This section provides information on SNMP MIB alarm changes in release 21.28.

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

New SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.28.

- starPasswordExpiryNotification
- starAHTAge



CHAPTER 5

Adding Abort Except Subscription Withdrawn Statistics as CLR Types

Feature Summary and Revision History

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

Revision History

Revision Details	Release
MME supports a statistics under Attach Reject category for HSS abort except subscription withdrawn.	21.28.m10

Feature Changes

In MME, CLR types other than subscription withdrawn under the Attach Reject category is counted as SMGR RESOURCE UNAVAILABLE.

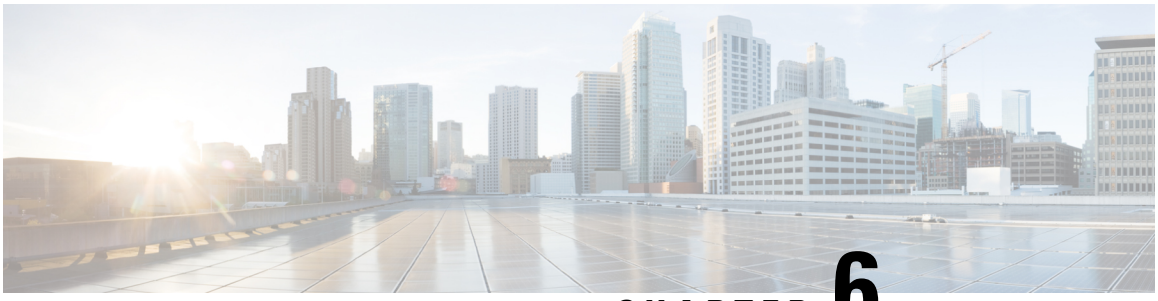
Previous Behavior: In MME, attach reject due to HSS abort except subscription withdrawn counter was not supported.

New Behavior: The HSS abort except subscription withdrawn counter is added to separate CLR attach reject from the SMGR RESOURCE UNAVAILABLE. This counter displays the contribution of a CLR except subscription that is withdrawn to the statistics SMGR RESOURCE UNAVAILABLE attach reject reason.

Command Changes

You can use the following counters to view total number of Attach Reject messages that are sent for an Attach Request, with a cause code Network Failure, when the rejection is due to HSS abort except subscription withdrawn.

- In the **show mme-service statistics** command the **HSS abort except subs withdrawn** statistics is added.
- In the MME Schema, the **emm-msgtx-attach-rej-network-fail-hss-abort-except-subscription-withdrawn** counter is added.



CHAPTER 6

Address Hold Timer Support

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
P-GW supports configuring of Address Hold Timer for IPv6.	21.28.m14

Feature Description

In P-GW, if the IPv4 **address-hold-timer** parameter is enabled and an active subscriber is disconnected, the IP address becomes held or considered still in use. The IP address does not return to the **Release** state until the **address-hold-timer** expires.

This enables subscribers who reconnect within the specified length of time (in seconds) to obtain the same IP address from the IP pool.

With this release, the Address Hold Timer feature supports IPv6 pools through a CLI configuration.

Using show CLI configuration commands, you can view the following:

- The address in USED, HOLD, FREE, and RELEASE state and list of addresses.
- The busyout states with the address hold timer state.
- The cumulative number of IP addresses in each state.

Upgrade and Downgrade Process

If the Address Hold Timer CLI is configured, post upgrade this feature works for the IPv6 pool.

If you have enabled the Address Hold Timer for IPv6, post downgrade, where AHT for IPv6 was not supported, the complete IPv6 pool configuration gets ignored. Ensure that the Address Hold Timer for IPv6 gets removed from the configuration before the downgrade procedure.

Configuring Address Hold Timer

Use the following sample configuration to enable the IPv6 address hold timer.

```
configure
   context context_name
      [ no ] ipv6 pool pool_name prefix ip_address/len public priority
address-hold-timer address_hold_timer_value
   end
```

NOTES:

- **ipv6 pool** *pool_name* **prefix** *ip_address/len* **public** *priority* **address-hold-timer** *address_hold_timer_value*: Enables address hold timer support for an IPv6 pool.

  If the **address-hold-timer** is enabled and an active subscriber is disconnected, the IP address is held or considered in use and is not returned to the Free state until the **address-hold-timer** expires. This enables subscribers who reconnect within the length of time specified (in seconds) to obtain the same IP address from the IP pool.

  For example, **Ipv6 pool PUBLIC1V6 prefix 5001::aaaa/48 public 0 address-hold-timer 120**

Note

- You can configure the **address-hold-timer** value under different keywords and under the IPv6 pool. However, the address hold timer gets configured with the latest **address-hold-timer** value configured.
- The **address-hold-timer** value is configured in seconds and the value of 0 represents that the address hold timer is disabled.
- In P-GW, the On the fly change of Address Hold Timer(AHT) is not supported. If the AHT is configured, then ongoing calls do not move to the Hold state. If the AHT is configured and then the call is connected then, the IP moves to the Hold state.

  The On-the-fly Address Hold Timer(AHT) behavior is similar for IPv4 and IPv6 pools.

- **no** : Removes the configured address hold timer for a specific pool. For example, `no ipv6 pool PUBLIC1V6 address-hold-timer`

Monitoring and Troubleshooting

This section provides information regarding the CLI command available in support of the Address Hold Timer feature.

Show Command(s) and/or Outputs

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

show ipv6 pool *pool_name*

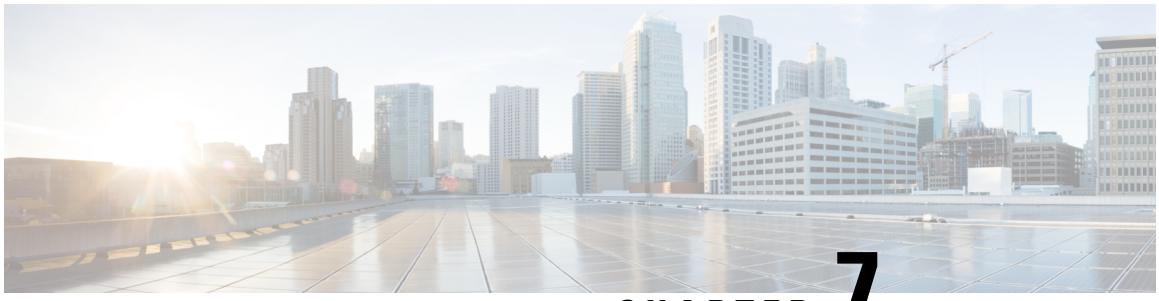
The output of the **show ipv6 pool pool_name PUBLIC1V6 { free | used | release | hold | limit | wide }** command is modified to display the Address hold timer CLI statistics. For example:

```
 show ipv6 pool pool-name PUBLIC1V6
    Pool Name:     PUBLIC1V6
    Group Name:
    Pool Type:     Public        Priority: 0
    Pool Id:       2001          Vrf: n/a
    Pool Status:   Good
    Start Prefix:  5001::/64
    End Prefix:    5001:0:0:ffff::/64
        Addr-Hold-Timer: 100
        Total Prefix:  65536        Used Prefix: 0      Free Prefix: 65533       On-Hold
Prefix: 1       Released Prefix: 2
        Pool Address Type: Normal
    Configured Prefix: 5001::aaaa/48
    User-Plane  ID   : N/A
    Virtual-FE  ID   : N/A
                 Nexthop Forwarding Address: Disabled
      Network Reachability Detection Server: Disabled
                  Suppress-Switchover-ADVS: Disabled
                   Allow-Static-Allocation: Disabled
                  Duplicate-Addr-Detection: Disabled
```

```
                     Send-Pilot-Packet: Enabled
                     Advertise-if-used: Disabled
  Addr-Hold-Timer-IPV6: 202                        Group Available Threshold: Disabled
Clear: Disabled
                   Pool-Free Threshold: Disabled    Clear: Disabled
                   Pool-Used Threshold: Disabled    Clear: Disabled
          cip-local-pool-used Threshold: Disabled    Clear: Disabled
   cip-local-pool-in-use-addr Threshold: Disabled    Clear: Disabled
```

Where:

- **used** - An address in the **used** state is one that is currently in use by a connected subscriber.
- **hold** – An address in the hold state is one that has recently been released from the pool, but for which the **address-hold timer** has not yet expired.
- **free** – An address in the free state is one that in not currently in use by a subscriber and has no NAI and IMSI data that are stored from a previous user of this address.
- **release** – An address in the released state is one that has been released from the pool, and the address-hold timer has expired for this address. This address has NAI and IMSI data that are stored for the previous subscriber.
- **limit** – An address in the limit state displays default 100 IP addresses information, if no limit value is specified.
- **wide** – An address in the wide state is one that displays information potentially formatted to greater than 80 columns.



CHAPTER 7

Bulkstats to Print Summarized PGW Roaming Data Rate

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First Introduced	2024.02.0

Feature Description

The bulkstats support is enhanced to print summarized subscriber data-rate for users based on the PLMN type (home, roaming, visiting).

In the existing **show subscribers pgw-only data-rate** command, the following plmn-type filters are added to enable the service providers to retrieve the subscriber data-rate based on the PLMN type:

- show subscribers pgw-only data-rate plmn-type home
- show subscribers pgw-only data-rate plmn-type roaming
- show subscribers pgw-only data-rate plmn-type visiting

This helps to find out the total number of roaming subscribers in a network and assist with a convenient billing process for the roaming subscribers.

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.

Show Commands and/or Outputs

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

show sub pgw-only data-rate

Use this command to view the combined PGW subscribers' data rate.

Field	Description
Peak rate from user(bps)	The peak data rate in bits per second is obtained for data that are sent from the subscriber to the network during the last sampling period. The sampling period is 30 seconds.
Peak rate to user(bps)	The peak data rate in bits per second is obtained for data that are received from the network by the subscriber during the last sampling period. The sampling period is 30 seconds.
ave rate from user(bps)	The average data rate in bits per second that is obtained for data that are sent from the subscriber to the network during the last sampling period. The sampling period is 30 seconds.
ave rate to user(bps)	The average data rate in bits per second is obtained for data that are received from the network by the subscriber during the last sampling period. The sampling period is 30 seconds.
sust rate from user(bps)	The mean data rate in bits per second is obtained for data that is sent from the subscriber to the network during the last three sampling periods. The sampling period is 30 seconds.
sust rate to user(bps)	The mean data rate in bits per second is obtained for data that are received from the network by the subscriber during the last three sampling periods. The sampling period is 30 seconds.

Peak rate from user(pps)	The speed that packets are received from the user in packets per second. The sampling period is 30 seconds.
peak rate to user(pps)	The speed at which the packets are sent to the user in packets per second. The sampling period is 30 seconds.
ave rate from user(pps)	The average speed at which the packets are received from the user in packets per second. The sampling period is 30 seconds.
ave rate to user(pps)	The average speed that packets are being sent to the user in packets per second. The sampling period is 30 seconds.
sust rate from user(pps)	The sustained speed at which the packets are received from the user in packets per second. The sampling period is 30 seconds.
sust rate to user(pps)	The sustained speed at which the packets are sent to the user in packets per second. The sampling period is 30 seconds.

Using the following show commands you can view similar P-GW roaming data rate details for the PLMN types such as home, roaming, and visiting:

- **show subscribers pgw-only data-rate plmn-type** *home*: Displays P-GW home subscribers' data rate.
- **show subscribers pgw-only data-rate plmn-type** *roaming*: Displays P-GW roaming subscribers' data rate.
- **show subscribers pgw-only data-rate plmn-type** *visiting*: Displays P-GW visiting subscribers' data rate.

Bulk Statistics

This feature supports the following bulk statistics.

PGW Schema

The following bulk statistics are added to the PGW schema:

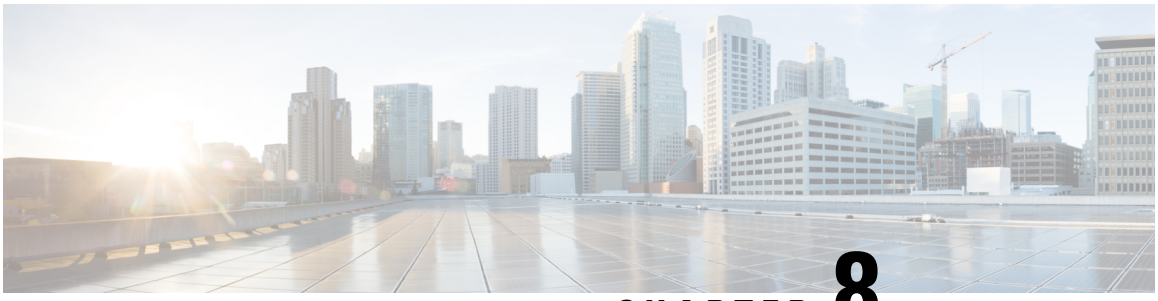
Variables	Description
Bulk Statistic Variables in the pgw-only data-rate	
pgw-subs-total	Displays the total number of the subscriber count.
pgw-data-active	Displays the total number of active subscribers.
pgw-data-dormant	Displays the total number of dormant subscribers.
pgw-data-fromuseravg-bps	Displays the average data rate from user in bits per second.
pgw-data-touseravg-bps	Displays the average data rate to user in bits per second.

Variables	Description
pgw-data-fromuserpeak-bps	Displays the Peak data rate from user in bits per second.
pgw-data-touserpeak-bps	Displays the Peak data rate to user in bits per second.
pgw-data-fromusersust-bps	Displays the mean data rate from user in bits per second.
pgw-data-tousersust-bps	Displays the Sust data rate to user in bits per second
pgw-data-fromuserpeak-pps	Displays the peak data rate from user in packets per second.
pgw-data-touserpeak-pps	Displays the peak data rate to user in packets per second. **Type:** Gauge
pgw-data-fromuseravg-pps	Displays the average data rate from user in packets per second.
pgw-data-touseravg-pps	Displays the average data rate to user in packets per second.
pgw-data-fromusersust-pps	Displays the Sust data rate from user in packets per second.
pgw-data-tousersust-pps	Displays the Sust data rate to user in packets per second. **Type:** Gauge
Bulk Statistic Variables in the pgw-only data-rate with plmn-type home	
pgw-subs-total-home	Displays the total number of the home subscriber count.
pgw-data-active-home	Displays the total number of active home subscribers.
pgw-data-dormant-home	Displays the total number of dormant home subscribers.
pgw-data-fromuseravg-bps-home	Displays the average data rate from user in bits per second.
pgw-data-touseravg-bps -home	Displays the average data rate to user in bits per second.
pgw-data-fromuserpeak-bps-home	Displays the peak data rate from user in bits per second.

Variables	Description
pgw-data-touserpeak-bps-home	Displays the peak data rate to user in bits per second.
pgw-data-fromusersust-bps-home	Displays the mean data rate from user in bits per second.
pgw-data-tousersust-bps-home	Displays the sust data rate to user in bits per second
pgw-data-fromuserpeak-pps-home	Displays the peak data rate from user in packets per second.
pgw-data-touserpeak-pps-home	Displays the peak data rate to user in packets per second.
pgw-data-fromuseravg-pps-home	Displays the average data rate from user in packets per second.
pgw-data-touseravg-pps -home	Displays the average data rate to user in packets per second.
pgw-data-fromusersust-pps-home	Displays the sust data rate from user in packets per second. **Type:** Gauge
pgw-data-tousersust-pps-home	Displays the sust data rate to user in packets per second.
Bulk Statistic Variables in the pgw-only data-rate with plmn-type roaming	
pgw-subs-total-roaming	Displays the total number of the roaming subscriber count.
pgw-data-active-roaming	Displays the total number of active roaming subscribers.
pgw-data-dormant-roaming	Displays the total number of dormant roaming subscribers.
pgw-data-fromuseravg-bps-roaming	Displays the average data rate from user in bits per second. **Type:** Gauge
pgw-data-touseravg-bps-roaming	The average data rate to user in bits per second.
pgw-data-fromuserpeak-bps-roaming	The peak data rate from user in bits per second.
pgw-data-touserpeak-bps-roaming	The peak data rate to user in bits per second.

Variables	Description
pgw-data-fromusersust-bps-roaming	The mean data rate from user in bits per second.
pgw-data-tousersust-bps-roaming	The sust data rate to user in bits per second
pgw-data-fromuserpeak-pps-roaming	The peak data rate from user in packets per second.
pgw-data-touserpeak-pps-roaming	The peak data rate to user in packets per second.
pgw-data-fromuseravg-pps-roaming	The average data rate from user in packets per second.
pgw-data-touseravg-pps -roaming	The average data rate to user in packets per second.
pgw-data-fromusersust-pps-roaming	The sust data rate from user in packets per second.
pgw-data-tousersust-pps-roaming	The sust data rate to user in packets per second.
Bulk Statistic Variables in the pgw-only data-rate with plmn-type visiting	
pgw-subs-total-visiting	Displays the total number of the visiting subscriber count.
pgw-subs-total-visiting	Displays the total number of the visiting subscriber count.
pgw-data-dormant-visiting	Displays the total number of dormant visiting subscribers.
pgw-data-fromuseravg-bps-visiting	Displays the average data rate from user in bits per second.
pgw-data-touseravg-bps -visiting	The average data rate to user in bits per second.
pgw-data-fromuserpeak-bps-visiting	Displays the peak data rate from user in bits per second.
pgw-data-touserpeak-bps-visiting	Displays the peak data rate to user in bits per second.
pgw-data-fromusersust-bps-visiting	Displays the mean data rate from user in bits per second.
pgw-data-tousersust-bps-visiting	Displays the sustained data rate to user in bits per second.

Variables	Description
pgw-data-fromuserpeak-pps-visiting	Displays the peak data rate from user in packets per second.
pgw-data-touserpeak-pps-visiting	Displays the peak data rate to user in packets per second.
pgw-data-fromuseravg-pps-visiting	Displays the average data rate from user in packets per second.
pgw-data-touseravg-pps -visiting	Displays the average data rate to user in packets per second.
pgw-data-fromusersust-pps-visiting	Displays the sustained data rate from user in packets per second.
pgw-data-tousersust-pps-visiting	Displays the sust data rate to user in packets per second.



CHAPTER 8

Bulk Busyout IP Pools based on VRFs

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced	2024.03.0

Busyout IP Pools

Busyout makes addresses from an IP pool in the current context unavailable once they are free.

Bulk Busyout IP Pools

Bulk Busyout IP pools is used to busyout:

- All IP pools in a context
- Specific Address range
- Specific IPv4/IPv6 Pool – range of addresses in the pool or group of addresses in the particular IP pool, or range of IP addresses or group of IP addresses pools.

Bulk Busyout IP Pools by VRF Names

In P-GW, by configuring busyout ip pool using VRF name option you can busyout all the ip pools that are associated with the VRF.

For example, if there are 'n' number of ip pools that are associated with a vrf say vrf_1, then the configuration **busyout ip pool vrf** *vrf_1* sets all the 'n' numbers of ip pools in busyout state. This **busyout ip pool vrf** configuration allows to avoid each pool to be marked busyout independently.

Enable Busyout IPv4 Pool with VRF

You can enable Busyout configuration for multiple IPv4 pools by using the CLI procedure.

Procedure

Step 1 Configure busyout for IPv4 pools based on VRF. The *vrf_name* is case-sensitive and you must enter the value of size 1–63.

busyout ip pool vrf *vrf_name*

Example:

```
[local]qvpc-si# config
[local]qvpc-si(config)# context context_name
[egress]qvpc-si(config-ctx)# busyout ip pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

Step 2 Verify whether the Busyout IPv4 pool is configured when the busyout configuration is in place for IPv4 pools.

show ip pool summary vrf *vrf_name*

Example:

```
[ISP1]laas-setup# show ip pool summary vrf mpls-vrf-1
context ISP1:
+-----Type:    (P) - Public    (R) - Private    (N) - NAT
```

```
|              (S) - Static    (E) - Resource   (O) - One-to-One NAT
|              (M) - Many-to-One NAT
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Busyout: (B) - Busyout configured
|||||
|||||
vvvvv Pool Name                        Start Address   Mask/End Address Used    Avail
----- -------------------------------- --------------- ---------------  ----------------
RG00B PRIVATEPOOL3                     10.140.150.0    255.255.255.0    0        254
RG00B PRIVATEPOOL2                     10.140.140.0    255.255.255.0    0        254
RG00B PRIVATEPOOL1                     31.33.0.0       255.255.0.0      0        65534
RG00B privatepool-1                    10.160.0.0      255.248.0.0      0        524286

Total Pool Count: 5
Total Pool Kernel Routes: 9    Max Pool Kernel Routes: 6000
Total Pool Explicit Host Routes: 0    Max Pool Explicit Host Routes: 24000

ISP1]laas-setup# show ip pool summary vrf mpls-vrf-1 wide
context ISP1:
+-----Type:    (P) - Public    (R) - Private    (N) - NAT
|              (S) - Static    (E) - Resource   (O) - One-to-One NAT
|              (M) - Many-to-One NAT
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Busyout: (B) - Busyout configured
|||||
|||||
vvvvv Pool Name                        Start Address   Mask/End Address Used     Hold     Quarantine
  Avail    Rel      Free     Group Name
----- -------------------------------- --------------- ---------------  -------- -------- -----------
 -------- -------- -------- --------------------------------
RG00B PRIVATEPOOL3                     10.140.150.0    255.255.255.0    0        0        0
   254      0        254
RG00B PRIVATEPOOL2                     10.140.140.0    255.255.255.0    0        0        0
   254      0        254
RG00B PRIVATEPOOL1                     31.33.0.0       255.255.0.0      0        0        0
   65534    0        65534
RG00B privatepool-1                    10.160.0.0      255.248.0.0      0        0        0
   524286   0        524286   int41
```

Enable Busyout IPv6 Pool with VRF

You can enable Busyout configuration for IPv6 pools by using the CLI procedure.

Procedure

Step 1 Enable the busyout multiple IPv6 pools based on VRF. The *vrf_name* is case-sensitive and you must enter the value of size 1–63.

busyout ipv6 pool vrf *vrf_name*

Example:

```
[local]qvpc-si# config
[local]qvpc-si(config)# context context_name
[egress]qvpc-si(config-ctx)# busyout ipv6 pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

Step 2 Verify whether the busyout IPv6 pool is configured when busyout configuration is in place for IPv6 IP pools.

show ipv6 pool summary vrf *vrf_name*

Example:

```
[ISP1]laas-setup# show ipv6 pool summary vrf mpls-vrf-1
context ISP1:
+-----Type:    (P) - Public    (R) - Private
|              (S) - Static    (H) - Shared
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Addr-Type: (N) - Normal  (T) 6to4
|||||
|||||+-Busyout: (B) - Busyout configured
||||||
||||||
vvvvvv Pool Name            Start Prefix                           End Prefix
             Used     Avail
------ -------------------- ---------------------------------------
----------------------------------------  -------- --------
RG00NB PRIVATEV6            7001::/64                              7001:0:0:ffff::/64
             0        65536
RG00NB PRIVATEV61           8001::/64                              8001:0:0:ffff::/64
             0        65536
RG00NB PRIVATEV62           6001::/64                              6001:0:0:ffff::/64
             0        65536

Total Pool Count: 3
[ISP1]laas-setup# show ipv6 pool summary vrf mpls-vrf-1 wide
context ISP1:
+-----Type:    (P) - Public    (R) - Private
|              (S) - Static    (H) - Shared
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Addr-Type: (N) - Normal  (T) 6to4
|||||
|||||+-Busyout: (B) - Busyout configured
||||||
```

```
||||||
vvvvvv Pool Name             Start Prefix                            End Prefix
             Used     Avail
------ -------------------- ----------------------------------------
---------------------------------------  -------- --------
RG00NB PRIVATEV6             7001::/64                               7001:0:0:ffff::/64
             0        65536
RG00NB PRIVATEV61            8001::/64                               8001:0:0:ffff::/64
             0        65536
RG00NB PRIVATEV62            6001::/64                               6001:0:0:ffff::/64
             0        65536
Total Pool Count: 3
```

Disable Bulk Busyout by VRF for IPv4 Pools

You can disable bulk busyout by VRF configuration using the CLI procedure.

Note Before unbusying a VRF, if an IP pool is already marked as busyout and associated with a VRF, and then when you configure or unconfigure VRF, the IP pool busyout status remains the same.

Procedure

Enter **no** to disable busyout for IPv4 pools based on VRF. If a pool associated with this VRF is marked as busyout then the IP pool stays busied out.

no busyout ip pool vrf *vrf_name*

Example:

```
[local]qvpc-si# config
[local]qvpc-si(config)# context egress
[egress]qvpc-si(config-ctx)# no busyout ip pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

Note The *vrf_name* is case-sensitive and you must enter the values of size 1–63.

You have successfully disabled the busyout configuration for IPv4 pools.

Disable Bulk Busyout by VRF for IPv6 Pools

You can disable Busyout configuration for multiple IPv6 pools by using the CLI procedure.

Note Before unbusying a VRF, if an IP pool is already marked as busyout and associated with a VRF, and then when you configure or unconfigure VRF, the IP pool busyout status remains the same.

Procedure

Enter **no** to disable busyout for IPv6 pools based on VRF. If a pool associated with this VRF is marked as busyout then the IP pool stays busied out.

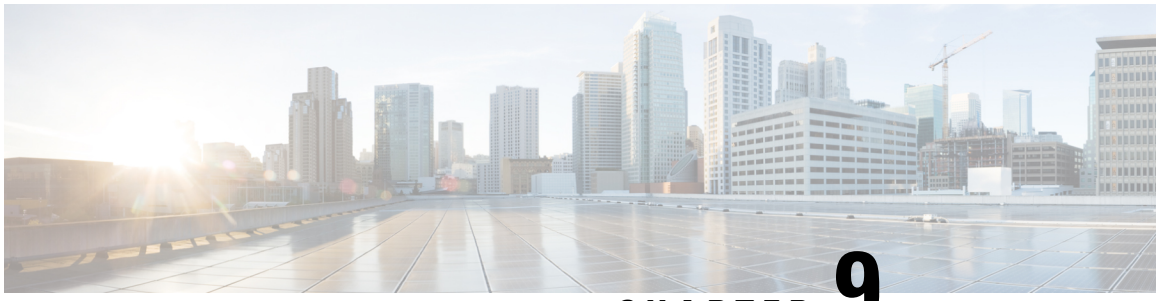
no busyout ipv6 pool vrf *vrf_name*

Example:

```
[local]qvpc-si# config
[local]qvpc-si(config)# context egress
[egress]qvpc-si(config-ctx)# no busyout ipv6 pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

Note The *vrf_name* is case-sensitive and you must enter the values of size 1–63.

You have successfully disabled the busyout configuration for IPv6 pools.



CHAPTER 9

5GIWK Active Sessions Count Support in ePDG

Feature Summary and Revison History

Summary Data

Applicable Product(s) or Functional Area	eDPG
Applicable Platform(s)	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 support 5G Active sessions count through Bulkstats counters and show command output.	2024.02.0

Feature Description

ePDG enables mobile operators to provide secure access to the EPC (EvolvedPacket Core) and to interwork with 5G SA Core from an untrusted non-3GPP IP access network.

Since Interworking with 5G SA Core functionality requires purchase of an extra ePDG 5G Sessions license, the ePDG 5G Active Sessions Count feature supports new counters for the total number of Active 5G Sessions and number of Active 5G Sessions of PDN types IPv4, IPv6, and Dual (IPv4v6).

These counters are provided as part of the command **show epdg-service statistics** and **epdg-interworking-5g** schema.

This enhancement to the Bulkstats counters and show command output allow the mobile operators to track and monitor the current usage against the installed 5G license.

The **Core-Network-Restrictions** AVP received from the AAA server in the Diameter EAP Answer (DEA) message is used to determine whether a subscriber session is 5G or 4G.

When this Core-Network-Restrictions AVP does not restrict access to the 5G Core the session gets treated as 5G with the following exceptions:

- 5G Session License is not installed or 5G interworking functionality is not enabled.
- 5G Interworking feature is enabled, the custom **pgw-selection select pgw 4gonly-ue** CLI is configured, and UE is not N1 Mode Capable.
- 5G Interworking feature is enabled, the custom **pgw-selection select pgw no-5gs-interworking** CLI is configured, and **Interworking-5gs-indicator** AVP is "NOT SUBSCRIBED" for the subscriber.
- 5G Interworking feature is enabled and the custom **pgw-selection select pgw smf-not-configure**d CLI is configured.

Note In the **show epdg-service statistics** CLI command there will not be any change in the existing cumulative (4G and 5G) Active Session counts. Upon successful Session Recovery, respective 5G Active Session counters get incremented based on the number of 5G sessions recovered successfully.

Relationships to Other Features

ePDG Interworking with SMF+P-GW-IWK Support: For Information Element and AVP Support, Custom CLIs, and 5G Interworking support details, refer the *ePDG Interworking with SMF+P-GW-IWK Support* chapter in the *ePDG Administration Guide.*

Configuring ePDG 5G Interworking Bulk Statistics

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

```
configure
     bulkstat mode
```

```
        [ no ] epdg-interworking-5g schema schema_name format <format_string> active-only
format <format_string>
        end
```

Note **epdg-interworking-5g schema schema_name format format_string active-only format <format_string>**

Allows ePDG to capture 5G interworking related bulk statistics.

no: Deletes bulkstats schema configuration for 5G interworking statistics.

Monitoring and Troubleshooting

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

Show Command(s) and/or Outputs

This section provides information about the show commands and outputs for the 5GIWK Active Sessions Count 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 **ePDG 5G Interworking statistics for all services** command displays output of Interworking 5G statistics for all ePDG-services. The interworking-5g option is available only with ePDG 5G license.

The following 5G session variables are newly added to the existing list of variables and counters of **show epdg-service statistics interworking-5g** command.

Note For more information about the existing list of counters/variables, refer to the Monitoring and Troubleshooting section of the *ePDG Interworking with SMF+P-GW-IWK Support* chapter.

Table 1: show epdg-service statistics interworking-5g Command Output Descriptions

Field	Description
5G Sessions – Counter for sessions with access to 5G core not restricted and exceptions as specified in the Limitation section.	
Active	Total number of 5G Active Sessions.
PDN-Type IPv4	Total number of 5G Active Sessions of PDN type IPv4.
PDN-Type IPv6	Total number of 5G Active Sessions of PDN type IPv6.

Field	Description
PDN-Type IPv4v6	Total number of 5G Active Sessions of PDN type Dual.

clear epdg-service statistics interworking-5g

The **clear epdg-service statistics interworking-5g** command does not clear newly introduced statistics as part of this feature.

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.

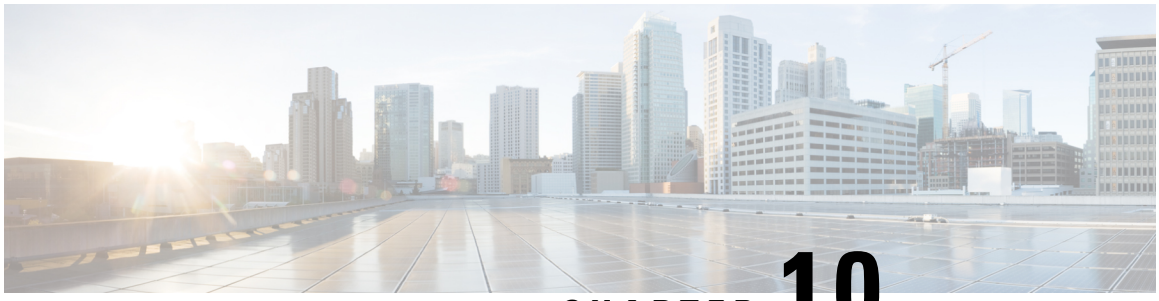
show bulkstats variables epdg-interworking-5g

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

The following 5G session bulkstats variables are newly added to the existing list of variables and counters of **show bulkstats variables epdg-interworking-5g** command.

Note For more information about the existing list of counters/variables, refer to the Monitoring and Troubleshooting section of the *ePDG Interworking with SMF+P-GW-IWK Support* chapter.

Bulk Statistics Variables	Description
5G Sessions:	
iwk5g-pdn-active	The total number 5G active sessions.
iwk5g-pdn-ipv4-active	The total number of 5G active sessions of PDN type IPv4.
iwk5g-pdn-ipv6-active	The total number of 5G active sessions of PDN type IPv6.
iwk5g-pdn-ipv4v6-active	The total number of 5G Active sessions of PDN type Dual.



CHAPTER 10

Changes in Bulkstat Schemas for EGTPC and GTPU1

Revision History

Revision Details	Release
P-GW and S-GW supports changes in Bulkstats schema for EGTPC and GTPU1.	2024.04.0

Behavior Changes

Previous Behavior: The gtpu schema does not increment Non-Std QCI (Non-GBR or GBR) gtpu statistics/bulkstats based on the qci-qos mapping configuration. Also, the following fields of EGTPC schema displayed the egtpc counters with maximum value limit of 32 bits:

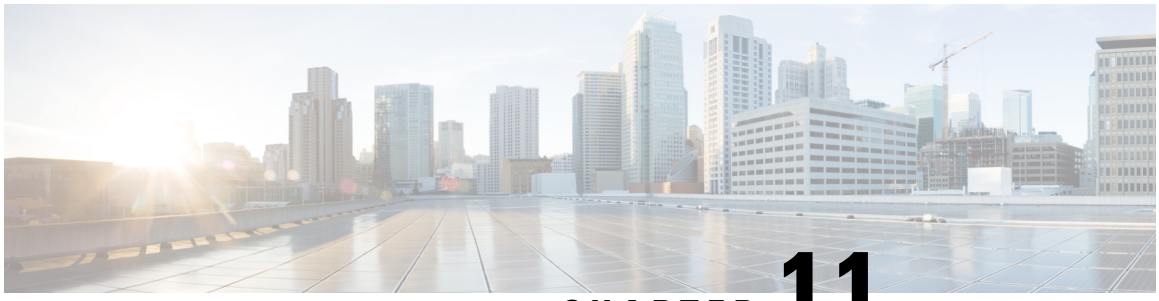
- tun-recv-crebearrespdeniedOtherCause
- tun-recv-delbearrespdeniedOtherCause
- tun-recv-updbearrespdeniedOtherCause

New Behavior: The gtpu schema increments Non-Std QCI (Non-GBR or GBR) gtpu statistics/bulkstats based on the qci-qos-mapping configuration for P-GW or S-GW service.

Also, the following fields of EGTPC schema displays egtpc counters with maximum value limit of 64 bits.

- tun-recv-crebearrespdeniedOtherCause
- tun-recv-delbearrespdeniedOtherCause
- tun-recv-updbearrespdeniedOtherCause

Customer Impact:Use the **show gtpu statistics gtpu-service** *gtpu_service_name* command to view the incremented statistics. You can also view the same statistics in the GTPU schema.



CHAPTER 11

Clear Hold IPs by Moving to Release State

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	• Disabled - Configuration Required for Thresholds • Not applicable for exec mode Clear CLIs
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Command Line Interface Reference* • *Thresholding Configuration*

Revision History

Revision Details	Release
P-GW supports clearing of IPs from Address Hold List for both IPv4 and IPv6 Pools.	2024.03.0

Feature Description

In P-GW, support for an exec level command to move IP address from HOLD to RELEASE state is introdcued.

When an IPv4/IPv6 pool is having huge number of addresses in HOLD state, you can use this clear CLI to move addresses from HOLD to RELEASE state.

You can perform the Address Hold Timer (AHT) clear operation to:

- manually change IPv4 or IPv6 state from hold to release for a specific IP or range of IPs belonging to an IPv4 or IPv6 pool name that is in the hold state.
- manually change IPv4 or IPv6 state from hold to release for the selected oldest IPs based on the age given for an IPv4 or IPv6 pool whose hold-age should be greater than or equal to specified age.

Guidelines, Limitations, and Restrictions for Clearing Address Hold Timer

Guidelines

Follow these guidelines for clearing Address Hold Timer:

- Check if the Address Hold Timer is enabled for the IP Pool. For more information, refer the Address Hold Timer Support chapter.
- For upgrade, you must enable the **ip-pool-usable** threshold CLI to provision again.

Note By default the IP Pool usable threshold both at context and pool level CLI configuration is disabled.

- For downgrade, remove the **ip-pool-usable** thresholds both at context and pool level CLI configurations, else IP Pool configuration will fail.

  To perform the removal, either reconfigure the required pool level CLI parameter or load the downgraded version configuration file that was already saved.
- Threshold configuration for the SNMP traps are applied on the fly.

Limitations

The Interchassis Session Recovery (ICSR) Checkpointing is not supported for **Clear HoldToRelease** CLI configuration. Following are the recommendations due to this limitation:

- Execute the **Clear HoldToRelease** CLI on both the chassis at the same time.

- All Clear range, age, and specific IP CLIs must be run on ICSR peer at the same time.

  Age-based clearing should be executed simultaneously on both Active and Standby chassis in an ICSR setup. Any time gap in running this command between the Active and Standby chassis may result in discrepancies in the Hold and Release IPs, potentially clearing more Hold IPs on the chassis where the command was executed later. Therefore, using the 'clear by range' command is preferred over the 'clear by age' command.

Note Clear command does not cause any changes to the Used IP addresses.

Restrictions

These restrictions apply to IP pool thresholds for clearing AHT:

- **ip-pool-usable** threshold must be less than its clear threshold value.
- **ip-pool-usable-final** threshold must be less than its clear threshold value.
- **ip-pool-usable-final** threshold should be less than ip-pool-usable threshold, and
- **ip-pool-usable-final** clear threshold must be less than ip-pool-usable clear threshold.

Change IPv4 Address State from Hold to Release for Single IP or Range of IPs

You can manually change the IPv4 IP state from HOLD to RELEASE for a single IP or range of IPs that belong to an IP pool,

Before you begin

Review the "Guidelines", "Limitations", and "Restrictions" sections of Clear Hold IPs by Moving to Release State , on page 43.

Procedure

Step 1 Enter a specific context in the exec mode.

context *context_name*

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>}  { <ipv4_address >| {
range <start_ip_address> <end_ip_address> count <1-5000>}}
```

Step 2 Enter the **clear ip hold-to-releasestate** parameters using the following command in the exec mode.

clear ip hold-to-releasestate{ pool-name *ipv4_pool_name } { ipv4_address* **| range** *start_ip_address end_ip_address* **count** *value* **} }**

- The **clear ip hold-to-releasestate** parameter moves the address from HOLD to RELEASE state.
- The IPv4 pool name indicates from where mentioned ip/range is removed from AHT hold list.You can configure a pool name of size 1 to 31 and the pool name is case sensitive.
- Specify the start IP address range from which the IP address is to removed from AHT list. Maximum of 5000 Hold IPs only gets cleared.
- The count parameter specifies MAXIMUM number of Ips to be moved from HOLD state to RELEASE state .Specify the count of ip addresses to be cleared in integer 1 -.5000

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>}  { <ipv4_address >|
{range <start_ip_address> <end_ip_address> count <1-5000>}}
 ---------------------------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA  ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA 11.0.2.3
---------------------------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20
 ---------------------------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20 coun?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20 count ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20 count 60
<cr>                - newline
```

Change IPv6 Address State from Hold to Release for Single IP or Range of IP Prefixes

You can manually change the IPv6 IP state from HOLD to RELEASE for a single IP prefix or range of IP prefixes that belong to an IPv6 pool,

Before you begin

Review the "Guidelines", "Limitations", and "Restrictions" sections of Clear Hold IPs by Moving to Release State , on page 43.

Procedure

Step 1 Enter a specific context in the exec mode

context*context_name*

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6  hold-to-releasestate { pool-name <ipv6-pool-name>}  {{ prefix
<ipv6_address>} | {range <startIPv6prefix> <endIPv6prefix> count <1-5000>}}
```

Step 2 Enter the clear ipv6 hold-to-release parameters using the following command in the exec mode

clear ipv6 hold-to-releasestate{ pool-name *ipv6_pool_name }* **{ { prefix** *ipv6_address }* **| { range** *startIPv6prefix endIPv6prefix* **count** *value* **} }**

- The **clear ipv6 hold-to-releasestate** parameter moves the address from HOLD to RELEASE state.
- The IPv6 pool name indicates from where mentioned *IPv6 range of prefixes* is cleared from the AHT hold list. You can configure a pool name of size 1 to 31 and the pool name is case sensitiveve.
- Specify the start and end IPv6 prefixes from which the IP address is to be cleared from AHT list. .
- The count parameter specifies maximum number of IPs to be moved from HOLD state to RELEASE state .Specify the count of IP addresses to be cleared in integer 1 -.5000.

View the example configuration output for single IP prefix clearing :

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6  hold-to-releasestate { pool-name <ipv6-pool-name>}  {{ prefix
<ipv6_address>} | {range <startIPv6prefix> <endIPv6prefix> count <1-5000>}}
 ----------------------------------------
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA prefix 2068::323
  <cr>                - newline
 ----------------------------------------------------------------------------------
```

View the example configuration output for range IP prefix clearing:

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6  hold-to-releasestate { pool-name <ipv6-pool-name>}  {{ prefix
<ipv6_address>} | {range <startIPv6prefix> <endIPv6prefix> count <1-5000>}}
 ----------------------------------------
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::  3001:0:0:5:: ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::  3001:0:0:5:: count
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::  3001:0:0:5:: count 60

 <cr>                - newline
 ----------------------------------------------------------------------------------
```

Age-based Clear IPv4 State for Address Hold Timer

You can manually change IPv4 state from hold to release for the selected IP's based on the age specifies for an IP pool,

Procedure

Step 1 Enter a specific context in the exec mode.

context *context_name*

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>} {age <hold-age-in-seconds
> count <1-5000>}
```

Step 2 Enter age parametes using the following command in the exec mode.

clear ip hold-to-releasestate { pool-name *ipv4_pool_name }* **{ age** *hold-age-in-seconds* **count** *value* **}**

Additional information:

- The **hold-to-releasestate** parameter moves the address from HOLD state to RELEASE state.
- The IPv4 pool name indicates the IPv4 Pool from where mentioned ip or range is cleared from AHT hold list. You can configure a pool name of size 1 to 31 and the pool name is case sensitive.
- The hold-age must be in seconds 60 - 31556926.
- The count parameter specifies MAXIMUM number of IPs to be moved. from HOLD state to RELEASE state .Specify the count of ip addresses to be cleared in integer 1 - 5000.

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>} {age  < hold-age-in-seconds
 > count <1-5000>}
  -----------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 120
-------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA?
-------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 300 ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 300 count ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 300 count 60
<cr>                - newline
```

Step 3 Verify the configured age for IPv4 addresses using the **show ip pool address** show commands

Example:

```
[egress]qvpc-si# show ip pool address pool-name ipv4-public
+-------- (B) Busyout
|
|+------- (F)-FREE (U)-USED (H)-HOLD (Q)-QUARANTINE (R)-RELEASE
||+------ Quarantine
||| Address         NAI/MSID Hash   Hold/Qrntn Timer/ Session Start/Disconnect  Hold Age
```

```
||                                  Session ID
vv ==============  ================ ================      ========================== =========

Pool: ipv4-public
 U 10.0.0.12       9cd3cb187bcbd63c         1          Wed Jul 03 06:14:54 2024   -
 F 10.0.0.13       0000000000000000         -                      -              -
 F 10.0.0.14       0000000000000000         -                      -              -
 H 10.0.0.10       4a97ad2930ffc700 230               Wed Jul 03 06:18:19 2024   70
 H 10.0.0.11       0c645044e6b388b9 249               Wed Jul 03 06:18:38 2024   51
```

Age-based Clear IPv6 State for Address Hold Timer

You can manually change IPv6 state from hold to release for the selected IP's based on the age specifies for an IP pool, Clear specific IP information, and specify age to select IPs having hold-age greater than or equal to the specified value in CLI and move their state from HOLD to RELEASE.

Procedure

Step 1 Enter a specific context in the exec mode.

context *context_name*

Example:

```
 [local]qvpc-si#context egress
 [egress]qvpc-si# clear ipv6 hold-to-releasestate { pool-name <ipv6-pool-name>} {age
<hold-age-in-seconds > count <1-5000>}
```

Step 2 Enter the age parameters using the following command in the exec mode.

clear ipv6 hold-to-releasestate { pool-name *ipv6_pool_name }* { **age** *hold-age-in-seconds* **count** *value***}**

Additional information:

- The **hold-to-releasestate** parameter moves the address from HOLD state to RELEASE state.
- The IPv6 pool name indicates from where mentioned IPv6 range of prefixes is cleared from AHT hold list. You can configure a pool name of size 1 to 31 and the pool name is case sensitive.
- The hold-age must be in seconds 60 - 31556926 .
- The count parameter specifies MAXIMUM number of IPs to be moved. from HOLD state to RELEASE state .Specify the count of ip addresses to be cleared in integer 1 - 5000.

Example:

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6 hold-to-releasestate { pool-name <ipv6-pool-name>} {age <hold-age-in-seconds
 > count <1-5000>}
----------------------------------------
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age?
```

```
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age 90 ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age 90 count ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age 64 count 60   <cr>
     - newline
```

Step 3 Verify the configured age for IPv6 addresses using the **show ipv6 pool pool-name** show command.

Example:

```
[egress]qvpc-si# show ipv6 pool pool-name ipv6-public
    Pool Name:     ipv6-public
    Group Name:
    Pool Type:     Public        Priority: 0
    Pool Id:       2001          Vrf: n/a
    Pool Status:   Good
    Start Prefix:  5001::/64
    End Prefix:    5001:0:0:4::/64
    Addr-Hold-Timer: 300
    Total Prefix:  5        Used Prefix: 1      Free Prefix: 1       On-Hold Prefix: 2       Released
 Prefix: 1
    Pool Address Type: Normal
    Configured Prefix: N/A
    User-Plane  ID   : N/A
    Virtual-FE  ID   : N/A
                 Nexthop Forwarding Address: Disabled
      Network Reachability Detection Server: Disabled
                  Suppress-Switchover-ADVS: Disabled
                   Allow-Static-Allocation: Disabled
                  Duplicate-Addr-Detection: Disabled
                         Send-Pilot-Packet: Enabled
                         Advertise-if-used: Disabled
                 Group Available Threshold: Disabled    Clear: Disabled
                       Pool-Free Threshold: Disabled    Clear: Disabled
                       Pool-Used Threshold: Disabled    Clear: Disabled
              cip-local-pool-used Threshold: Disabled    Clear: Disabled
       cip-local-pool-in-use-addr Threshold: Disabled    Clear: Disabled
                     Pool-Usable Threshold: Disabled    Clear: Disabled
               Pool-Usable-Final Threshold: Disabled    Clear: Disabled    age: Disabled

+-------- (B) Busyout
|
|+------- (F)-FREE (U)-USED (H)-HOLD (R)-RELEASE
||
|| Address                  NAI/MSID Hash    Hold Timer/           Session Start/Disconnect  Hold
Age
||                                           Session ID

vv ======================= ================ ================     ======================== =========

Pool Name: ipv6-public
 U 5001:0:0:1::/64          4a97ad2930ffc700 2                     Wed Jul 03 06:29:02 2024      -

 F 5001:0:0:4::/64          0000000000000000         -                        -                -

 R 5001::/64                c9600956165ae917         -             Wed Jul 03 05:13:02 2024      -

 H 5001:0:0:2::/64          0c645044e6b388b9 276                   Wed Jul 03 06:30:16 2024  24

 H 5001:0:0:3::/64          9cd3cb187bcbd63c 292                   Wed Jul 03 06:30:32 2024  8
```

Set Poll Intervals

Use this task to define poll intervals for **ip-pool-usable** and **ip-pool-usable-final** thresholds. This configuration is applicable for both pre and final threshold configurations.

Procedure

Configure poll intervals in the Global configuration mode.

threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-pool-release | ip-pool-used | **ip-pool-usable** } interval time

Example:

```
[local]qvpc-si# configure
[local]qvpc-si# threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-pool-release
 | ip-pool-used | ip-pool-usable } interval <time>
```

Configure Pre and Final Thresholds at Context Level

The Clear Hold IPs by Moving to Release State feature supports two thresholds at context level.

Use this task to enable the **ip-pool-usable** and **ip-pool-usable-final** thresholds for ip pool usable of IPs, which are in either FREE or RELEASE states.

These are the types of Pre and final threshold SNMP alarms generated based on the configured thresholds:

- PreThreshIPPoolUsable alarm for entering condition
- PreThreshClearIPPoolUsable alarm for clearing condition
- FinalThreshIPPoolUsable alarm for entering condition
- FinalThreshClearIPPoolUsable alarm for clearing condition

Before you begin

Check if you have configured **ip-pool-usable** for configuring **ip-pool-usable-final**.

To enable the IP Pool Threshold monitoring at pool-level and context-level, refer the IP Pool Thresholds chapter in the Thresholding Configuration Guide.

Procedure

Step 1 Configure the IP pool usable pre threshold state as either free or release.

Example:

```
[local]qvpc-si# configure
[local]qvpc-si# threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-pool-release
 | ip-pool-used | ip-pool-usable } interval <time>
[local]qvpc-si#context egress
[egress]qvpc-si# threshold ip-pool-usable <low_thresh> [ clear <high_thresh> ] [ip-pool-usable-final
 <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si# threshold ip-pool-usable 40 clear 50 ip-pool-usable-final 35 clear 36
```

The **PreThreshIPPoolUsable** trap is raised if the ip pool usable is less than or equal to the configured **ip-pool-usable** low threshold value.

The **PreThreshClearIPPoolUsable** trap gets triggered if the pool usable value is greater than a clear high threshold value.

Step 2 Configure the IP pool usable final threshold state in either free or release state.

threshold ip-pool-usable *low_thresh* [clear *high_thresh*] **[ip-pool-usable-final** *low_thresh* **[clear** *high_thresh* **]]]**

The **FinalThreshIPPoolUsable** alarm is raised when the measured pool usable value is less than or equal to the ip-pool-usable-final value. The **FinalThreshClearIPPoolUsable** trap clears when the **ip-pool-usable-final** clear value is greater than a clear threshold.

Example:

```
[local]qvpc-si# configure
[local]qvpc-si# threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-pool-release
 | ip-pool-used | ip-pool-usable } interval <time>
[local]qvpc-si#context egress
[egress]qvpc-si# threshold ip-pool-usable <low_thresh> [ clear <high_thresh> ] [ip-pool-usable-final
 <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si# threshold ip-pool-usable 40 clear 50 ip-pool-usable-final 35 clear 36
```

Step 3 Verify the configured values for **ip-pool-usable** and **ip-pool-usable-final** using the **show threshold** CLI command..

Example:

```
 [egress]qvpc-si# show threshold

Threshold operation model: ALARM

No non-default threshold configured

Active thresholds:

Name:             ip-pool-used
Config Scope:     Context[egress]
Threshold:        0%
Clear Threshold:  0%
                        Poll Interval:    60Seconds
Next Poll Time:   2024-Mar-28+13:08:00
```

```
Name:             ip-pool-hold
Config Scope:     Context[egress]
Threshold:        0%
Clear Threshold:  0%
Poll Interval:    300Seconds
Next Poll Time:   2024-Mar-28+13:10:00

Name:             ip-pool-release
Config Scope:     Context[egress]
Threshold:        0%
Clear Threshold:  0%
Poll Interval:    300Seconds
Next Poll Time:   2024-Mar-28+13:10:00

Name:             ip-pool-free
Config Scope:     Context[egress]
Threshold:        0%
Clear Threshold:  0%
Poll Interval:    300Seconds
Next Poll Time:   2024-Mar-28+13:10:00

Name:             ip-pool-usable
Config Scope:     Context[egress]
Threshold:        0%
Clear Threshold:  0%
Poll Interval:    60Seconds
Next Poll Time:   2024-Mar-28+13:10:00

Name:             ip-pool-usable-final
Config Scope:     Context[egress]
Threshold:        0%
Clear Threshold:  0%
Poll Interval:    60Seconds
Next Poll Time:   2024-Mar-28+13:10:00


Name:             available-ip-pool-group
Config Scope:     Context[egress]
Threshold:        10%
Clear Threshold:  10%
Poll Interval:    300Seconds
Next Poll Time:   2024-Mar-28+13:10:00

Name:             cip-local-pool-used
Config Scope:     Context[egress]
Threshold:        0%
Clear Threshold:  0%
Poll Interval:    300Seconds
Next Poll Time:   2024-Mar-28+13:10:00

Name:             cip-local-pool-in-use-addr
Config Scope:     Context[egress]
Threshold:        0
Clear Threshold:  0
Poll Interval:    300Seconds
Next Poll Time:   2024-Mar-28+13:10:00


NOTE: IP pool threshold values can be overridden
      by IP pool configurations.

Enabled threshold groups: (name, scope)
available-ip-pool-group        Context[egress]
```

```
Non-default poll intervals:
ip-pool-used                              60Sec
place-holder                               0Sec
ip-pool-usable                            60Sec
```

Configure Pre and Final Thresholds IPv4 Pool Level

The Clear Hold IPs by Moving to Release State feature supports two thresholds at IPv4 Pool level.

Use this task to enable the **pool-usable** and **pool-usable final** thresholds for ip pool usable of IPs, which are in either FREE or RELEASE states.

These are the types of Pre and final threshold SNMP alarms generated based on the configured thresholds:

- PreThreshIPPoolUsable alarm for entering condition
- PreThreshClearIPPoolUsable alarm for clearing condition
- FinalThreshIPPoolUsable alarm for entering condition
- FinalThreshClearIPPoolUsable alarm for clearing condition

Before you begin

Check if you have configured **pool-usable** for configuring **pool-usable-final**.

To enable the IP Pool Threshold monitoring at pool-level and context-level, refer the IP Pool Thresholds chapter in the *Thresholding Configuration Guide*.

Procedure

Step 1 Configure the IP pool usable pre threshold state as either free or release.

ip pool name alert-threshold [pool-usable *low_thresh* **[clear** *high_thresh* **]]**

Example:

```
 [local]qvpc-si# context egress
 [egress]qvpc-si[egress]qvpc-si #ip pool name alert-threshold pool-usable < low_thresh > [ clear <
high_thresh > ] [pool-usable-final < low_thresh > [ clear < high_thresh > ]]
[egress]qvpc-si# ip pool name alert-threshold pool-usable 50 clear 60 pool-usable-final 30 [clear 50
```

The **PreThreshIPPoolUsable** trap is raised if the ip pool usable is less than or equal to the configured **ip-pool-usable** low threshold value.

The **PreThreshClearIPPoolUsable** trap gets triggered if the pool usable value is greater than a clear high threshold value.

Step 2 Configure the IP pool usable final threshold state in either free or release.

ip pool name alert threshold [pool-usable low_thresh [clear high_thresh] **[pool-usable-final** *low_thresh* **[clear** *high_thresh* **]]]**

The **FinalThreshIPPoolUsable** alarm is raised when the measured pool usable value is less than or equal to the **pool-usable** value. The **FinalThreshClearIPPoolUsable** trap clears when the **pool-usable-final** clear value is greater than clear threshold.

Example:

```
 [local]qvpc-si# context egress
 [egress]qvpc-si[egress]qvpc-si #ip pool name alert-threshold pool-usable < low_thresh > [ clear <
high_thresh > ] [pool-usable-final < low_thresh > [ clear < high_thresh > ]]
[egress]qvpc-si# ip pool name alert-threshold pool-usable 50 clear 60 pool-usable-final 30 [clear 50
```

Configure Pre and Final Thresholds at IPv6 Pool Level

The Clear Hold IPs by Moving to Release State feature supports two thresholds at IPv6 Pool level.

Use this task to enable the **pool-usable** and **pool-usable-final** thresholds for ip pool usable of IPs, which are in either FREE or RELEASE states.

These are the types of Pre and final threshold SNMP alarms generated based on the configured thresholds:

- PreThreshIPPoolUsable alarm for entering condition
- PreThreshClearIPPoolUsable alarm for clearing condition
- FinalThreshIPPoolUsable alarm for entering condition
- FinalThreshClearIPPoolUsable alarm for clearing condition

Before you begin

Check if you have configured **pool-usable** for configuring **pool-usable-final**.

To enable the IP Pool Threshold monitoring at pool-level and context-level, refer the IP Pool Thresholds chapter in the Thresholding Configuration Guide.

Procedure

Step 1 Configure the IP pool usable pre threshold state as either free or release.

ipv6 pool name alert-threshold [pool-usable *low_thresh* **[clear** *high_thresh* **]]**

Example:

```
 [local]qvpc-si# context egress
[egress]qvpc-si# ipv6 pool testv6 alert-threshold pool-usable <low_thresh> [ clear <high_thresh> ]
[ pool-usable-final <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si#  ipv6 pool testv6 alert-threshold pool-usable 40 clear 50 pool-usable-final 35 clear
 36
```

The **PreThreshIPPoolUsable** trap is raised if the ip pool usable is less than or equal to the configured **pool-usable** low threshold value.

The **PreThreshClearIPPoolUsable** trap gets triggered if the pool usable value is greater than a clear high threshold value.

Step 2 Enter the IP pool usable final threshold state as either free or release.

ipv6 pool *alert_name* **alert-threshold pool-usable** *low_thresh* [clear *high_thresh* **[pool-usable-final** *low_thresh* **[clear** *high_thresh* **]]**

Example:

```
[local]qvpc-si# context egress
[egress]qvpc-si# ipv6 pool testv6 alert-threshold pool-usable <low_thresh> [ clear <high_thresh> ]
[ pool-usable-final <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si#  ipv6 pool testv6 alert-threshold pool-usable 40 clear 50 pool-usable-final 35 clear
 36
```

The **FinalThreshIPPoolUsable** alarm is raised when the measured pool usable value is less than or equal to the **pool-usable-final** low threshold value. The **FinalThreshClearIPPoolUsable** trap clears when the **pool-usable** value is greater than a clear high threshold value.

Set Default Threshold Configurations

Use this task to configure default value for context level **ip-pool-usable** and **ip-pool-usable-final** thresholds.

Before you begin

Procedure

Configure the following to set default value for context level **ip-pool-usable** and **ip-pool-usable-final threshold**.

default threshold ip-pool-usable

Example:

```
[egress]qvpc-si(config-ctx)# default threshold ip-pool-usable
[egress]qvpc-si(config-ctx)# default threshold ?
available-ip-pool-group cip-local-pool-in-use-addr cip-local-pool-used ip-pool-free ip-pool-hold
ip-pool-release ip-pool-used ip-pool-usable monitoring
```

Set Default Poll Intervals

Use this task to configure default poll interval for **ip-pool-usable** and **ip-pool-usable-final** thresholds

Procedure

Step 1 Configure default poll interval for **ip-pool-usable** and **ip-pool-usable-final** thresholds.

default threshold poll ip-pool-usable interval

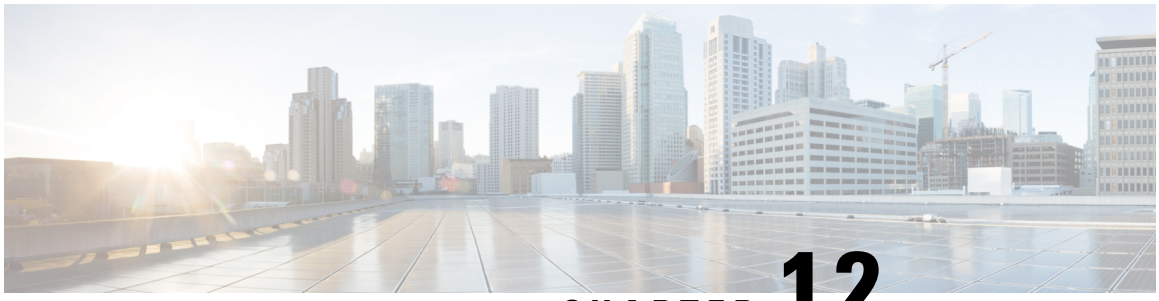
Example:

```
[egress]qvpc-si(config)# default threshold poll ?
ip-pool-free ip-pool-hold ip-pool-release ip-pool-used ip-pool-usable
[egress]qvpc-si(config)# default threshold poll ip-pool-usable ?
[egress]qvpc-si(config)# default threshold poll ip-pool-usable interval
```

Step 2 Verify the default values of thresholds.

Example:

```
[local]qvpc-si# show threshold default | grep -i pool
(context)ip-pool-used 5Min Notify Above 0%
(context)ip-pool-hold 5Min Notify Above 0%
(context)ip-pool-release 5Min Notify Above 0%
(context)ip-pool-free 5Min Notify Below 0%
(context)ip-pool-usable 5Min Notify Below 0%
(context)ip-pool-usable-final 5Min Notify Below 0%
(context)available-ip-pool-group 5Min Notify Below 10%
(context)cip-local-pool-used 5Min Notify Above 0%
(context)cip-local-pool-in-use-addr 5Min Notify Above 0
(disc-rsn)Pool-IP-address-not-valid 15Min Notify Above 0
(disc-rsn)lpool-ip-validation-failed 15Min Notify Above 0
(disc-rsn)lpool-static-ip-addr-not-allowed 15Min Notify Above 0
(disc-rsn)mipha-ip-pool-busyout 15Min Notify Above 0
(disc-rsn)All-dynamic-pool-addr-occupied 15Min Notify Above 0
(disc-rsn)NAT-Pool-BusyOut-Or-Pend-Delete 15Min Notify Above 0
```



CHAPTER 12

Enable Cinder Volume Multi-attach to Multiple VNFs

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In P-GW and SAEGW,the Cinder Volume Multi-attach functionality is enhanced to: • Monitor system volume status through the **monitor system volume** CLI command • Modify the switchover reasons during detach multi-attach cinder volume function • Raise an SNMP trap notification	2024.02.0
First introduced.	21.25

Feature Description

Cinder is the OpenStack Block Storage service for providing volumes to the VNFs. Volumes are block storage devices that is attached to instances to enable persistent storage.

In P-GW, prior to OSP 16.0, operational issues developed when working with Virtual Customer Premises Equipment (VCPE) and RedHat. The Recover VM functionality brings down the VM Control Function (CF) of QvPC-DI and tries to bring it back up on a different compute host due to compute host failures. When a new CF instance comes up and redundant array of independent disks (RAID1) is formed, the active CF instance performs disk synchronization over the internet Small Computer System Interface (iSCSI) channel. This process is done block by block and iterates over the entire disk. Disk synchronization takes place over DI-LAN. When disk sizes are larger than 250GB, it takes time depending on how storage is configured, and DI-LAN network bandwidth, and traffic.

To overcome this issue, OSP16.1 is used to support the Cinder volume multi-attach . You can use this Cinder multi-attach capability to simultaneously attach volumes to multiple VNF instances.

- CF1 (Active) and CF2 (Standby) of QvPC-DI connects to the same multi-attach volume when bringing up the orchestrator.
- StarOS detects if CF1 and CF2 are connected to the same disk volume over the iSCSI channel.
- If a cinder volume multi-attach case is detected, the HD-RAID gets formed using the HD-local disk alone (disk connected to active CF). This process avoids the HD-RAID mirroring to solve the operational issues.

Disk Failures in Multi-attach

For disk failure in multi-attach, CF switchover is not possible as both CFs point to the same volume. If a disk failure is detected for Cinder volume multi-attach, it initiates an automatic ICSR switchover. The Interchassis Session Recovery (ICSR) setup is used to handle disk failure scenarios for Cinder volume multi-attach.

Monitor System Volume Status

When multi-attach cinder volume fails on the active CF card of vPGW, the monitor system volume functionality under the Service Redundancy Protocol (SRP) global configuration mode allows:

- Monitoring the system volume during volume attach and detach using a CLI command.
- Modification of switchover reason when the multi-attach cinder volume detaches from the active CF card and the SRP switch over happens.
- SNMP traps notification when the standby CF card from the active VNF detects volume detach.

Configure Multi-attach Cinder Volume

Use the following CLI command to enable the system to monitor multi-attach cinder volume status from the active CF.

```
configure
   context context_name
      service-redundancy-protocol
      [ no ] monitor system volume
   end
```

NOTES:

- **monitor system volume**: Enables Service Redundancy Protocol (SRP) to monitor volumes.
- **no**: Disables the volume monitoring.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show hd raid verbose

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

- HD Raid
  - Degraded—No (Multiattach)

The following is the sample output:

```
HD RAID:
  State                : Available (clean)
  Degraded             : No(Multiattach)
  UUID                 : 643094ff:2cb03262:6e34e7e0:eddbca63
  Size                 : 214GB (214000000000 bytes)
  Action               : Idle
  Disk                 : hd-local1
```

```
  State                : In-sync component
  Created              : Tue Apr  9 09:00:17 2024
  Updated              : Wed Apr 24 02:21:18 2024
  Events               : 113252
  Model                : QEMU QEMU HARDDISK 2.5+
  Serial Number        : d6ae9d7e-12b1-4b62-93c3-1946ae882113
  Location             : CFC1 A7E5A7CF-561C-48A9-8784-F9580A3A7DAD
  Size                 : 214.7GB (214748364800 bytes)
  Disk                 : hd-remote1
  State                : Valid image of 643094ff:2cb03262:6e34e7e0:eddbca63
  Created              : Tue Apr  9 09:00:17 2024
  Updated              : Wed Apr 24 02:21:18 2024
  Events               : 113252
  Model                : QEMU QEMU HARDDISK 2.5+
  Serial Number        : d6ae9d7e-12b1-4b62-93c3-1946ae882113
  Location             : CFC2 59AE2254-E3C6-4E8C-8A94-03556C1B2EEB
  Size                 : 214.7GB (214748364800 bytes)
```

show srp monitor

The **show srp monitor** command is enhanced to display the volume monitor status for multi-attach cinder volumes.

```
Auth. probe monitor state: Success
Auth. probe monitors up:   0
……
…….
VPP monitor state:          Success
SX monitor state:           Success
Volume monitor state:       Success
```

The **show srp monitor volume** command is enhanced to display the status of multi-attach cinder volumes.

```
[local]laas-setup# show srp monitor volume
+----- Type:  (A) - Auth. probe  (B) - BGP  (D) - Diameter  (F) - BFD  (E) - EGQC
|                     (C) - Card (V) - VPP  (S) - Sx  (M) - Multiattach Cinder Volume
|
|+---- State: (I) - Initializing (U) - Up   (D) - Down
||
||+--- GroupId
|||
vvv IP Addr         Port  Context(VRF Name)                    Last Update
-------------------------------------------------------------------------------
MI-   -                 -          -                 Tue Feb 06 06:04:50 2024
-------------------------------------------------------------------------------
```

show srp call-loss statistics

The **show srp call-loss statistics** show command displays the switchover reason as **Cinder Volume failure** on volume detach in the active CF.

```
[local]CXTMVPGWVNC-Primary-11# show srp call-loss statistics
Thursday December 21 16:23:28 UTC 2023
Switchover-4  started at : Thu Dec 21 16:20:44 2023,  took 1 seconds to finish.
    Switchover reason : Cinder Volume failure
```

Note When the multi-attach volume is detached from the Standby VNF, the following two situations can occur:

- An event of multi-attach volume detachment on the active VNF can cause service impact. This service impact occurs even if the auto SRP switchover is restricted to happen, because both the VNF are not having their Volumes attached.
- Manual execution of the SRP switchover command with or without force can cause the switchover to happen. This service impact is because the peer VNF also does not have multi-attach volume attached to it.

  Hence it is recommended to rectify the HD Raid status of Peer as soon as possible. Also verify that peer HD Raid status is proper before issuing any manual SRP Switchover.

Verify SRP Switchover Reasons through SNMP Traps Notification

The standby CF card raises the following SNMP traps:

- **StorageNotFound**—volume detach
- **StorageFound**—volume attach

When the switchover occurs due to multi-attach volume detach from an active CF card, the SRPSwitchoverOccurred trap displays the reason as **Cinder Volume Failure**.

```
Internal trap notification 1278
 (SRPSwitchoverOccured)  vpn SRP ipaddr 2002:4888:34:13:386:200:0:11 rtmod
 18 Switchover Reason: (18) Cinder Volume Failure
```

Note When cinder volume is re-attached to the active card, it is not automatically detected by the system unless a soft reload is done.

CHAPTER 13

Collision Handling of Modify Bearer Request over Modify Bearer Request Drop and Retry

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 • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide* • *Command Line Interface Reference*

Revision History

Revision Details	Release
First Introduced.	21.28.mx

Feature Description

During a call creation MME sends the first MBR message and while S-GW processes the call, the MME can receive an E-RAB modification indication to send the second MBR to S-GW. To avoid collision over Modify bearer request (mbreq) message over mbreq, the MME supports collision of MBR over MBR Drop and Retry functionality through a `mbreq-over-mbreq drop` CLI configuration under the egtp-service. The following functions occur:

- MME sends modify bearer request when service request modify bearer request is in pending state
- S-GW drops the E-RAB procedure modify bearer request message
- MME retries the dropped MBR until first MBR response.

Enabling or Disabling Modify Bearer Request Messages

Use the following configuration commands to configure the collision handling of Drop second MBreq when first MBreq is pending.

```
configure
   context  context_name
      egtp-service  egtp_service_name
         collision-handling
             csreq-reject-cause
             dbcmd-over-mbreq  { drop | queue }
          mbreq-over-mbreq  { drop }
         { default | no } collision-handling csreq-reject-cause
         { default | no } collision-handling dbcmd-over-mbreq
         { default | no } collision-handling mbreq-over-mbreq
         end
```

NOTES:

- **csreq-reject-cause**: Configures collision handling of CSreq when CSreq or DSreq is pending. The Default or No behavior rejects a new MBreq with cause - No resources available(73).
- **mbreq-over-mbreq**: Configures collision handling of drop second MBreq when MBreq is pending. The Default or No behavior rejects a new MBreq with cause - No resources available(73).
- **mbreq-over-mbreq { drop }** : Drops the received messages.

Monitoring and Troubleshooting

This section describes how to monitor the collision handling feature for MBR over MBR.

Show Command (s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the collision handling on the P-GW/SAEGW/S-GW feature.

show configuration

The output of this command indicates if collision handling for the DBcmd message when the MBreq message is pending is enabled or disabled or for the mbreq over mbreq drop messages:

- collision-handling dbcmd-over-mbreq queue
- no collision-handling dbcmd-over-mbreq queue
- collision-handling mbreq-over-mbreq drop

show egtp-service all-name

The output of this command indicates how the P-GW is configured to handle the MBreq when MBreq messages for the Default Bearer is pending at the P-GW or S-GW.

- Collision handling:
  - DBcmd when MBreq pending: <Queue DBcmd>, <Drop DBcmd>, or <Abort MBreq and handle Dbcmd>

show egtpc statistics debug-info

The output of this show command has been modified to display the following fields for Collision Scenarios MBR over MBR and MBR over MBR Drop and Retry:

```
 Modify Bearer Request RX:
        Total Discarded:                    1   Decode/Validation Failure:          0
        Invalid Transaction State:          0   Piggy Backing Errors:               0
        Invalid Bearer State:               1   Context Not Found:                  0
        Unknown:                            0

Error Events in EGTPC Stack :

Messages from invalid peer:                     0
 DBR/DSR transation created but not used:       0
 Teid Collision with uli mismatch for MBR:      0
 Teid Collision with uli mismatch for BRcmd:    0
 Teid Collision with uli mismatch for DBCmd:    0
 MBReq discarded due to pending MBReq:          1
```

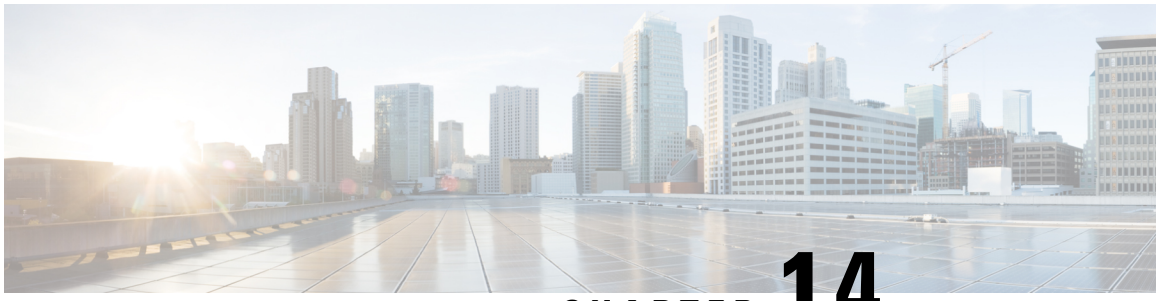
show egtpc statistics verbose

The output of this show command has been modified to display the following fields for Collision Scenarios MBR over MBR and MBR over MBR Drop and Retry:

```
Message Collision Statistics:

 Interface            Old Proc(Msg Type)              New Proc(Msg Type)
   Action            Counter

SGW(S4/S11)    Non-Handover MBReq( 11)   MME/SGSN Trgr MBReq( 11)    Silent Drop New
    1
```



CHAPTER 14

Configuring ACL SRP Checkpoint

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The Access List (ACL) configuration is supported in SRP checkpoint functionality.	2024.02.0
VRF configuration under the BGP router configuration is supported in SRP checkpoint functionality.	21.27.m0

Feature Description

The ICSR setup enables SRP Peer configuration validation for access list (ACL) configurations through the **srp-validate access-list** CLI command. Without the configuration of the CLI, access list configuration were not validated for identicalness between the active and standby in ICSR, resulting in denied traffic to be permitted and vice-versa after a switchover.

For more information, refer to the Configuring SRP Checkpoint section in the *ASR 5500 System Administration Guide*.

Configuring ACL SRP Checkpoint

Use the following configuration to allow the IP and IPv6 access list configurations for the SRP checkpoint functionality.

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] srp-validate access-list
      end
```

NOTES:

- **srp-validate**: Enables SRP Peer configuration validation for specific configurations
- **access-list**: Enables SRP Peer configuration validation for ACL.
- **no**: Disables associating with the access list.

Monitoring and Troubleshooting

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

Show Commands and Output

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

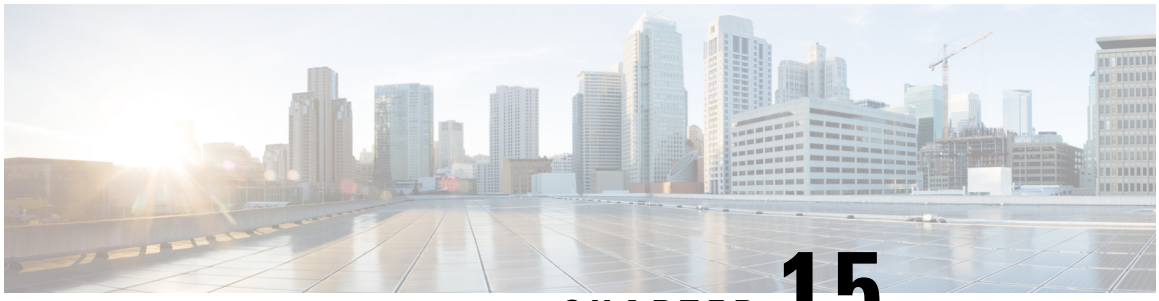
show configuration srp

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

Table 2: show configuration srp Command Output Descriptions

Field	Description
vrf-srp-validate	Indicates that the SRP validation for BGP VRF configuration is enabled.

Field	Description
srp-validate access-list	Displays that the IP and IPv6 access list configurations for the SRP checkpoint validation is enabled.



CHAPTER 15

Detecting Reuse of TCP Ports

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
P-GW supports TCP port reuse through CLI configuration.	21.28.m15

Feature Changes

Previous Behavior: In P-GW, the non-detection of TCP source port reuse lead to Out-of-order (OOO) packet and retransmission packet which inturn resulted in bypassing the charging module and traffic allowed to the server.

New Behavior: In P-GW, the **tcp-detect-port-reuse** CLI is introduced to control the specific flow matching the charging action to detect the source port reuse by TCP SYN packet. The **tcp-detect-port-reuse** CLI also clears the flow in which port is reused and creates new credentials.

Command Changes

This command allows you to detect the source port reuse by TCP packets. When a packet matches to the rule that includes charging action that is enabled with tcp-detect-port-reuse, TCP SYN packet checks for the port reuse. When port reuse is detected the respective flow is cleared and a new flow is created with the new credentials.

```
configure
   context context-name
      active-charging service service_name
         charging-action charging_action_name
           [ no ] tcp-detect-port-reuse
```

NOTES

- **tcp-detect-port-reuse** : Detects the source port reuse by TCP packets. By default this CLI is disabled.
- **no** : Removes the tcp-detect-port-reuse configuration from the charging action.

Monitoring and Troubleshooting

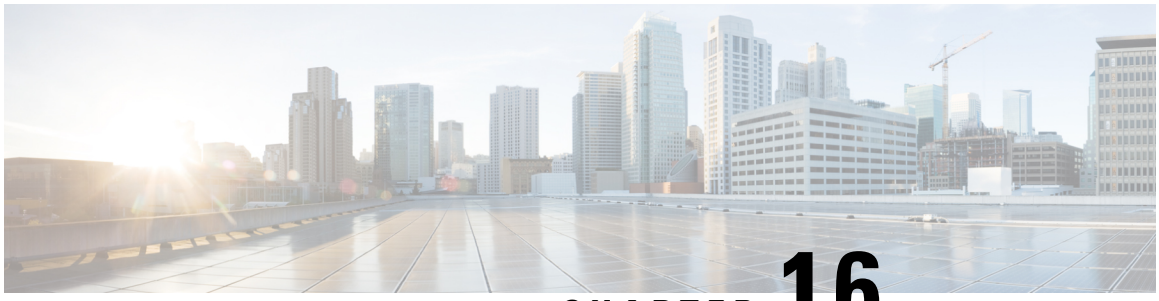
This section provides information about the CLI commands available to monitor and/or troubleshoot TCP port reuse feature.

Show Command(s) and/or Outputs

show active-charging rulebase statistics name

This command displays the following specific flow information matching the charging action to detect the source port reuse. Following is a sample output:

```
show active-charging rulebase statistics name RB_IITC_DAIMLER
      Detect TCP Port Reuse and Flow Cleared:                1
[local]laas-setup# show active-charging charging-action statistics name CA_RG1_NORMAL
 Service Name: ecs-svc1
  Charging Action Name: CA_RG1_NORMAL
    Uplink Pkts Retrans:             32   Downlink Pkts Retrans:             7
    Uplink Bytes Retrans:         13567   Downlink Bytes Retrans:         3558
    Flows Readdressed:                0   PP Flows Readdressed:              0
    Bytes Charged Yet Packet Dropped:                 0
    Predef-Rules Deactivated:         0
    Outer IP header dscp marked Pkts:                0
Detect TCP Port Reuse and Flow Cleared:                  1
```



CHAPTER 16

Differential Charging with 5G NSA

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Fiist Introduced	21.28.M1

Feature Description

MME captures prepaid charging for DCNR subscriber differentially under 4G and 5G coverages through:

- Presence Reporting Area (PRA) action provided by the P-GW
- Tracking of S1-U transport layer address in the Initial Context Setup Response message, E-RAB modification indication message, Path switch request message, and handover required message at the time of forming the Modify Bearer Request against the configuration specified in the MME.
- Configuration of S1-U transport layer addresses (IPv4 and IPv6) in the 5G coverage in a separate profile.
- Enabling the feature in the MME service by associating the profile appropriately.
- Parsing the Presence Reporting Area Action IE in Create Session Response message and Modifying a Bearer Response message from S-GW over an S11 interface.

Standards Compliance

Cisco's implementation of the Differential Charging with 5G NSA makes use of the following standards:

- 3GPP specification 23.401, Section 5.3.3.1
- 3GPP specification 23.401, Section 5.3.3.2
- 3GPP specification 23.401, Section 5.3.4.1
- 3GPP specification 23.401, Section 5.5.1.2.2
- 3GPP specification 23.401, Section 5.3.5
- 3GPP specification 23.401, Section 5.4.7
- 3GPP specification 37.340, Section 10.3.1
- 3GPP specification 37.340, Section 10.4.1
- 3GPP specification 37.340, Section 10.5.1
- 3GPP specification 37.340, Section 10.7.1
- 3GPP specification 37.340, Section 10.8.1
- 3GPP specification 37.340, Section 10.9.1

How it Works

P-GW requests the tracking of UE's presence in the Presence Reporting Area (PRA) in the Create Session Response through the PRA Action IE.

To enable the feature, perform the following functions:

- Create a PRA profile with S1-U IP addresses or address ranges that match gNodeBs.
- Associate the PRA profile with mme-service.

MME stores the PRA ID and the action in the PDN context.

If P-GW sets the action to Start:

- MME compares the S1-U addresses in the bearers with the S1-U address in the S1AP messages and marks if there's a change in address. Then the new S1-U address is compared against the configured address and a change in PRA is identified, which becomes the **Derived RAT Type**.

  S1-U address type is decided based on the Transport Layer address length. With the length as 16 bytes or 20 bytes, it's considered as IPv6 address and with length as 4 bytes, it's considered as IPv4.

- At the time of performing the Modify Bearer Request, if there's a change marked, PRA Information IE is created.

  This feature is available only for the DCNR subscribers with the DCNR flag set in UE network capability in the Initial UE message.

  This section explains call flows and procedures for the following functionalities:

  - Attach procedure.
  - GGSN to PGW Handover procedure
  - Procedure to add Secondary Node.
  - Procedure initiated either by the MN-eNB or by the SN-gNB
  - MN Initiated SN release
  - Secondary Node Change (MN / SN Initiated)
  - Tracking Area Update without S-GW change
  - Tracking Area Update with S-GW change
  - Service Request
  - Inter-Master Node Handover with / without Secondary Node change
  - Master Node to eNB / gNB change
  - eNB / gNB to Master Node change
  - S1 Handover with MME change
  - S1 Release

Initial Attach over S11 Interface

When the Differential Charging with 5G NSA feature is enabled in MME, the following functions occur:

- PRA-based RAT identification and reporting by MME gets triggered when the S-GW sends the PRA ID and the action as **Start** in the Create Session Response message for LTE Initial attach over an S11 interface. This PRA ID is stored in its PDN Context.
- MME receives the S1-U transport layer address from eNB in the Initial Context Setup Response message. By default, the derived RAT type value in a PDN context will be considered as 4G.

While processing the Initial context setup response, the S1 U address will be checked with the configured IP address in the profile and change identified. While framing the Modify Bearer Request, the derived RAT type is found by checking the bearer in that PDN.

GGSN to P-GW Handover

During this GGSN to P-GW handover procedure:

- Forward Relocation Request sent by SGSN does not have PRA Action IE.

Note As Forward Relocation request does not have PRA action , which is sent by SGSN, MME does not send any PRA information as part of GGSN-PGW Handover (HO).

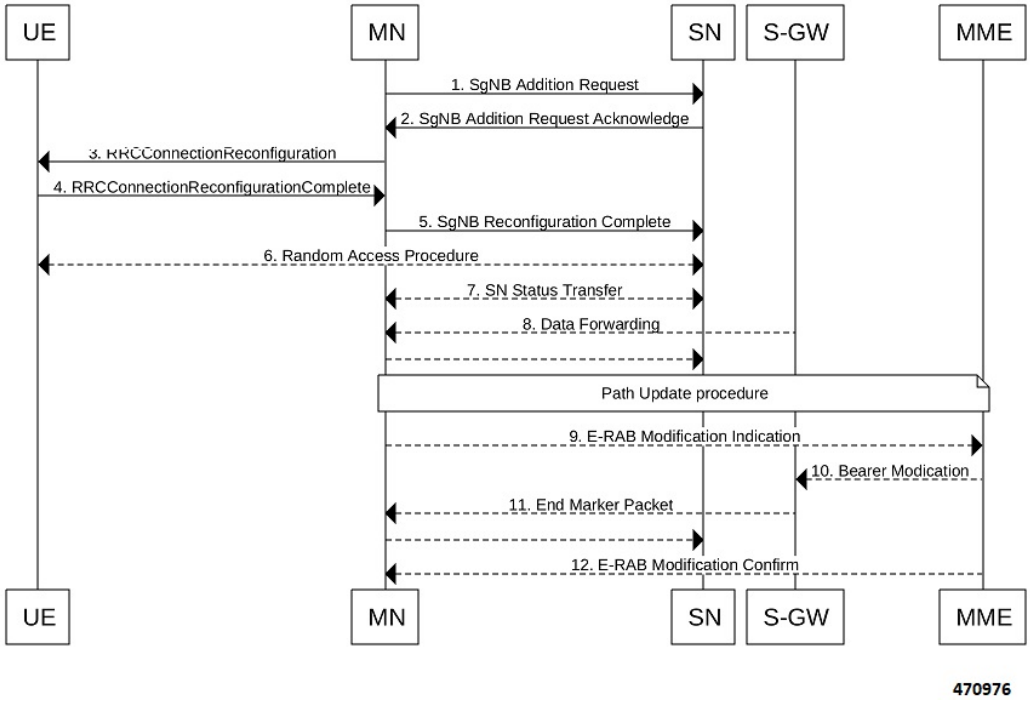
- MME gets PRA Action IE from the Create Session Response message.
- MME sends Create session request to S-GW with DCNR bit set in UP Function Selection Indication Flags, if:
  - The UE is DCNR capable with Dual connectivity of E-UTRA with New Radio (NR) capability bit set in the MS network in MM Context.
  - The NR as Secondary RAT Not Allowed (NRSRNA) is not set in Extended Access Restriction Data in the MM Context of Forward Relocation Request from SGSN.

Adding a Secondary Node

The Secondary Node (SN) addittion procedure follows the procedure defined in 3GPP specification 37.340, Section 10.2.1.

The following call flow shows the secondary node additon.

Figure 1: Call Flow



The secondary node addition procedure captures the LTE attach followed by E-RAB Modification Indication scenario.

When the data bearers move from MN-eNB to SN-gNB, MN-eNB sends E-RAB Modification Indication with bearers to be modified list with the new S1-U transport layer address.

While processing the ERMI message, change in the new S1-U address with the already existing S1-U address in the modified bearer list is marked; it is then compared with the IP address configured in the **pra-profile** for 5G PRA.

While forming the Modify Bearer Request, with the marked changes , if there is a match, the flag IPRA is set to 1 and PRA ID is sent in PRA Information IE in the Modify Bearer Request message over S11.

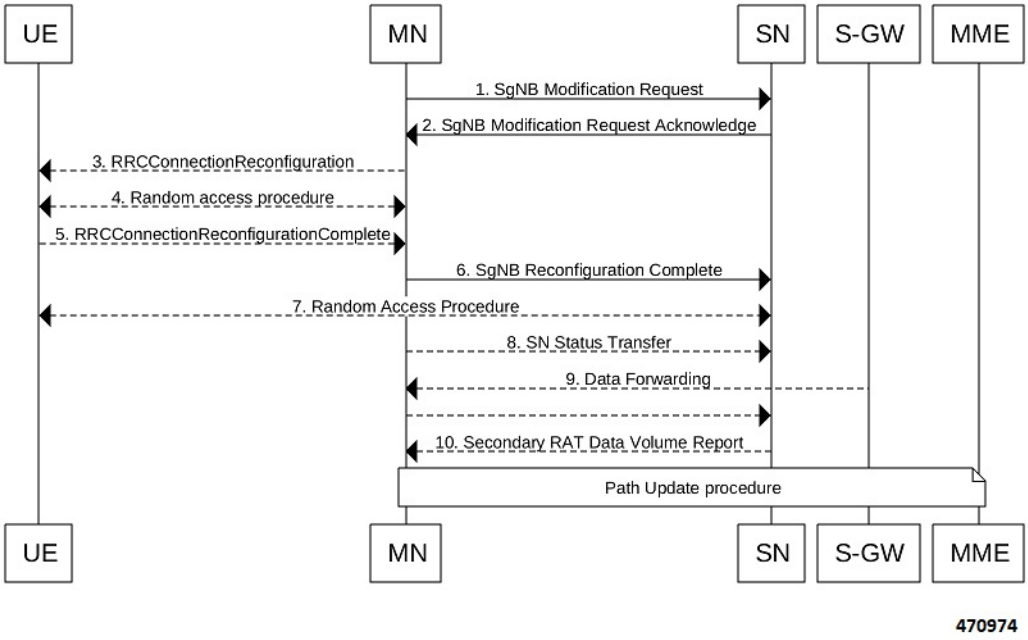
If there is no match, the flag OPRA is set to 1 and PRA ID is ssent in PRA Information IE in the Modify Bearer Request message over S11. PRA Information IE will be sent only if there is any change in the previously sent PRA Information IE for that PDN to that S-GW and the derived RAT type is updated with the current data.

Modifying a Secondary Node

Secondary Node (SN) modification procedure follows the procedure defined in 3GPP specification 37.340, Section 10.3.1.

The following call flow shows the secondary node modification.

Figure 2: Call Flow



This procedure is initiated either by the MN-eNB or by the SN-gNB and used to:.

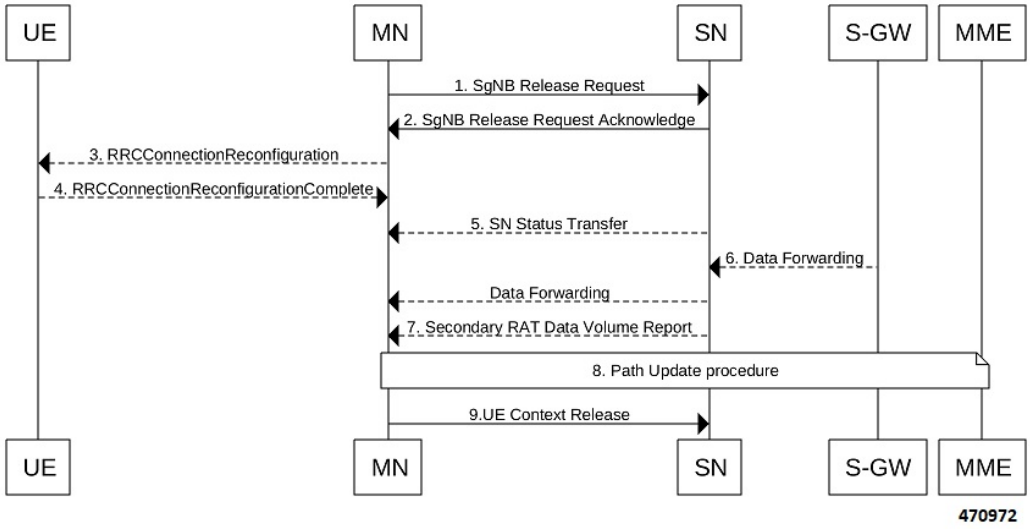
- Modify, establish, or release bearer contexts.
- Transfer bearer contexts to and from the SN-gNB
- Modify other properties of the UE context within the same SN-gNB. This includes the Path Update procedure as explained in the *Adding a Secondary Node* section.

Secondary Node Release Procedure

The Secondary Node release procedure follows the procedure defined in 3GPP specification 37.340, Section 10.4.1.

The following call flow shows the Secondary Node release procedure.

Figure 3: Call Flow



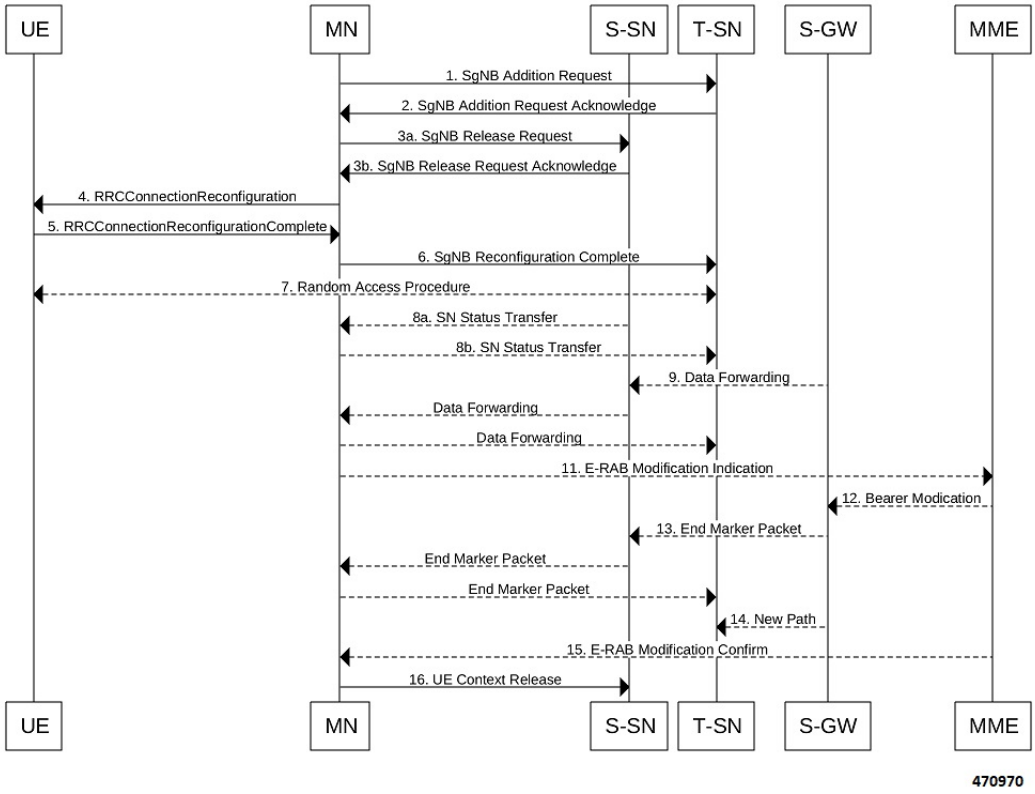
The Secondary Node Release procedure is initiated either by the MN or by the SN and is used to initiate the release of the UE context at the SN. The recipient node of this request can reject the release. For example, if a SN change procedure is triggered by the SN. This includes the Path Update procedure as explained in the section, *Adding a Secondary Node*.

Secondary Node Change

The Secondary Node (SN) change procedure follows the procedure defined in 3GPP specification 37.340, Section 10.5.1. The SN change procedure is initiated either by MN or SN and used to transfer a UE context from a source SN to a target SN, and to change the SCG configuration in an UE from one SN to another. This includes the E-RAB Modification Indication procedure as explained in the section *Adding a Secondary Node*.

The following call flow shows the master node initiated change procedure.

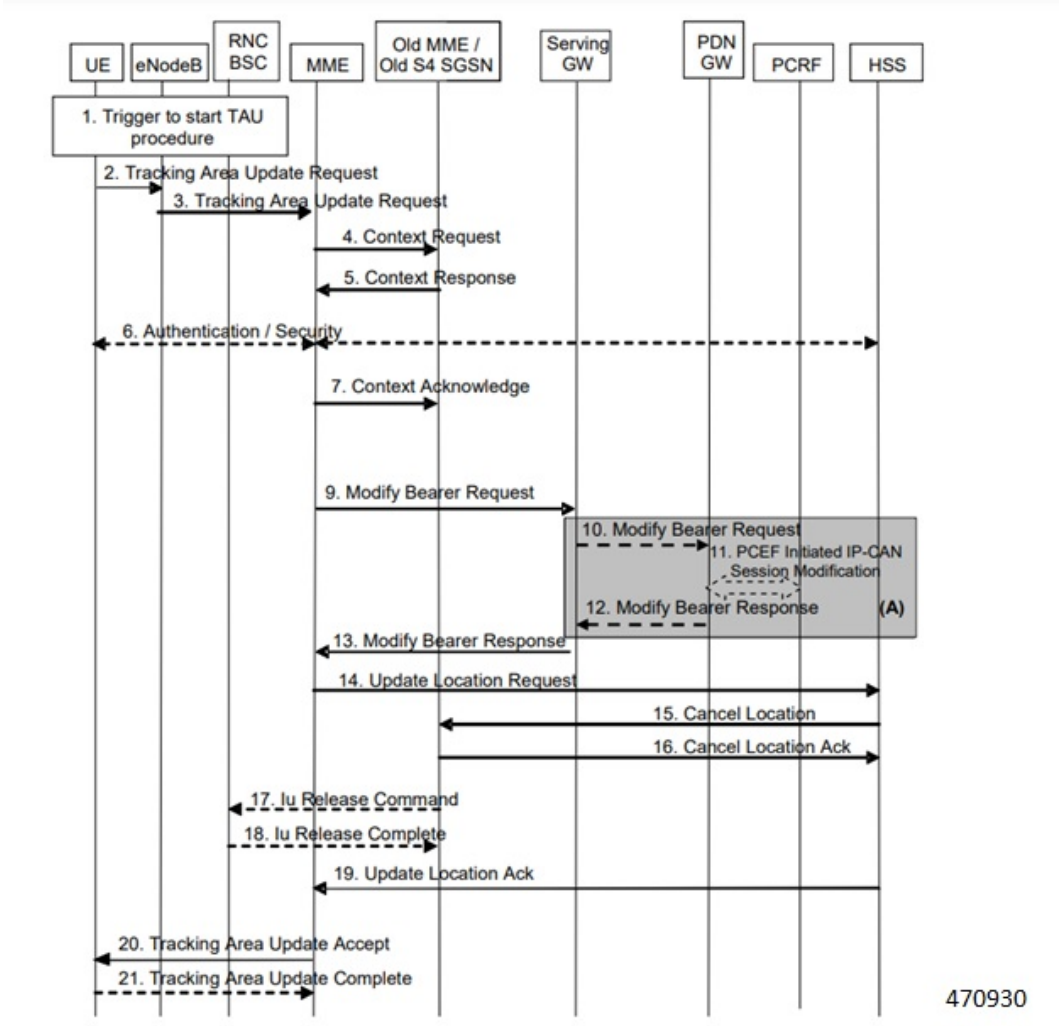
Figure 4: Call Flow



Tracking Area Update without SGW change

Tracking Area Update procedure follows the procedure defined in 3GPP specification 23.401, Section 5.3.3.2. The following call flow shows the Tracking Area Update without SGW change.

Figure 5: Call Flow



Procedure:

- After enabling the Differential Charging with 5G NSA feature in New MME, Presence Reporting Area (PRA) based Radio Access Technology (RAT) identification and reporting by New MME gets triggered when the Old MME sends the PRA ID and the action as **Start** in Context Response message as part of Tracking Area Update procedure over S10 interface.
- As part of Inter MME TAU procedure, if the new MME has established the bearers, it indicates the PRA information in the Modify Bearer request as below whenever MME knows about the s1u IP address:
  - IPRA provided s1u IP address matches with the PRA pool configuration.
  - MME sends OPRA if the previous session was in IPRA with old MME or S-GW. If s1u address is not matched with **pra-profile** there will be no PRA information.

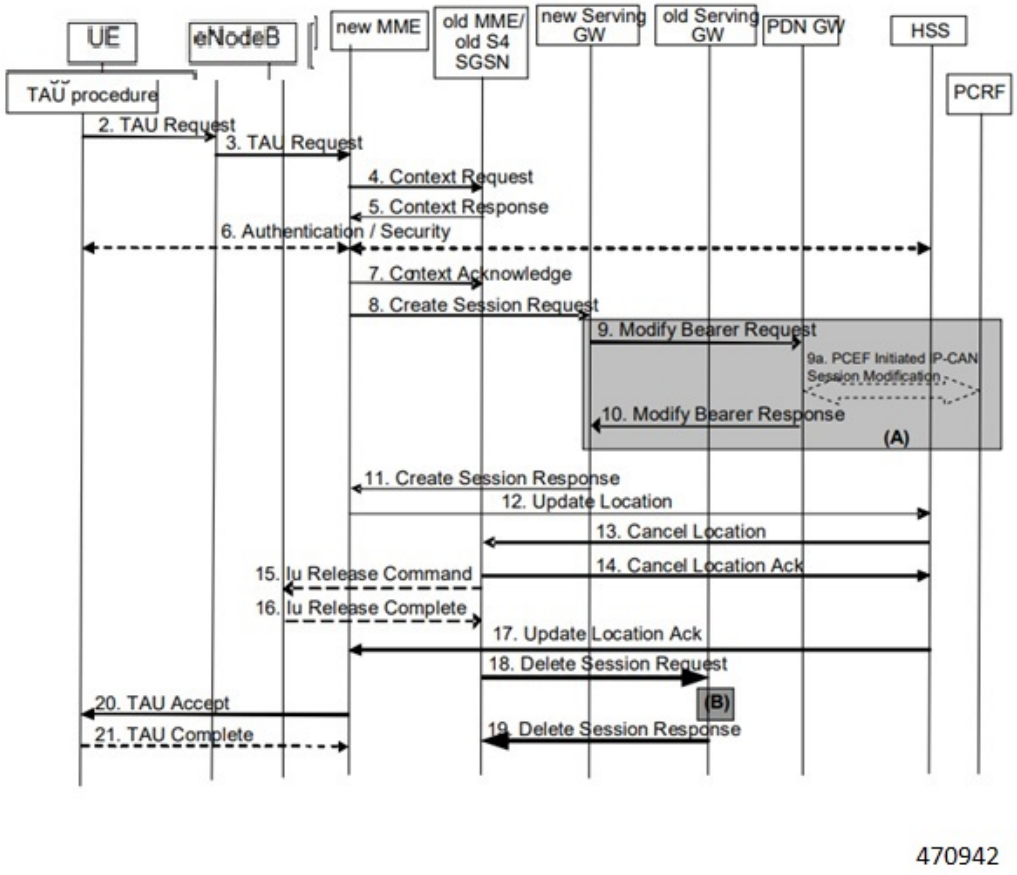
If any changes are identified in s1u address in the subsequent procedure, IPRA or OPRA is calculated accordingly.

Tracking Area Update with SGW Change

Tracking Area Update procedure follows the procedure defined in 3GPP specification 23.401, Section 5.3.3.1.

The following call flow shows the Tracking Area Update with SGW change.

Figure 6: Call Flow



Procedure:

- After enabling the differential charging with 5G NSA feature in New MME, PRA based RAT identification and reporting by New MME gets triggered when the Old MME sends the PRA ID and the Action as ‘Start’ in Context Response message as part of Tracking Area Update procedure over S10 interface.
- As part of Inter MME TAU procedure, if the new MME has established the bearers, it indicates the PRA information in any Modify Bearer Request followed by the Create Session Request as below whenever MME knows about the S1 U IP address:
  - IPRA provided that the S1 U IP address matches with the PRA pool configuration.
  - MME sends OPRA if the previous session was in IPRA with old MME or S-GW. If s1u address is not matched with **pra-profile** there will be no PRA information.

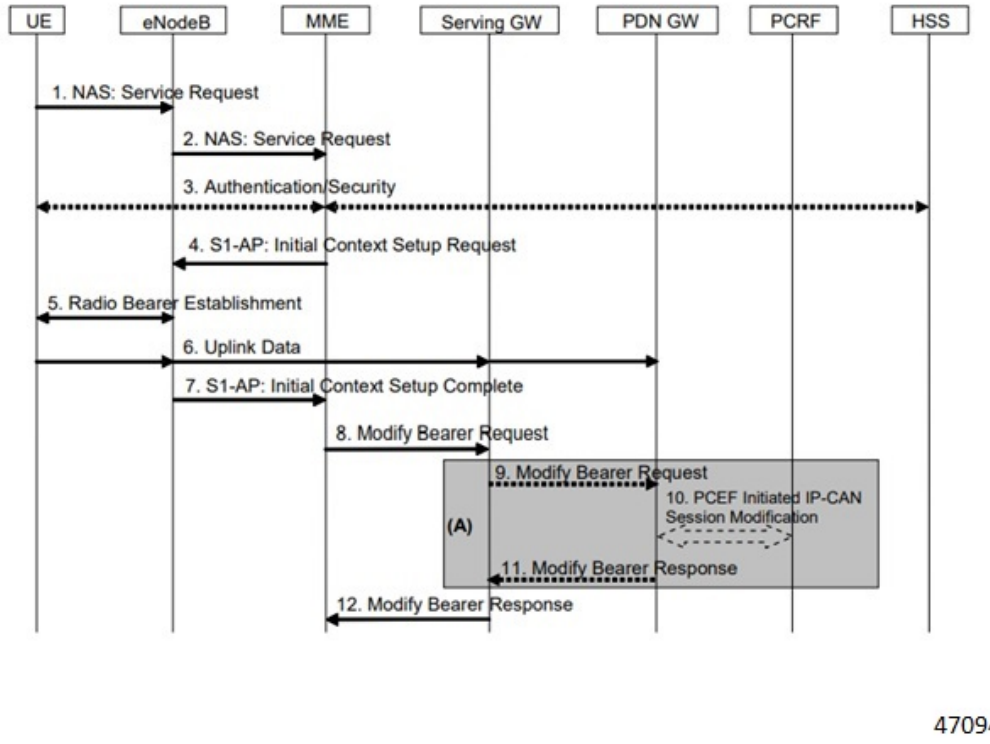
If any changes are identified in S1 U address in the subsequent procedure, IPRA or OPRA is calculated accordingly.

Service Request

Service Request procedure follows the procedure defined in 3GPP specification 23.401, Section 5.3.4.1.

The following call flow shows the Service Request procedure.

Figure 7: Call Flow



Following are few deviations from the defined procedure:

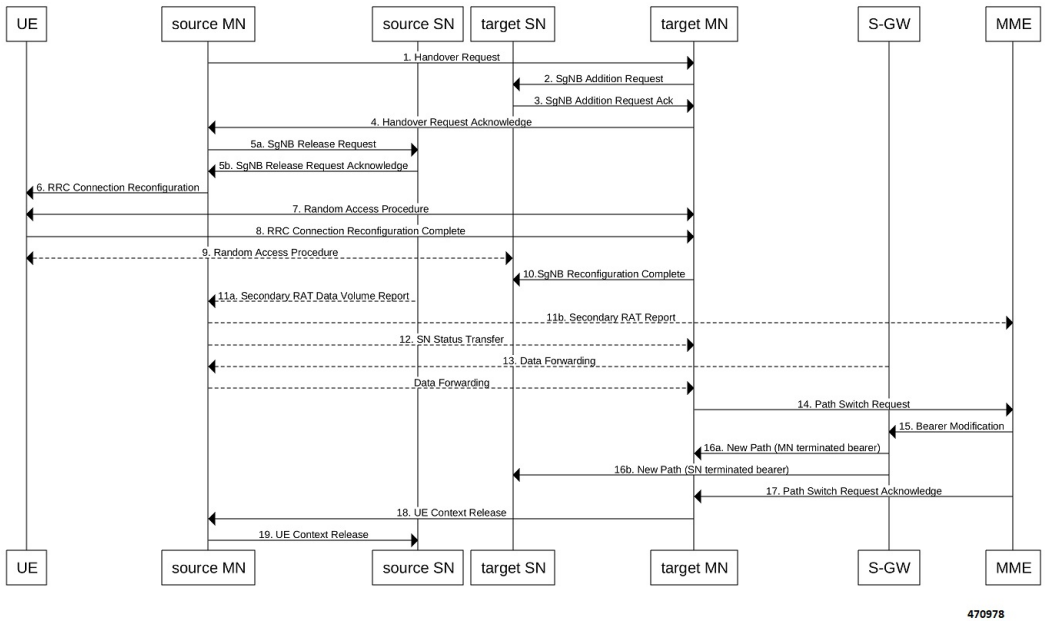
- MME receives the S1-U address in an Initial Context setup Response message.
- S1-U adddress is first matched with the IP address in the respective bearer context and change is marked.
  - If there is a change identified, it is then compared with the IP address configured in the PRA profile for 5G PRA.
  - If there is a match, the flag IPRA is set to 1, and PRA ID is sent in PRA Information IE in the Modify Bearer Request message over S11.
  - If there is no match, the flag OPRA is set to 1 and PRA ID is sent in PRA Information IE in the Modify Bearer Request message over S11.
  - PRA Information IE is sent only if there is any change in the previously sent PRA Information IE for that PDN to that S-GW and the derived RAT type is updated with the current data.

Inter-Master Node Handover with or without Secondary Node Change

Inter-Master Node handover procedure follows the procedure defined in 3GPP specification 37.340, Section 10.7.1.

The following call flow shows the processing of Path Switch Request.

Figure 8: Call Flow



The new S1-U transport layer address in the E-RABs Switched in Downlink Item IEs in Path Switch Request message is first matched with the IP address in the already existing respective bearer context and change is identified.

While forming the Modify Bearer Request:

- If there is a change identified, it is compared with the IP address configured in the PRA profile for 5G PRA.
- If there is a match, the flag IPRA ia set to 1 and PRA ID ia sent in PRA Information IE in the Modify Bearer Request message over S11.
- If there is no match, the flag OPRA is set to 1 and PRA ID is sent in PRA Information IE in the Modify Bearer Request message over S11.

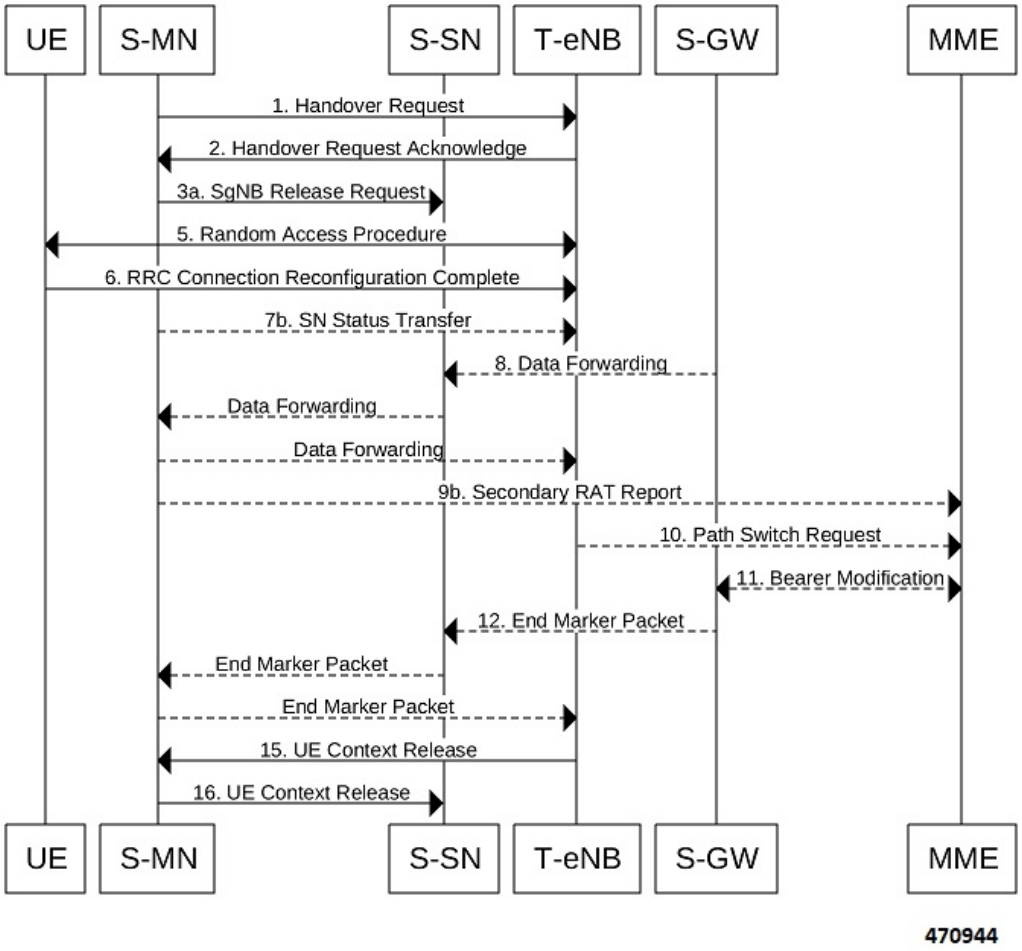
  PRA Information IE is only sent if there is any change in the previously sent PRA Information IE for that PDN to that S-GW and the derived RAT type is updated with the current data.

Master Node to eNB / gNB Change

Master Node (MN) to eNB or gNB change procedure follows the procedure defined in 3GPP specification 37.340, Section 10.8.1. Processing of Path Switch Request is same as explained in the section *Inter-Master Node Handover with or without Secondary Node Change*.

The following call flow shows the master node to eN /gNB change procedure.

Figure 9: Call Flow



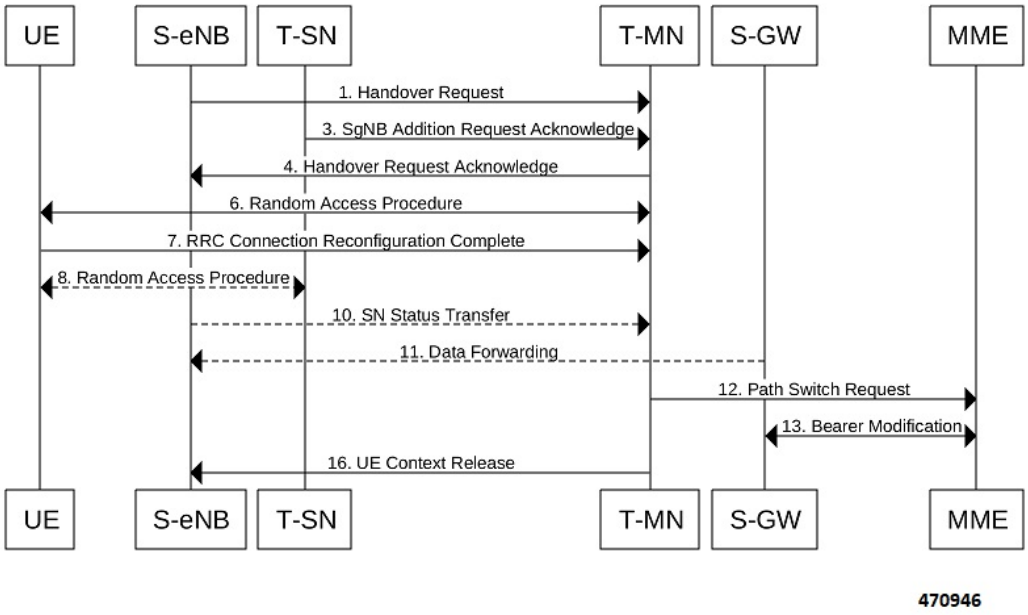
eNB or gNB to Master Node Change

The eNB or gNB to master node change procedure follows the procedure defined in 3GPP specification 37.340, Section 10.9.1. Processing of Path Switch Request is same as explained in the section *Master Node to eNB / gNB Change*.

The eNB or gNB to Master Node Change procedure transfers context data from a source eNB to a target Master Node (MN) that adds an Secondary Node (SN) during the handover.

The following call flow shows the eNB or gNB to master node change procedure.

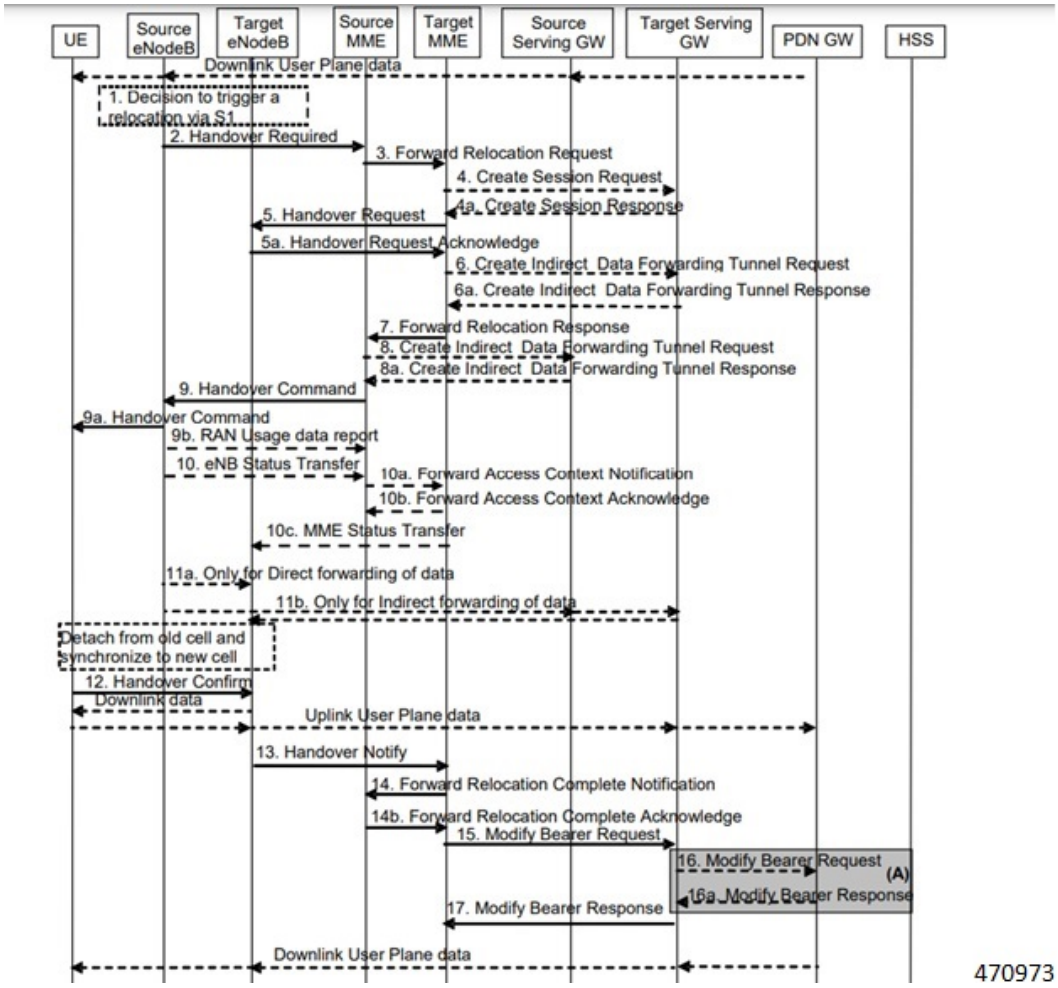
Figure 10: Call Flow



S1 Handover with MME Change

Service Request procedure follows the procedure defined in 3GPP specification 23.401, Section 5.5.1.2.2. The following call flow shows the S1 handover with MME change procedure.

Figure 11: Call Flow



Procedure:

- With feature enabled in Target MME, PRA-based RAT identification and reporting by Target MME gets triggered, when the Source MME sends the PRA ID, and the action as **Start** in Forward Relocation Request message as part of an S1-based handover relocation procedure over S10 interface.
- As part of Inter MME TAU, if the target MME has established the bearers, it indicates the PRA information in the Modify Bearer Request followed by a Create Session Request whenever MME knows about the S1-U IP address:
  - IPRA provided S1-U IP address matches with the PRA pool configuration.
  - MME sends OPRA if the previous session was in IPRA with old MME or S-GW. If s1u address is not matched with **pra-profile** there will be no PRA information.

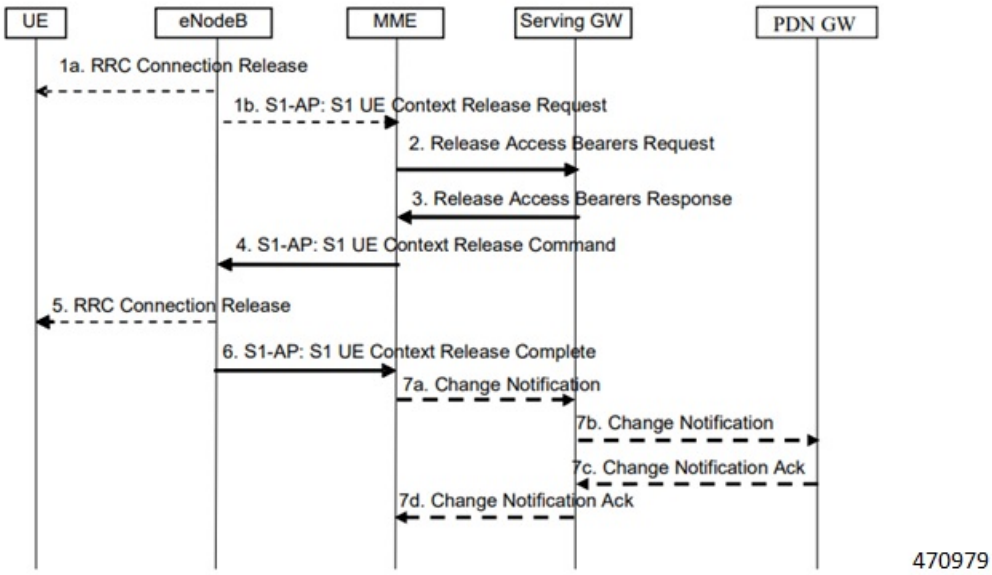
If any changes are identified in S1 U address in the subsequent procedure, IPRA or OPRA is calculated accordingly.

S1 Release

S1 Release procedure follows the procedure defined in 3GPP specification 23.401, Section 5.3.5.

The following call flow shows the S1 release procedure.

Figure 12: Call Flow



PRA based RAT identification and reporting by the MME is stopped as part of this procedure until the connection is resumed. PRA is not supported in the Change Notification.

Configuring gNB S1-U IP Addresses

Use the following commands to configure the gNB S1-U IP addresses in ranges. By default, an gNB S1-U IP address is not configured.

For IPv4 addresses or IPv6 addresses, a maximum of 50 entries can be given in a PRA profile. Altogether, a maximum of 100 entries can be given in a PRA profile and only one PRA profile is supported.

```
configure
  context context_name
    lte-policy
    [ no ] pra-profile dcnr-5g-radio  profilename1
      [ no ] gnb-s1u ipv4-network <address>/[ mask ]
      [ no ] gnb-s1u ipv4-range from <start-ip/mask> to <end-ip/mask>
      [ no ] gnb-s1u ipv6-prefix <address>/[mask]
      [ no ] gnb-s1u ipv6-prefix-range from <start-ip/mask> to
<end-ip/mask>
      [ no ] gnb-s1u ipv6-prefix-pattern <address/mask> start-bit <bit
position>
            end-bit <bit position> pattern <pattern in hex value>
```

NOTES:

- **pra-profile**: Configures PRA Profile.
- **dcnr-5g-radio**: Configures PRA Profile to identify DCNR subscriber in 5G coverage.

  profile_name: Specifies the PRA profile name with a string of size 1–63..

  - **do**: Spawns an exec mode command which displays information to the administrator.
  - **end**: Exits configuration mode and returns to the Exec Mode
  - **exit**: Exits current configuration mode, returning to previous mode
  - **gnb-s1u**: Configures gNB S1-U Addresses for 5G radio connectivity
  - **no**: Disables options.

- **gnb-s1u**
  - **ipv4-network** : Configures gNB S1-U IPv4 network for 5G radio connectivity.
  - **ipv4-range**: Configures gNB S1-U IPv4 address range for 5G radio connectivity.
  - **ipv6-prefix**: Configures gNB S1-U IPv6 network for 5G radio connectivity.
  - **ipv6-prefix-pattern**: Configures gNB S1-U IPv6 prefix range with hex-pattern for 5G radio connectivity.
  - **ipv6-prefix-range**: Configures gNB S1-U IPv6 prefix range for 5G radio connectivity

- **gnb-s1u ipv4-network** *address/mask*: Configures block of addresses. If the mask is not specified, a default mask of 32 bits for the IPv4 address is considered.

  When **gnb-s1u ipv4-network** *0.0.0.0* is configured, it indicates that any IPv4 address will be considered as gnb-s1u address, and no lookup is done with the already configured IPv4 addresses in the profile. In this input, default mask is taken irrespective of any configured mask.

- **gnb-s1u ipv4-range from <start-ip/mask> to <end-ip/mask>**: Specifies a range of IP addresses for a given mask. The mask value should be the same in the *start-ip* and in *end-ip*. Following are few conditions:
  - In the range, if Network ID is specified, then starting address and ending address is calculated according to the mask.
  - In the range, if host address is specified then it will be taken.
  - You can specify either Network ID for both the starting address and ending address or Host ID for both the starting address and ending address.
  - In the range, if mask is not specified, a default mask of 32 bits is considered for IPv4 and the specified address is considered as host address.

- **gnb-s1u ipv4-range**
  - **from**: Enter the first gNB S1-U IPv4 address in the range.
  - **to**: Enter the last gNB S1-U IPv4 address in the range.

- **gnb-s1u ipv6-prefix** *address/mask*: Configures block of addresses. If the mask is not specified, default mask of 128 bits for an IPv6 address is considered. For example, if an ipv6 range is specified from 2001:4900:0050:2001::0/64, then all addresses with the network id 2001:4900:0050:2001 is considered.

Note When **gnb-s1u ipv6-prefix :: is** configured, it indicates that any IPv6 address is considered as gnb S1 U address, and there is no lookup with the already configured IPv6 addresses in the profile. In this input, a default mask is taken irrespective of any configured mask.

  - **ipv6-prefix** : Configures S1-U IPv6 addresses.

- **gnb-s1u ipv6-prefix-range from <start-ip/mask> to <end-ip/mask>** : Specifies a range of IP addresses for a given mask. Ensure to enter the same mask value in the *start-ip* and in the *end-ip*.
  - **from**: Enter the first gNB S1-U IPv6 address in the range.
  - **to**: Enter the last gNB S1-U IPv6 address in the range.

    For example, If you specifiy ipv6 range from 2001:4900:0050:2001::0/64 to 2001:4900:0050:20aa::0/64", then all addresses with the network id "2001:4900:0050:2001" to "2001:4900:0050:20aa" is considered.

  In the range if:
  - Network ID is specified, then starting address and ending address is calculated according to the mask.
  - Host address is specified then, it will be taken.
  - You can specify either Network ID for both the starting address and ending address or Host ID for both the starting address and ending address.
  - Mask is not specified, default mask of 128 bits is considered for IPv6 and the specified address is considered as the host address.

- **gnb-s1u ipv6-prefix-pattern <address/mask> start-bit** *bit position* **end-bit** *bit position* **pattern** *pattern in hex value*
  - **start-bit** *bit position* : Starting bit position of the pattern. It should be outside the mask bits
  - **end-bit** *bit position* : Ending bit position of the pattern. It should be outside the mask bits.
  - **pattern** *pattern in hex value*: Enter the pattern in hexadecimal. A maximum of 64 bit pattern is supported.

Note The start-bit and end-bit position should not be within the mask bits. For example, if you specify gnb-s1u ipv6-prefix-pattern 2001:4900:0050:2000::0/16 start-bit 61 end-bit 64 pattern 0x3", then all addresses with the network id "2001:4900" and with bits 61–64 matching to 0x3 are considered. A maximum of 64-bit pattern is supported for an IPv6 address.

Limitations: Following are the limitations:

- It is recommended to provide non duplicate, or non overlapping IP addresses, or non conflicting inputs across the CLIs.
- It is recommended not to configure multicast or broadcast IP addresses.

Associating pra-profile dcnr-5g-radio with mme-service

You can associate the pra-profile dcnr-5g-radio with the mme-service using the following CLI commands.

```
configure
  context context_name
    mme-service mme service name
      [ no ] associate pra-profile dcnr-5g-radio profilename1
```

NOTES:

- **associate pra-profile**: Associates a PRA profile to the MME service
- **associate pra-profile dcnr-5g-radio**: Associates PRA Profile for 5G-RADIO access to enable differential charging in 5G NSA to the MME service.
- *profilename*: Enter the profile name with a string of size 1–63.

Monitoring and Troubleshooting

This section provides information regarding show commands and outputs available to monitor and troubleshoot the Differential Charging with 5GNSA feature.

Show Commands and Outputs

This section provides information regarding show commands and/or their outputs in support of the PRA based RAT identification and reporting feature.

show lte-policy pra-profile dcnr-5g-radio full all

The **show lte-policy pra-profile dcnr-5g-radio full all** command displays PRA profile of DCNR subscribers in 5G coverage. The output of this command includes the following fields.

Field	Description
PRA Profile to identify DCNR subscriber in 5G coverage	Displays the configured profile name.

Field	Description
S1 U IPv4 address	Displays the configured IPv4 range of addresses. Example: <starting IP address> to <ending IP address> … <IP address> / <mask> …
S1 U IPv6 address	Displays the configured IPv6 range of addresses. Example: <starting IP address> to <ending IP address> … <IP address> / <mask> … <IP address> / <mask> Pattern - <pattern> from bit <starting bit#> to bit <ending bit#> …

show mme-service all

The output of this command includes the following information:

```
When PRA profile is associated with mme-service:
PRA Profile to identify
DCNR subscriber in 5G coverage : Enabled
PRA Profile Name               : <profile name>

When PRA profile is not associated with mme-service:
PRA Profile to identify
DCNR subscriber in 5G coverage : Disabled
```

show mme-service session full

The **show mme-service session full** command shows the last reported PRA information per PDN.

```
…
PDN Information:
…
PDN PRA Info:
PRA ID : <PRA id>
PRA Action: <0 – Action is not set yet, 1 – Start, 2 – Stop >>
PRA Status: <1 – IPRA, 0 – OPRA >
```

show mme-service statistics verbose

The **show mme-service statistics [verbose]** displays procedure -wise statistics for IN PRA and OUT PRA along with the Overall Total counts.

You can view similar statistics information using the **show mme-service statistics esm-only [verbose]** command.

Field	Description
DCNR NSA PRA Statistics:	
Total IPRA	Shows the total number of IPRA count.

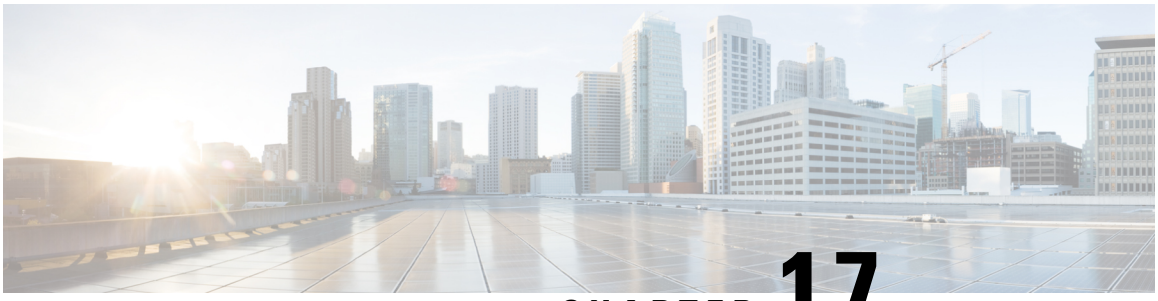
Field	Description
Total OPRA	Shows the total number of OPRA count.
IPRA:	
S1-Handoff	Shows the S1 handoff procedure-wise statistics count for IPRA.
Intra-MME-S1-Handoff-SGW-Change	Shows the Intra MME S1 handoff S-GW change procedure-wise statistics count for IPRA.
TAU	Shows the Tracking Area Update (TAU) procedure-wise statistics count for IPRA.
Intra-MME-TAU-SGW-Change	Shows the Intra MME Tracking Area Update (TAU) S-GW change procedure-wise statistics count for IPRA.
X2HO	Shows the X2HO procedure-wise statistics count for IPRA.
X2HO-SGW-Change	Shows the X2HO S-GW change procedure-wise statistics count for IPRA.
Service Request	Shows the service request procedure-wise statistics count for IPRA.
S10-Handoff	Shows the S10 handoff procedure-wise statistics count for IPRA.
ERAB-Modify	Shows the ERAB modification procedure-wise statistics count for IPRA.
OPRA:	
S1-Handoff	Shows the S1 handoff procedure-wise statistics count for OPRA.
Intra-MME-S1-Handoff-SGW-Change	Shows the Intra MME S1 handoff S-GW change procedure-wise statistics count for OPRA.
TAU	Shows the Tracking Area Update (TAU) procedure-wise statistics count for OPRA.
Intra-MME-TAU-SGW-Change	Shows the Intra MME Tracking Area Update (TAU) S-GW change procedure-wise statistics count for OPRA.
X2HO	Shows the X2HO procedure-wise statistics count for OPRA.
X2HO-SGW-Change	Shows the X2HO S-GW change procedure-wise statistics count for OPRA.
Service Request	Shows the service request procedure-wise statistics count for OPRA.
S10-Handoff	Shows the S10 handoff procedure-wise statistics count for OPRA.
ERAB-Modify	Shows the ERAB modification procedure-wise statistics count for OPRA.

Bulk Statistics

show mme-service statistics

The following two Bulk statistics are added in the MME schema to show the total IN PRA and OUT PRA count:

- dcnr-nsa-ipra-count: Shows the total number of IPRA count.
- dcnr-nsa-opra-count: Shows the total number of OPRA count.



CHAPTER 17

Dynamic S-GW Selection for Interworking-5GC

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
CLI configuration support is added for enabling the reject EPS to 5Gs procedure without n1 mode support.	2024.02.0
Support is introduced for dynamic selection mechanism to select SGW-C+SMF through s11 interface.	21.28.m7
Support is introduced for dynamic selection mechanism to select PGW-C+SMF and peer-AMF.	21.25

Revision Details	Release
The N26 interface for interworking with 5GS functionality is fully qualified in this release.	21.20.3
MME supports N26 interface between AMF in 5GC and MME in Evoloved Packet Core (EPC) to provide seamless session continuity for single registration mode UE. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.20
First introduced. This release supports N26 Interface for interworking with 5GS functionality. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.19

Feature Description

MME supports selection of combined SGW-C/SMF on the base of DNS S-NAPTR queries using the **3gpp-x-3gpp-sgw:x-s11** service parameter for UEs supporting N1 mode and optionally matching an UE Usage type.

DNS Mechanism to Select SGW-C+SMF

MME supports the SGW-C+SMF selection for Nonemergency PDN connection based on the following conditions:

- UE N1 Mode capability (UE Network Capability)
- (Optional) Matching a UE Usage type

S-NAPTR query is performed to identify the SGW-C+SMF based on the below S-NAPTR procedure with service parameters:

- MME considers the **n1-mode 5gs-interworking-with-n26 sgw-selection s11** CLI when forming the service parameter in the SGW-C+SMF DNS S-NAPTR requests.

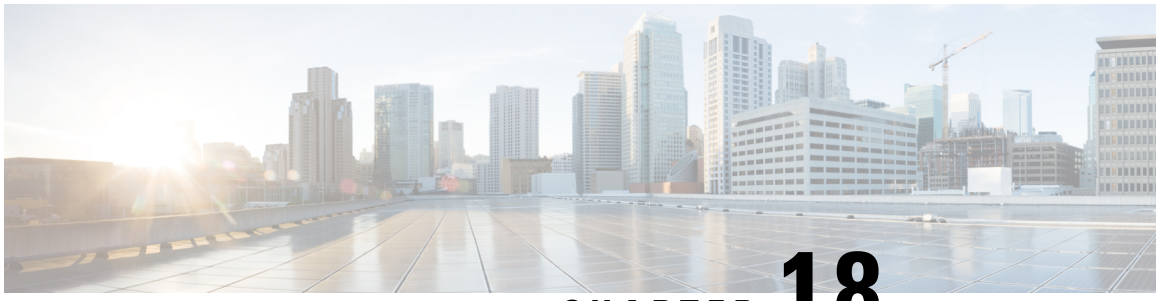
  If the UE is in N1 mode and CLI is configured with S11 and no UE usage type is specified, then, MME sends the DNS S-NAPTR query using the x-3gpp-sgw:x-s11 service parameter to select the SGW-C+SMF.

- If UE is in N1 mode and CLI is configured with S11 and UUT, MME matches the UE's UUT with CLI UUTs. Then MME, sends DNS S-NAPTR query using the x-3gpp-sgw:x-s11 service parameter. Else, sends the DNS S-NAPTR query using the **x-3gpp-sgw:x-s11** service parameter to select the S-GW.

  ```
  Example: n1-mode 5gs-interworking-with-n26 sgw-selection s11 ue-usage-type 128 129 130
  131 132 133 134 135
  ```

The S-NAPTR procedure logically displays a list of host names each with a service, protocol, port, and a list of IPv4 and IPv6 addresses. From the candidate list, MME selects the best node based on the Topology, Collocation, Order, or Weight.

For more information, see the *5GS Interworking using N26 Interface Support* chapter in the *MME Configuration and Administration Guide*.



CHAPTER 18

Encoding Subscription-ID AVP in CCR-I Messages on the Gy Server

Revision History

Revision History

Revision Details	Release
P-GW supports encoding of Subscription-ID AVP in CCR-I message towards Gy server.	2024.02.0

Behavior Change

Currently, Subscription-Id AVP is encoded in the Gy CCRs based on dictionary and service-type checks.. Each service can have a maximum of three Subscription-Id types (e164, imsi, and nai) that can be configured through CLI command.

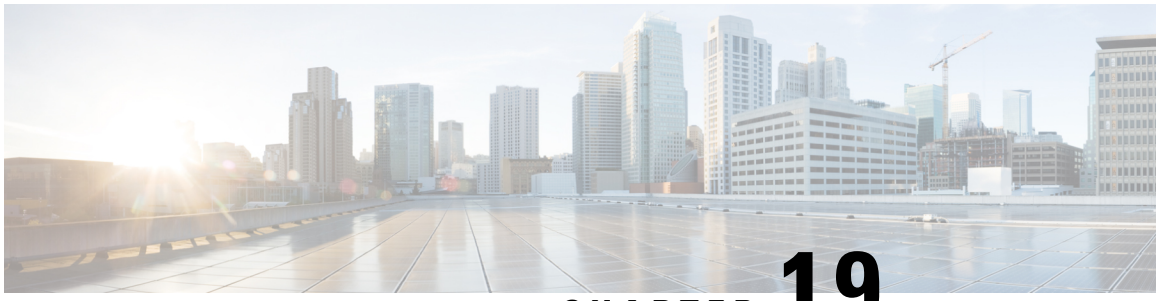
Previous Behavior: The IMSI value is encoded in e164 Subscription-Id type in the CCR-I message toward the Gy server when MSISDN is not present in the Create Session Request message.

New Behavior: When MSISDN is not present in the Create Session Request message, the e164 type Subscription-Id AVP is not encoded.

For example, the following command configures a combination of all three Subscription-Id type such as **e164**, **imsi**, or **nai** type for P-GW service:

subscription-id service-type pgw { e164 | imsi | nai }

Customer Impact: No impact on the online charging as the mandatory IMSI IE gets included in the Gy CCR-I messages.



CHAPTER 19

Encoding Subscription-ID AVP in CCR-I Messages on the Gy Server

Revision History

Revision History

Revision Details	Release
P-GW supports encoding of Subscription-ID AVP in CCR-I message towards Gy server.	2024.02.0

Behavior Change

Currently, Subscription-Id AVP is encoded in the Gy CCRs based on dictionary and service-type checks.. Each service can have a maximum of three Subscription-Id types (e164, imsi, and nai) that can be configured through CLI command.

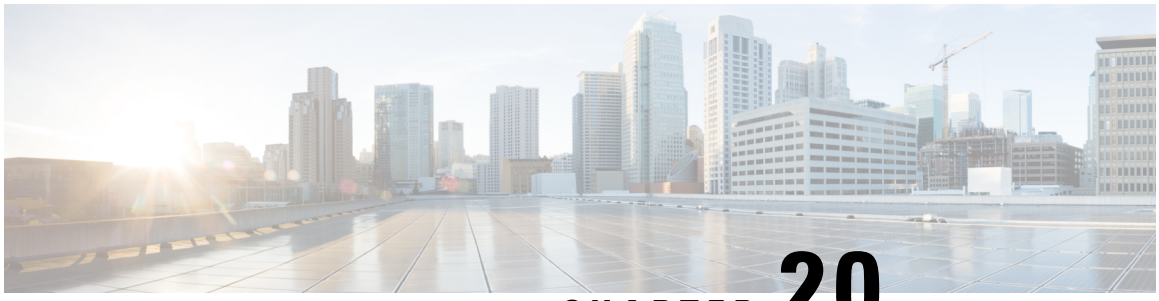
Previous Behavior: The IMSI value is encoded in e164 Subscription-Id type in the CCR-I message toward the Gy server when MSISDN is not present in the Create Session Request message.

New Behavior: When MSISDN is not present in the Create Session Request message, the e164 type Subscription-Id AVP is not encoded.

For example, the following command configures a combination of all three Subscription-Id type such as **e164**, **imsi**, or **nai** type for P-GW service:

subscription-id service-type pgw { e164 | imsi | nai }

Customer Impact: No impact on the online charging as the mandatory IMSI IE gets included in the Gy CCR-I messages.



CHAPTER 20

Enhancement in Bulkstats in MME Schema for HSS CLR

Revision History

Revision Details	Release
Update in the existing Bulkstats **emm-msgtx-attach-rej-network-fail-smgr-resource-unavailable** and **emm-msgtx-attach-rej-nw-fail-hss-abort-ex-sub-withdrawn** and new bulkstat **emm-msgtx-attach-rej-network-fail-hss-cancel-except-sw**.	21.28
First Introduced.	21.11

Behavior Change

Previous Behavior: The existing counter **emm-msgtx-attach-rej-network-fail-smgr-resource-unavailable** was incrementing in following two events:

- When system resource limits have been crossed.
- When Cancel Location Request message(excluding the subscription withdrawal) is received from HSS.

However, the name and description of the counter was not reflecting the second event.

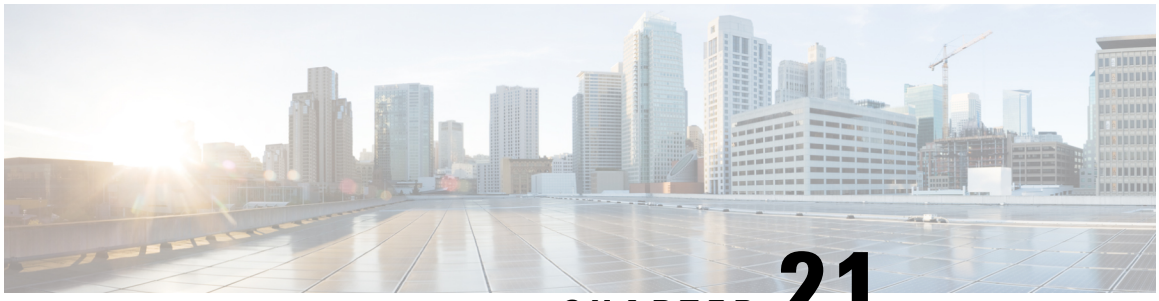
New Behavior: To handle this, the decsription of the counter **emm-msgtx-attach-rej-network-fail-smgr-resource-unavailable** is modified. This counter shows the total number of attach reject messages sent for an attach request for an attach request with a cause code Network Failure, when the rejection is due to SessMgr resources being unavailable.

The description of the existing counter **emm-msgtx-attach-rej-nw-fail-hss-abort-ex-sub-withdrawn** is also changed. Now, this counter shows the total number of Attach procedure not completing due to HSS CLR, excluding cancellation type of subscription withdrawal. This includes scenario of attach reject with network

failure and also attach abort where CLR abort happened after attach accept is sent and before attach complete received.

A new counter **emm-msgtx-attach-rej-network-fail-hss-cancel-except-sw** is introduced provides the total number of Attach Reject messages sent for an Attach Request, with a cause code Network Failure, when the rejection is due to HSS CLR, excluding cancellation type of subscription withdrawal.

Customer Impact: As a result of this enhancement, the customer needs to update the KPI formula for attach success ratio and configure new bulkstats.



CHAPTER 21

Enhanced SGW CDR nodeID Encoding for Larger Instance Numbers Support

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	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Reference Guide* • *ASR 5500 System Administration Guide* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide*

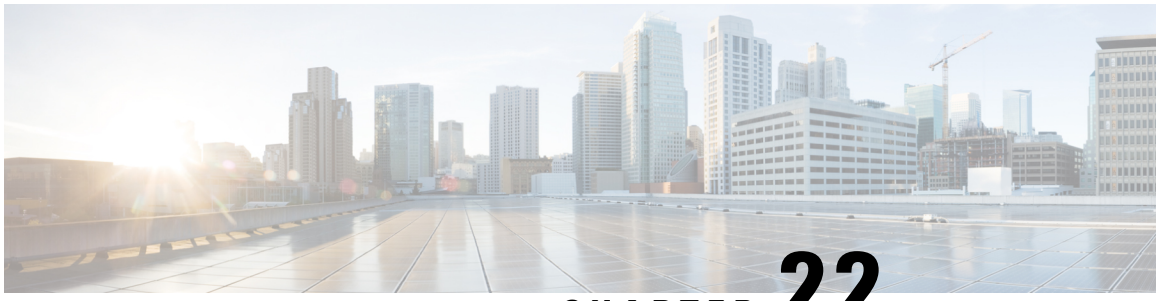
Revision History

Revision Details	Release
First Introduced.	2024.04.0 (21.28.m4)

Behavior Change

Previous Behavior: When Serving Gateway (SGW) Call Detail Records (CDR) were triggered from a 4-digit AAA manager with an instance number greater than 998, the nodeID field was updated with "1". This nodeID attribute was not in the expected ndddSTRING format and was encoded in a 3-digit decimal format. This format restricted the system to handle instance numbers in the range of 0 to 998 only. This behavior resulted in incorrect nodeID values as the system could not accommodate the larger instance numbers.

New Behavior: The nodeID attribute is encoded in a 3-digit hexadecimal format, extending support for instance numbers in the range of 0 to 4095. With this behavior, the system displays the accurate larger instance numbers in the nodeID field, ensuring accurate data recording and transfer across various functions.



CHAPTER 22

Encrypt AES-GCM Algorithm

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First Introduced	21.28

Feature Description

The P-GW (Packet Data Network Gateway) support IPsec and IKEv2 encryption using IPv4 and IPv6 addressing in LTE/SAE (Long-Term Evolution/System Architecture Evolution) networks.

IPsec and IKEv2 encryption enables network domain security for all IP packet switched networks, providing confidentiality, integrity, authentication, and anti replay protection through secure IPsec tunnels.

In StarOS 21.28.0 and later releases, URL redirection encryption mechanism is enhanced with an aes-gcm-256 encryption option:

The following preferences are supported for the AES-GCM Encryption Algorithm:

- AES Key size (Preferred 256)
- GCM IV length (Preferred 12)
- GCM Tag length (Preferred 16)
- MD (SHA384)

Note The aes-gcm-256 algorithms do not affect the function that supports multiple algorithms with different rulebase that is installed from PCRF at the same time.

Configuring aes-gcm-256 Encryption

The encryption mechanisms list is enhanced by additionally supporting AES-GCM.

```
configure
  active-charging service service_name  charging-action  charging_action_name
    billing action rf
   flow action redirect-url redirect_url encryption  aes-gcm-256  encrypted
 key key
    flow limit-for-bandwidth { { direction { downlink | uplink }
peak-data-rate bps peak-burst-size bytes violate-action  lower-ip-precedence

    pco-custom 1 3
    tft packet-filter tft-pmb
  exit
```

NOTES:

- **flow action redirect-url** *redirect_url* **encryption aes-gcm-256 encrypted key** *key* : Performs AES-GCM-256 encryption for redirect URL data.

Monitoring and Troubleshooting

This section provides information regarding monitoring and troubleshooting the AES-GCM Encryption Algorithm feature.

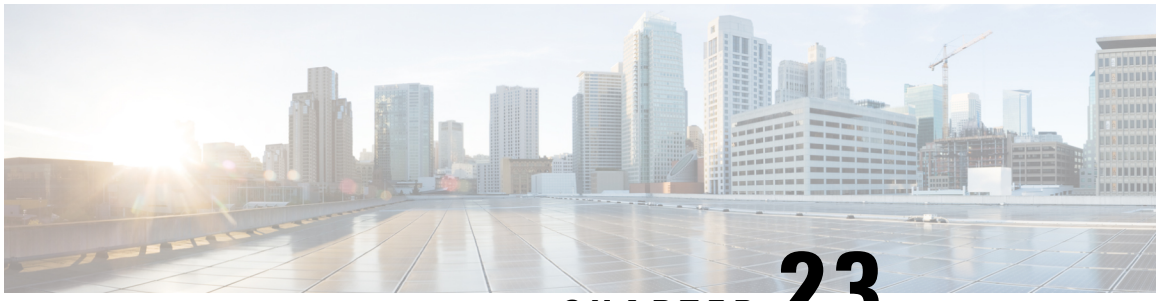
Show Commands and Outputs

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

show configuration active-charging service all | grep flow

The following example displays the flow action of the redirect URL performed for AES-GCM-256 encryption method.

```
[local]qvpc-si(config)# active-charging service acs
[local]qvpc-si(config-acs)# charging-action sa-redirect-pmb
[local]qvpc-si(config-charging-action)# billing-action rf
[local]qvpc-si(config-charging-action)# flow action redirect-url abc.com encryp
tion
encryption - Enable encryption for dynamic fields of redirect url
[local]qvpc-si(config-charging-action)# flow action redirect-url abc.com encryp
tion
aes-cbc-128 aes-cbc-256 aes-gcm-256 blowfish128 blowfish64
[local]qvpc-si(config-charging-action)# flow action redirect-url abc.com encryp
tion aes-gcm-256 encrypted key 7625e224dc0f0ec91ad28c1ee67b1eb96d1a5459533c5c95
0f44aae1e32f2da3
```



CHAPTER 23

EPS to 5Gs Mobility Procedure without n1 Mode Support

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
CLI configuration support is added for enabling the reject EPS to 5Gs procedure without n1 mode support.	2024.02.0

Revision Details	Release
Support is introduced for dynamic selection mechanism to select SGW-C+SMF through s11 interface.	21.28.m7
Support is introduced for dynamic selection mechanism to select PGW-C+SMF and peer-AMF.	21.25
The N26 interface for interworking with 5GS functionality is fully qualified in this release.	21.20.3
MME supports N26 interface between AMF in 5GC and MME in Evoloved Packet Core (EPC) to provide seamless session continuity for single registration mode UE. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.20
First introduced. This release supports N26 Interface for interworking with 5GS functionality. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.19

Feature Description

The MME accepts context requests from AMF regardless of the n1-mode support that UE indicates to EPS. This feature is enabled by default.

To reject context requests when the UE indicates that it does not support n1-mode, you can disable this feature by enabling the **reject-EPS-to-5GS-without-n1-mode** configuration.

Disabling EPS to 5G Mobility without n1 Mode

Use the following configuration to disable EPS to 5GS mobility without n1 mode support.

```
configure
  context context_name
    mme service  service_name
       [ no ] n1-mode 5gs-interworking-with-n26 [ sgw-selection |
reject-EPS-to-5GS-without-n1-mode ]
       end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* and must be a string of 1–63 characters.
- **n1-mode**: Configures interworking with 5Gs for UEs supporting N1 mode.
- **5gs-interworking-with-n26**: Enables 5GS-EPS interworking with N26 interface.

- **no**: Enables EPS to 5GS mobility without n1 mode support.
- **reject-EPS-to-5GS-without-n1-mode**: If this CLI is configured, MME enables rejection EPS to 5GS context request from AMF when the UE indicates N1 Mode is not supported.

Disabling EPS to 5Gs Mobility in Call Control Profile

Use the following configuration to disable EPS to 5GS mobility without n1 mode support in the Call Control Profile.

```
configure
   call-control-profile profile_name
       [ no | remove ] n1-mode 5gs-interworking-with-n26 sgw-selection
ue-usage-type | reject-EPS-to-5GS-without-n1-mode
    end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of a call control profile entered as an alphanumeric string of 1-64 characters.
- **n1-mode** : Configures interworking with 5GS for UEs supporting N1 mode.
- **5gs-interworking-with-n26** : Enables 5GS-EPS interworking with N26 interface.
- **no** : Disables the configuration..
- **remove**: Removes the configuration from the Call Control Profile and the MME service configuration applies.
- **reject-EPS-to-5GS-without-n1-mode**|: If this CLI is configured, MME enables rejection of EPS to 5GS context request from AMF when the UE indicates N1 Mode is not supported.

Monitoring and Troubleshooting

This section provides information regarding show commands and outputs available to monitor and troubleshoot the N26 Interface feature.

Show Commands and Outputs

show call-control-profile full name

The output of this command includes the **5GS-EPS interworking with N26 interface** field, which indicates if the 5GS-EPS interworking with N26 interface feature is enabled or disabled under N1 mode at call control profile.

show mme-service all

The output of this command includes the following fields:

- **5GS-EPS interworking with N26 interface**

- **Peer AMF GUAMI**
- **Peer AMF TAI**

show configuration verbose

Following are the sample configuration commands of **show configuration verbose** and **show configuration** CLI commands.

The **show configuration verbose** with reject-EPS-to-5Gs-without-n1-mode not configured in the MME service.

```
call-control-profile ccp1
    remove n1-mode 5gs-interworking-with-n26
  exit

  mme-service mme1
    no n1-mode 5gs-interworking-with-n26 reject-EPS-to-5GS-without-n1-mode
  exit
```

The **show config verbose** with **n1-mode 5gs-interworking-with-n26** and **reject-EPS-to-5GS-without-n1-mode** disabled.

```
show configuration verbose/show configuration
     call-control-profile ccp1
    n1-mode 5gs-interworking-with-n26
      no n1-mode 5gs-interworking-with-n26 reject-EPS-to-5GS-without-n1-mode

  #exit

  mme-service mme1
    n1-mode 5gs-interworking-with-n26
      no n1-mode 5gs-interworking-with-n26 reject-EPS-to-5GS-without-n1-mode
  #exit
```

The following is the sample configuration of **show configuration verbose** and **show configuration** commands where, n1-mode 5gs-interworking-with-n26, sgw-selection, and reject-EPS-to-5GS-without-n1-mode option is enabled.

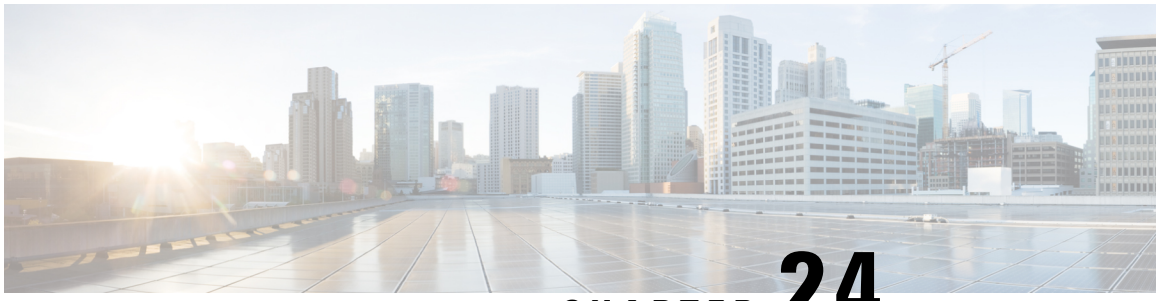
```
show configuration verbose/show configuration
  call-control-profile ccp1
    n1-mode 5gs-interworking-with-n26 sgw-selection s11
    n1-mode 5gs-interworking-with-n26 reject-EPS-to-5GS-without-n1-mode
  #exit

      mme-service mme1
    n1-mode 5gs-interworking-with-n26 sgw-selection s11
    n1-mode 5gs-interworking-with-n26 reject-EPS-to-5GS-without-n1-mode
   #exit
```

The following is the sample configuration of **show configuration verbose** and **show configuration** commands where, n1-mode 5gs-interworking-with-n26, reject-EPS-to-5GS-without-n1-mode is enabled and sgw-selection is not configured.

```
show configuration verbose/show configuration
  call-control-profile ccp1
       n1-mode 5gs-interworking-with-n26 reject-EPS-to-5GS-without-n1-mode
  #exit

      mme-service mme1
       n1-mode 5gs-interworking-with-n26 reject-EPS-to-5GS-without-n1-mode
        #exit
```



CHAPTER 24

ePDG Support on VPC-SI and VPC-DI

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	VPC-SI VPC-DI
Feature Default	Disabled – License required to enable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable.

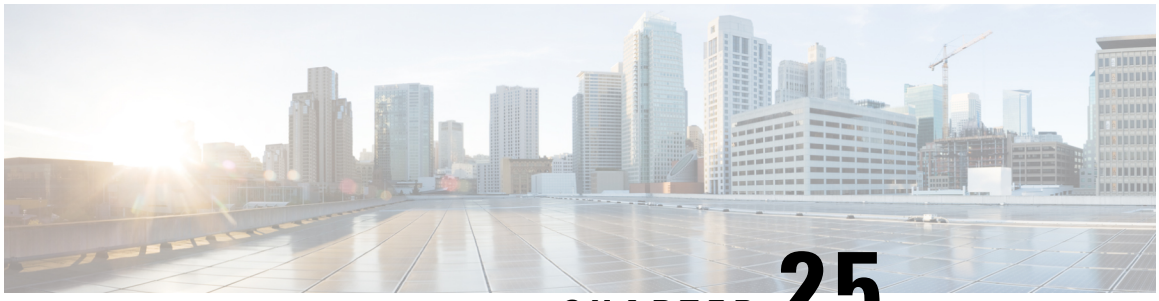
Revision History

Revision Details	Release
ePDG supports Red Hat OpenStack Platform (RHOSP) 17.1 version.	2024.04.0
First introduced.	21.4

Feature Description

ePDG is supported on the VPC-SI platform with CVIM 4.4.

ePDG is also supported on the VPC-DI platform with CVIM 5.0 and OSP 17.1 version. For more information, see the *Cisco UCS C220 M6 Server* section in the *VPC-DI System Administration Guide.*



CHAPTER 25

Fetching the Target eNB based on the Target en-gNB ID without TAC

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Enabled - Always-On
Related Changes in This Release	Not Applicable
Related Documentation	*MME Administrartion Guide*

Revision History

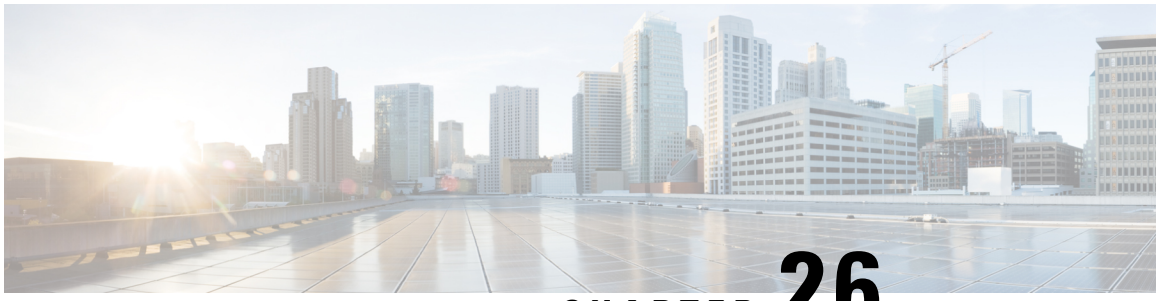
Revision Details	Release
MME supports fetching target eNodeB based on the en-gNB-ID without TAC. For more information, see the *MME Support for EN-DC SON Configuration Transfer IE on S1-AP* chapter in the *MME Administration Guide*.	• 2024.2.0 • 21.28.m5

Feature Description

In some scenarios, when the UE moves to a coverage of en-gNB, which is not added as secondary node to the eNodeB, but the UE is presently connected to eNodeB uses ANR procedures to add en-gNB as secondary

node and send the ENB CONFIGURATION TRANSFER message to the MME. Currently eNodeB may not send the right Tracking Area Update (TAC) in the selected TAI of target en-gNB. This mapping of eNodeB to en-gNB id with PLMN and TAC in MME could result in secondary node addition failure.

To overcome this scenario, MME supports seamless mobility between two gNBs connected with eNodeBs in the same or different TACs. MME maps eNodeB to en-gNB ID plus bPLMN received in the S1 setup and eNodeB Configuration Update requests. Thus the en-gNB ID and PLMN key fetch target eNodeB connected to target en-gNB ID seamlessly. If a multiple target eNodeB ID matches, the first available eNodeB with the association state in MME as **UP** is selected.



CHAPTER 26

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

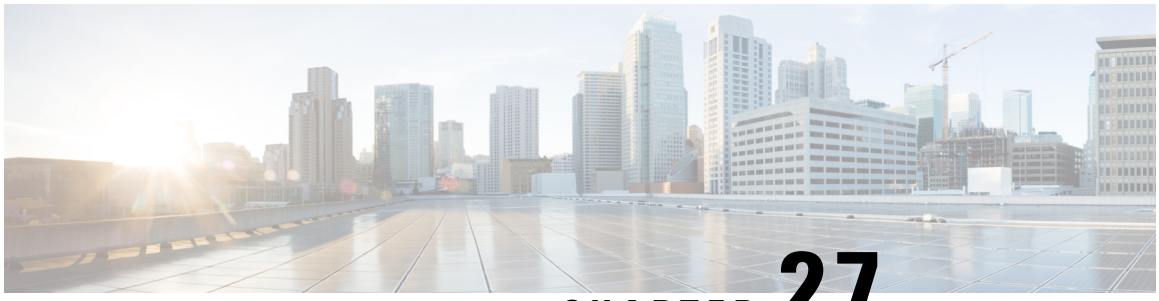
Revision Details	Release
P-GW supports handling of CC-Request-Number AVP during Assume Positive state.	• 21.28.m7 • 21.26.h5
First Introduced.	21.26.19

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 successful 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 27

Handling Simultaneous Gy RARs from Different DRAs with Different RGs

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Command Line Interface Reference*

Revision History

Revision Details	Release
Enhancement of Gy interface on P-GW to handle multiple DRA.	21.28

Feature Description

In P-GW, if there are Multiple Diameter Routing Agents (DRA) and if P-GW receives simultaneously more than one Reauthorization Request (RAR) each with different rating-group (RG) from different DRAs than from the last diameter request, P-GW aborts the previous transaction (the one with the Credit Control Request –Update message, which is pending from a previous RAR) and re-uses the same cc-request-number for next Credit Control Request –Update message (CCR-U) (binding toward new peer).

This resulted in quota not getting applied to RG received through previous RARs. Hence, traffic does not get forwarded for that rating group or service-id wRAs.

In StarOS 21.28 and later releases, P-GW accepts both RGs from different peer by using a configurable CLI command **diameter pending-ccau allow-on-rar-peer-switch** under the ACS configuration mode. That is, this CLI allows you to configure the DCCA client to prevent the aborting of a pending CCRU request received in case of RAR, which is received from a different host or peer on the Gy interface.

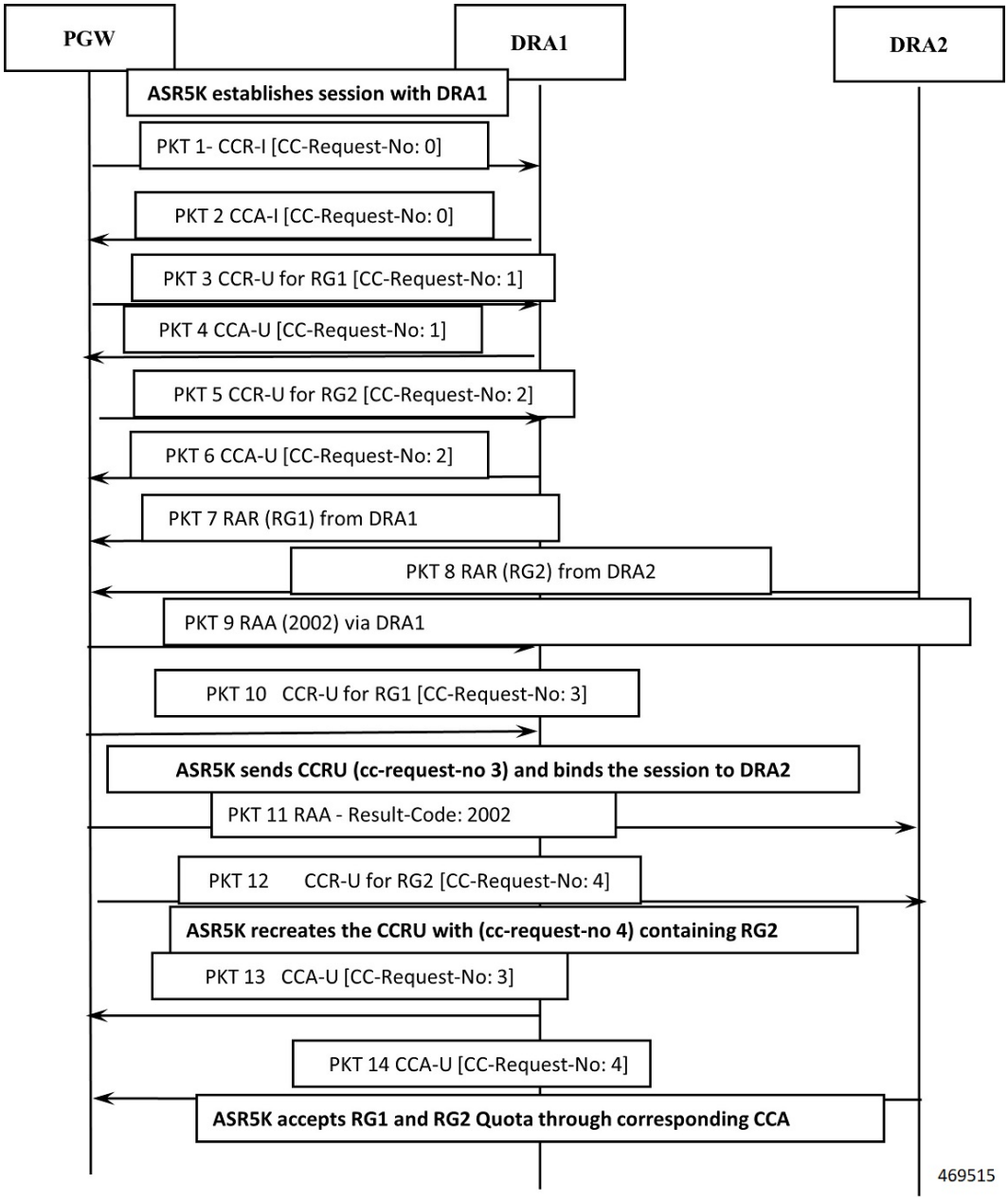
How it Works

There is a change in the handling of aborting the previous pending requests. Currently, When a DCCA client is in pending state, upon receiving RAR through a different peer, the DCCA client aborts the diameter message (at ACS manager level). Due to the enhancement of the Gy interface on P-GW to handle multiple DRA features, P-GW now avoids this aborting of previous pending requests and accepts both RGs from a different peer.

After receiving a new RAR either from a new peer or host, P-GW updates the session to a new peer or host. Then checks for any pending state of Multiple Service Credit Control (MSCC) and avoids the subsequent action of aborting of pending CCRU requests.

The following call flow and procedure describes how P-GW accepts both RGs from different peer.

Figure 13: Call Flow



Configuring Multiple DRA over Gy Interface

Use the following configuration commands to configure different DRAs.

```
configure
     context context_name
     active-charging service acs_service_name>
```

```
credit-control [ group cc_group_name ]
     diameter dictionary dictionary
    [ no ] diameter pending-ccau allow-on-rar-peer-switch
exit
```

NOTES:

- **diameter dictionary** *dictionary*: Set the diameter dictionary to handle different DRAs. For example, **diameter dictionary** *dcca-custom-26*
- **diameter pending-ccau allow-on-rar-peer-switch** : Allows DCCA client to prevent the abort of pending CCAU request in case of RAR being received from different host/peer on the Gy interface.
- **[no] diameter pending-ccau allow-on-rar-peer-switch** : Disables the DCCA client from preventing the abort of pending CCAU requests.

Monitoring and Troubleshooting

This section provides information regarding monitoring and troubleshooting of multiple DRA messages on the Gy interface.

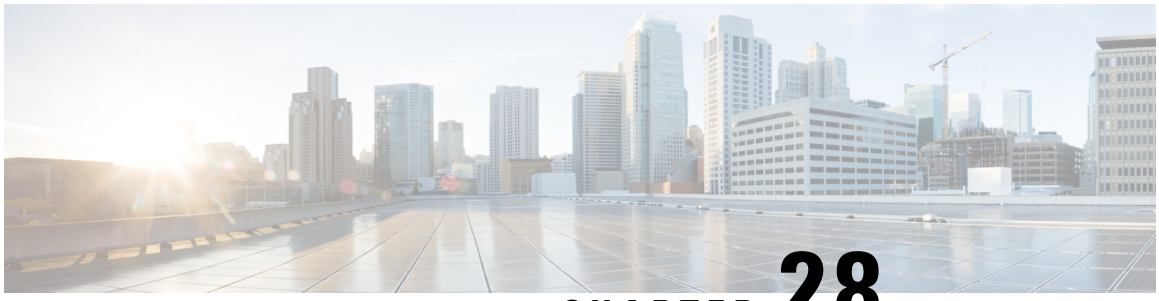
Show Commands and Outputs

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

show active-charging service all

Table 3: show active-charging service all

Field	Description
pending ccau:	
allow-on-rar-peer-switch	Displays whether abort of pending CCAU request in case of RAR being received from different host/peer on Gy interface is enabled or disabled. If this feature is enabled the functionality is applicable only to new diameter sessions.



CHAPTER 28

Handling Duplicate eNodeB Path

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In MME, handling of Duplicate eNodeB Path support is introduced.	21.28.m0

Feature Changes

Previous Behavior: When a duplicate eNodeB path is detected, **mmedemux** retains the old stale path and deletes the new path.

New Behavior: Enable the **delete-old-on-duplicate-enodeb-detection** CLI under mme-service to control the duplicate eNodeB path. When a duplicate eNodeB path is detected, **mmedemux** deletes the old stale path, and allows the new path to get established.

Note The **delete-old-on-duplicate-enodeb-detection** CLI is a critical parameter, which will restart the mme service and remove active sessions.

Command Changes

Use the following commands to configure the MME to delete an old eNodeB path and retain a new eNodeB path while detecting duplicate eNodeB id.

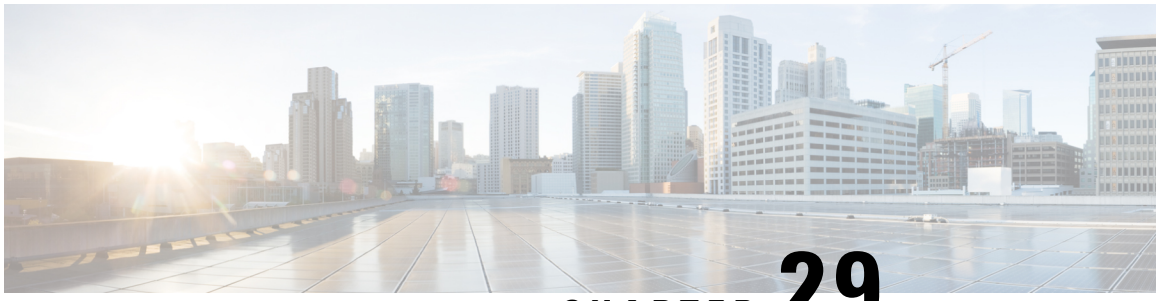
```
configure
  context context_name
      mme-service service_name
      [ no ] delete-old-on-duplicate-enodeb-detection
      exit
    exit
```

NOTES:

- **delete-old-on-duplicate-enodeb-detection**: The **mmedemux** deletes the old stale path and establishes a new path. By default it is disabled.

Note The **delete-old-on-duplicate-enodeb-detection** CLI is a critical parameter, which will restart the mme service and remove active sessions.

- **no**: The **mmedemux** retains the old eNodeB path.



CHAPTER 29

IKEV2 VRF Support

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	• 21.28.m6

Feature Description

In StarOS, without the IKEv2 VRF feature, only IPSec IKEv1 tunnels were VRF-aware, and where IKEv1 tunnels encrypted traffic originating from any VRF. Whereas the IPSec IKEv2 tunnels establish and encrypt

traffic only on default VRF. IKEv2 VRF feature supports IPSec IKEv2 tunnel establishment and traffic encryption on any VRF.

How it works

To support VRF for IKEv2 in the ASR5500 and VPC-DI environment, the decrypted packet needs to be processed in the right VRF so that it doesn't get discarded. The following function happens:

- The ACL gets hit for control and trigger packets for the first time.
- Sends packets to the IPSec and creates a tunnel.
- Starts the exchange of keys and a key pair establishes the tunnel.
- After the tunnel is established, that particular ipsecmgr flow DB entry gets deleted and creates a new entry. This ensures that the next packet passes to the crypto engine and gets forwarded. This is common to IPv4 and IPv6.

.

Limitations

Following are the limitations:

- The Key exchange and tunnel establishment occurs in the Default-VRF and not in the VRF whose traffic needs to be encrypted.
- The maximum number of IPSec ACLs per crypto map is seven. To support multiple IP chunks in an APN, multiple access-lists need to be configured. This might lead to multiple IPSec tunnels per enterprise VRF.
- Reconfiguring ACL rules that are corresponding to a crypto map requires reestablishment of the existing tunnels. This operation is disruptive for Uplink and Downlink subscriber traffics.

Configuring IKEv2 IPSec with VRF

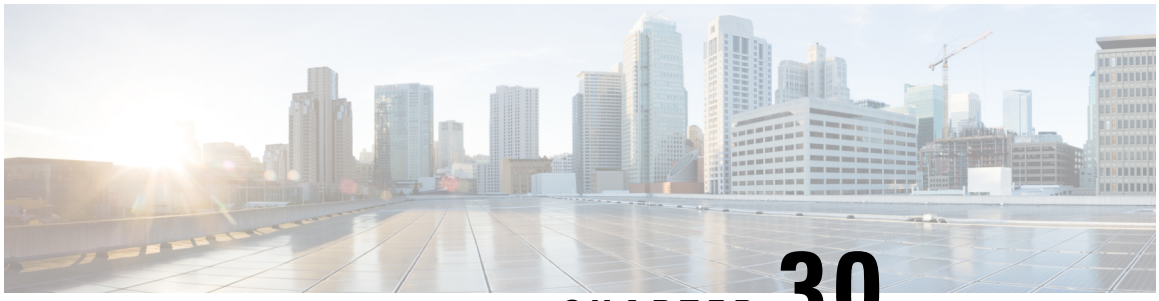
Use the following sample configuration commands to configure IKEv2 IPSec with VRF. The following sample configuration shows how the loopback IP overlaps in the enterprise VRF and the Default-VRF to allow the exchange of keys from the Default-VRF but also allow crypto map to be applied in a VRF interface in the same time.

```
context ipsec-s
    ip vrf i-s
    #exit
    ip access-list boo
      permit ip host 2.1.1.1 host 2.2.1.1
    #exit
    crypto ipsec transform-set A-foo esp hmac sha1-96 cipher aes-cbc-128
      mode tunnel
    #exit
    ipsec transform-set B-foo
      hmac sha2-256-128
```

```
      group 14
    #exit
    ikev1 policy 1
    #exit
    ikev2-ikesa transform-set ikesa-foo
      group 14
      hmac sha2-256-128
      prf sha2-256
    #exit
    crypto map foo ikev2-ipv4
      match address boo
      authentication local pre-shared-key encrypted key
+B0bqvzhrkkwujr2kt37b0yxo4631silym4g2zn9r2rs0o7xrn3r4i09aexdk701t8d0cqt2ivg039da1267r6tcurpyk3qhdjbfwo7t6s

      authentication remote pre-shared-key encrypted key
+B0975tvzeoi0lg2zl78a17mnhv20yw3cesh97zi436qvsyoadulmh2pbgcnndjxchq0c3fn5p2i3y7b12uqc4bwsmi5x324ikw0wfzus8

      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa rekey
      payload foo-sa0 match ipv4
        ipsec transform-set list B-foo
        rekey keepalive
      #exit
      peer 5.2.1.1
    #exit
    interface ike
      ip address 192.168.110.120 255.255.255.0
    #exit
    interface iv1 loopback
      ip vrf forwarding i-s
      ip address 2.1.1.1 255.255.255.255
    #exit
    interface iv2 loopback
      ip vrf forwarding i-s
      ip address 5.1.1.1 255.255.255.255
      crypto-map foo
    #exit
    interface iv3 loopback
      ip address 5.1.1.1 255.255.255.255
    #exit
    subscriber default
    exit
    aaa group default
    #exit
    gtpp limit-secondary-rat-usage 32
    ip route 5.2.1.1 255.255.255.255 192.168.110.89 ike
  #exit
  port ethernet 1/10
    no shutdown
    vlan 110
      no shutdown
      bind interface ike ipsec-s
    #exit
  #exit
```



CHAPTER 30

IMSI Privacy on ePDG

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	VPC-DI
Feature Default	Disabled – Configuration Required
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	**Release**

In this StarOS release, ePDG is enhanced to perform AUTH calculation based on the 'anonymous' or any other configured parameter received in the IDi payload. The existing support of performing AUTH calculation based on International Mobile Subscriber Identity (IMSI) shall be provided through the **imsi-privacy auth-imsi** CLI command.	2024.03.0
First introduced.	21.4

IMSI Privacy

The IMSI Privacy feature protects the exposure of IMSI to the untrusted ePDG and shares it over the wire only after the User Equipment (UE) has authenticated the ePDG.

By default, ePDG uses Peer IDi such as 'anonymous' or any other configured parameter for AUTH calculation instead of IMSI.

Limitation

The IMSI Privacy feature is not applicable for non-UICC (universal integrated circuit card) devices.

AUTH Calculation for IMSI Privacy

When the User Equipment (UE) sends an IKE-AUTH request to the evolved Packet Data Gateway (ePDG), the IKE-AUTH message includes the IDi payload. The ePDG decodes the IDi payload and compares it with the configured string in the ePDG to determine if the call flow is using IMSI privacy. If it is an IMSI privacy-based call flow, the ePDG then checks if auth-imsi is configured. The ePDG supports authentication (AUTH) calculation using two approaches:

- If auth-imsi is configured, authentication calculation will be based on the IMSI.
- If auth-imsi is not configured, authentication calculation will be based on the configured string.

How it Works

The following steps describe authenticaton process for IMSI-based AUTH Calculation.

Table 4: Procedure

Step	Description
1.	The UE sends IKE_SA_INIT Message.
2.	ePDG responds with IKE_SA_INIT_RSP Message.

Step	Description
3.	The UE sends the anonymous or configured value (in the IDi payload), APN (in the IDr payload), and CERTREQ information in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain an IPv4 home IP Address and/or a Home Agent Address.
4.	ePDG decodes and processes the string anonymous or any configured value received in IDi payload in the IKE_AUTH request. In addition to the ePDG server certificate, the IKEv2 server initiates an EAP Identity request towards the IKEv2 client.
5	The IKEv2 client (UE) authenticates the server using the certificate and provides the IMSI in the EAP Identity response.
6	The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN.
7.	The 3GPP AAA Server shall fetch 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 lookup 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.
8.	The ePDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it 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 in order to start the EAP procedure over IKEv2.
9.	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.
10	The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server.
10a	The AAA checks, if the authentication response is correct.

Step	Description
11.	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 shall consist of the MSK generated during the authentication process. When the SWm and SWd interfaces between ePDG and 3GPP AAA Server are implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key-AVP, as defined in RFC 4072.
12.	The MSK shall be used by the ePDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified for IKEv2 in RFC 4306. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 4306 [3], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.
13.	The EAP Success/Failure message is forwarded to the UE over IKEv2.
14	The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.
15	The ePDG checks the correctness of the AUTH parameter calculated based on: • IMSI - if **auth-imsi** is configured • amonymous or configured value - if **auth-imsi** is not configured
16	On successful authentication the ePDG selects the P-GW 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 shall be 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.
17.	The P-GW allocates the requested IP address 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.
18.	The ePDG calculates the AUTH parameter calculated based on IDr payload, which authenticates the second IKE_SA_INIT message.

Step	Description
19.	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 terminates.
20.	Router Advertisement will be sent for IPv6 address assignments, based on configuration. **Note** If the ePDG detects that an old IKE SA for that APN already exists, it will delete the IKE SA and send the UE an INFORMATIONAL exchange with a Delete payload in order to delete the old IKE SA in UE.

Configuring IMSI Privacy and AUTH Calculations

This section describes the configuration of IMSI Privacy and if Auth calculation is done based on the IMSI or 'anonymous' or configured value received in the IDi payload.

Configure IDi

You can use this task to match IDi from peer, which enables the ePDG to request the real identity using EAP-Identity Request.

Procedure

Step 1 Specify a crypto template name to identify the Crypto template and IKEv2 Security Association parameter that are derived from this Crypto template.

crypto template *template_name* **ikev2-dynamic**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa idi anonymous1@realm.com
request-eap-identity
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 2 Specify the IDi value to match IDi from peer and request for EAP-Identity from peer. The *peer_idi_value* must be of size 1–127.

ikev2-ikesa idi *peer_idi_value* **request-eap-identity**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa idi anonymous1@realm.com
```

```
request-eap-identity
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 3 (Optional) Disable the peer IDi value.

no ikev2-ikesa idi *peer_idi_value*

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# no  ikev2-ikesa idi anonymous1@realm.com
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Enable Use of IMSI for AUTH Calculation

Use this task to enable ePDG to use IMSI for AUTH calculation on the Context Configuration mode when the IMSI Privacy feature is used.

Also, verify whether the IMSI based AUTH calculation is enabled on the ePDG using the .**show configuration** and **show crypto template** coomands.

Procedure

Step 1 Specify a crypto template name to identify the Crypto template and IKEv2 Security Association parameter that are derived from this Crypto template.

crypto template *template_name* **ikev2-dynamic**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
[
```

Step 2 Enable ePDG to use IMSI for AUTH calculation with IMSI Privacy related parameters.

ikev2-ikesa imsi-privacy auth-imsi

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 3 Verify whether the IMSI based AUTH calculation is enabled on the ePDG.

a) Use the **show configuration** command to verify if the IMSI Privacy AUTH calculation enabled with auth-imsi.

Example:

```
show configuration
crypto template boston ikev2-dynamic
authentication remote eap-profile eapl
ikev2-ikesa transform-set list ikesa-boston  ikev2-ikesa rekey
   payload foo-saO match childsa match any
    ipsec transform-set list tselsa-boston
    rekey keepalive
   #exit
    ikev2-ikesa policy error-notification.
    ikev2-ikesa imsi-privacy auth-imsi
    iKev2-iKesa Keepaiive-user-activity
    allow-custom-fqdn-idr
 #exit
```

b) Use the **show crypto template** command to verify if a certain crypto template has the IMSI or IMSI Privacy string configured for AUTH calculation and if the IKE SA IDi value is defined.

Example:

```
[local]EPDGCHASSIS# context pdif
[pdif]EPDGCHASSIS# show crypto template
Map Name: boston
Map status: Incomplete
Crypto Map Type: IPSEC IKEv2 Template
IKE SA Transform 1/1
  Transform Set: ikesa-boston
    Encryption Cipher: aes-cbc-128 Encryption Accel: AES-NI Pseudo Random Function: shal
    Hashed Message Authentication Code: shal—96 HMAC Accel: None Diffie-Hellman Group: 2 IKE SA
Rekey:
Enabled
IKE SA User Activity Keepalive: Enabled IKE SA Setup Timer: 120 [Default]
IKE SA Backoff Timer per Notify Msg Type:
   No APN Subscription: 3600 sec [Default]
   Network Failure : 3600 sec [Default]
IKE SA Max Retransmission Count : 5 [Default]
IKE SA Max Retransmission Timeout: 500 [Default] IKE SA Ignore Rekeying request: Disabled IKE SA
 Cert Sign: PKCS 1.5 [Default]
IKE SA Use CDP: Disabled IKE SA Mobike: Disabled
IKE SA RFC5996 Notification: Disabled
IKE SA Ignore Notify Protocol ID: None [Default]
IKE SA DSCP Value: 0x0 [Default]
IKE SA IDi [Peer]: Disabled
imsi-privacy used Id for AUTH calculation : imsi
```

You have successfully configured IMSI based AUTH calculation under the Crypto template configuration mode.

Disable Use of IMSI for AUTH Calculation

Use this task to revert to the default behavior of IKESA using the configured IDi parameters, which is used for AUTH calculation when IMSI Privacy feature is used.

View the IMSI Privacy AUTH calculation disabled using the **show configuration** and **show crypto template** commands.

Procedure

Step 1 Specify a crypto template name to identify the Crypto template and IKEv2 Security Association parameter that are derived from this Crypto template.

crypto template *template_name* **ikev2-dynamic**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)#  context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# no ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 2 Disable IMSI based AUTH calculation.

no ikev2-ikesa imsi-privacy auth-imsi

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)#  context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# no ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 3 Verify whether the IMSI based AUTH calculation is disabled on the ePDG using **show configuration** and **show crypto template** CLI commands.

a) Using **show configuration** command:

Example:

```
crypto template boston ikev2-dynamic
authentication remote eap-profile eapl ikev2-ikesa transform-set list ikesa-boston ikev2-ikesa
rekey
payload foo-saO match childsa match any
ipsec transform-set list tselsa-boston     reley keepalive
#exit
ikev2-ikesa policy error-notification
ikev2-ikesa keepalive-nspr-activity
ikev2-ikesa idi anonymousl@realm.com request-eap-identity allow-custom-tqdn-idr
#exit
```

b) Using **show crypto template** command:

Example:

```
[pdif]EPDGCHASSIS# show crypto template
Map Name: boston
Map status: Incomplete
Crypto Map Type: IPSEC IKEv2 Template
IKE SA Transform 1/1
Transform Set: ikesa-boston
 Encryption Cipher: aes-cbc-128
 Encryption Accel: AES-NI
 Pseudo Random Function: shal
 Hashed Message Authentication Code: shal-96
 HMAC Accel: None
```

```
 Diffie—Heilman Group: 2 IKE SA Rekey: Enabled
IKE SA User Activity Keepalive: Enabled
IKE SA Setup Timer: 120 [Default]
IKE SA Backoff Timer per Notify Msg Type:
  No APN Subscription: 3600 sec [Default]
  Network Failure : 3600 sec [Default]
IKE SA Max Retransmission Count: 5 [Default]
IKE SA Max Retransmission Timeout: 500 [Default] IKE SA Ignore Rekeying request: Disabled IKE SA
 Cert Sign: PKCS 1.5 [Default]
IKE SA Use CDP: Disabled
IKE SA Mobike: Disabled
IKE SA RFC5996 Notification: Disabled
IKE SA Ignore Notify Protocol ID: None [Default]
IKE SA DSCP Value: 0x0 [Default]
IKE SA IDi [Peer]:
  anonymousl@realm.com [Request EAP-Identity]
imsi-privacy used Id for AUTH calculation: configured-string
```

You have successfully disabled IMSI based AUTH calculation.

Monitoring and Troubleshooting

Show Commands and Outputs

This section provides information on show commands and their corresponding outputs for the IMSI Privacy Support feature.

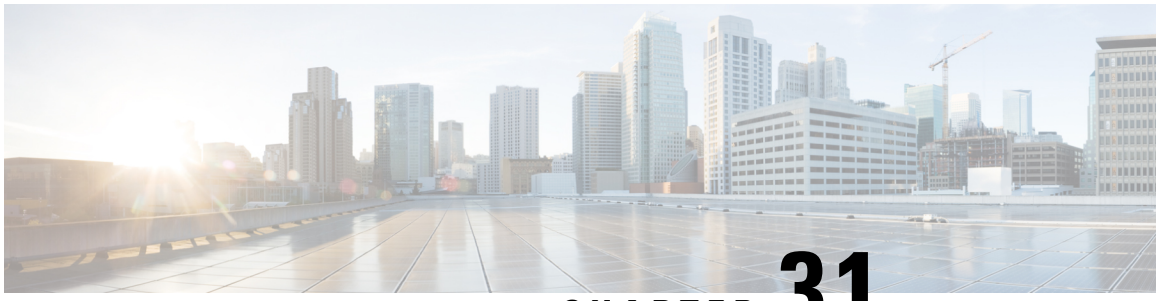
show crypto statistics ikev2

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

- EAP-Identity Req Sent

  It will increment once EAP-Identity request is sent to peer after receiving the configured IDi.
- EAP-Identity Rsp Rcvd

  It will increment when any of the configured IDi is received from peer.



CHAPTER 31

Increasing CPU threshold from 30 to 70

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	StarOs
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

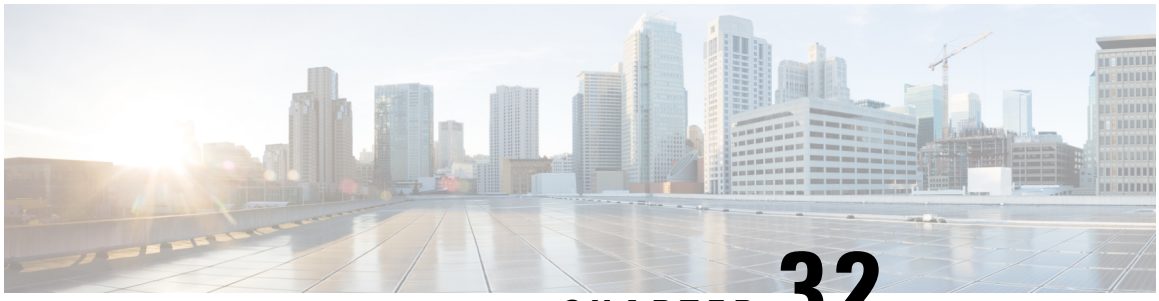
Revision Details	Release
The CPU threshold limit has been increased from 30 to 70.	21.28.M0

Feature Changes

Previous Behavior: For CPU usage, the threshold limit was 30.

New Behavior: There has been an increase in the CPU threshold limit from 30 to 70.

Impact on the Customer : Through the CLI, the customer has now set a higher CPU threshold value.



CHAPTER 32

Handling 5G to 4G TAU when n1-mode is not Supported

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
MME supports Tracking Area Update (TAU) with N1 Mode = Not supported.	21.28.m5
Support is introduced for a dynamic selection mechanism to select PGW-C+SMF and peer-AMF.	21.25
The N26 interface for interworking with 5GS functionality is fully qualified in this release.	21.20.3

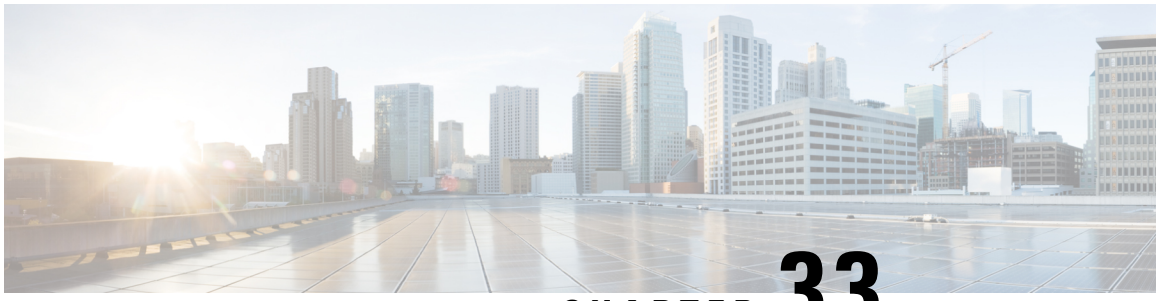
Revision Details	Release
MME supports N26 interface between AMF in 5GC and MME in Evoloved Packet Core (EPC) to provide seamless session continuity for single registration mode UE. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.20
First introduced. This release supports N26 Interface for interworking with 5GS functionality. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.19

Feature Description

During a 5G Standalone (SA) operation to 4G network, if the MME uses N1 Mode flag to decide N26 (AMF->MME) or S10 (MME->MME), it might lead to a Tracking Area Update (TAU) failure and the device can lose its data session.

To overcome such scenarios, MME supports TAU with **N1 Mode = Not supported**. MME considers AMF as peer if N1-Mode-Reg bit is set to **5GMM-REGISTERED** in the **UE Status IE**.

For more information, see the Use case section in the *5GS Interworking using N26 Interface Support* chapter in the *MME Administration Guide*.



CHAPTER 33

IP Source Violation

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* • *Command Line Interface Reference*

Revision History

Revision Details	Release
First introduced.	21.28

Feature Description

The P-GW supports packet source validation on the control-Plane. Configuration from Control Plane gets pushed to User Plane and based on that information, User Plane acts on the source violated packet.

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network. Source validation requires the source address of received packets to match the IP address that is assigned to the subscriber either statically or dynamically during the session.

In the StarOS 21.28.0 and later releases the **ip source-violation** command, which is part of the APN configuration mode is used to track the behavior of IP source violation for IPv4 and IPv6 addresses.

Configuring IP Source Violation

Use the following configuration to enable or disable packet source validation for a given APN:

```
configure
   context context_name
      apn apn_name
         ip source-violation { ignore | check [ drop-limit limit ] [
exclude-from-accounting ][ drop-count-timeout time-interval ] }[
traffic-type { ipv4 | ipv6 } ]
         default ip source-violation
         end
```

NOTES:

- **default**: Enables the checking of source addresses received from subscribers for violations, with a drop limit of 10 invalid packets that can be received from a subscriber prior to their session being deleted.
- **ignore**: Disables source address checking for the APN.
- **check [drop-limit** *limit* **]**: Default: Enabled, limit = 10.

  Enables the checking of source addresses received from subscribers for violations. A drop-limit can be configured to set a limit on the number of invalid packets that can be received from a subscriber prior to their session being deleted.

  limit: can be configured to any integer value between 0 and 10000. A value of 0 indicates that all invalid packets will be discarded, but the session will never be deleted by the system.
- **exclude-from-accounting**: Excludes the packets identified with IP source violation from the statistics generated for accounting records.
- **check [drop-count-timeout time-interval]**: The **drop-count-timeout** is used to configure the time interval for violation drop count update timer. This specifies in which time interval drop counter value should be updated. Time interval should be specified in minutes. Default value is 120 seconds (2 minutes).
- **check [traffic-type { ipv4 | ipv6 }]**: Specifies the packet traffic type as IPv4 or ipv6. By default configurations will be common for both IPv4 and IPv6. If CLI is configured with a "traffic-type" then "ip source violation" cli for that traffic-type takes priority than the CLI configured w/o "traffic-type".

Note The violation count increments even if the drop limit and timer values are zero. The session is not deleted, but the violated packets gets dropped.

Monitoring and Troubleshooting

This section provides information regarding monitoring and troubleshooting the IP Source Violation feature.

Show Commands and Outputs

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

show subscribers full all

Display all statistics that are related to the IPv4 and IPv6 counter violations separately.

Table 5: show subscribers full all Command Output Descriptions

Field	Description
ipv6 source violations	The number of IPv6 source validation violations.
ipv6 source violations no acct	The IPv6 source validation violations that were detected but not included in the statistics.
ipv6 source violations ignored	The IPv6 source validation violations that were detected but then ignored.
ipv6 source violations active	The total number of active IPv6 source validation violations.

show apn name *apn_name*

Display all statistics that are related to the IPv4 and IPv6 counter violations separately.

Table 6: show apn name apn_name Command Output Descriptions

Field	Description
ipv4 source violations	The number of IPv4 source validation violations.
drop limit	The number of drop limits for IPv4 source validation violations.
ipv4 source violations no acct	The IPv4 source validation violations that were detected but not included in the statistics.
ipv6 source violations	The number of IPv6 source validation violations.
drop limi	The number of drop limits for IPv6 source validation violations.

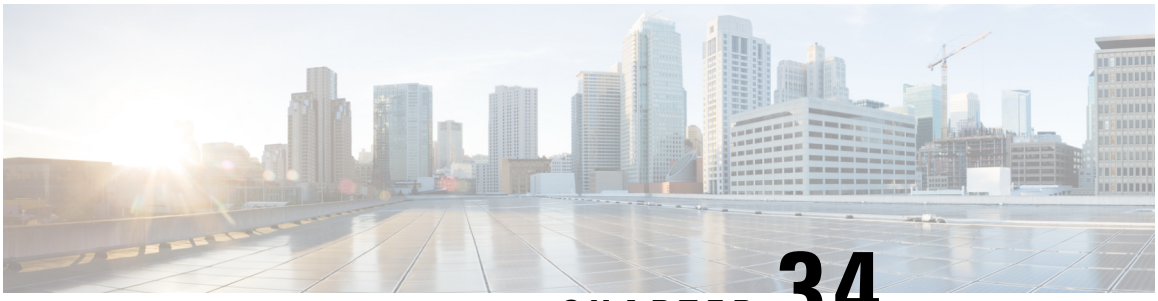
Field	Description
ipv6 source violations no acct	The IPv6 source validation violations that were detected but not included in the statistics.

show apn statistics name *apn_name*

Display all statistics that are related to the IPv4 and IPv6 counter violations separately.

Table 7: show apn statistics name apn_name Command Output Descriptions

Field	Description
IPv4 src violations	The number of IPv4 source validation violations.
IPv4 src violations no acct	The IPv4 source validation violations that were detected but not included in the statistics.
IPv4 src violations ignored	The IPv4 source validation violations that were detected but then ignored.
ipv6 src violations	The number of IPv6 source validation violations.
ipv6 src violations no acct	The IPv6 source validation violations that were detected but not included in the statistics.
IPv6 src violations ignored	The IPv6 source validation violations that were detected but then ignored.



CHAPTER 34

IPv4 and IPV6 Notification Support for IP Address Alignment

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The IPv4 and IPv6 Notification for IP Address Alignment feature is enhanced with CLI and Bulk Statistic counters	21.28.mx

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.

When a UE requests for both IPv4 and IPv6 addresses, the ePDG provides only one type of address to the UE based on the configured PDN Type in the P-GW and network preference. To indicate this, the ePDG sends a notification to the UE, either PDN_TYPE_IPv6_ONLY_ALLOWED or PDN_TYPE_IPv4_ONLY_ALLOWED, instructing it to use only the type of address as per the network preference. It is expected that the UE, upon receiving this notification, requests for the type of address it has received earlier during subsequent roaming.

The table below details the IPv4 and IPv6 notification alignment.

Table 8: IPv4 and IPv6 Notification for Alignment

S.No.	UE IKE CFG request to ePDG	ePDG CS request to P-GW	P-GW CS Response (based on PDN type)	ePDG Response in IKE CFG_REPLY
1	Both IPv4 and IPv6	Both IPv4 and IPv6	IPv4	IPv4 address sent and IPv4 only private notification sent.
2	Both IPv4 and IPv6	Both IPv4 and IPv6	IPv6	IPv6 address sent and IPv6 only private notification sent.

Through CLI configurations and Bulk Statistic counters, ePDG supports enabling and disabling of sending the PDN type notification to the UE associated with the subscriber.

Configuration to Enable or Disable IPv4 and IPv6 Notification

Use the following configuration to enable or disable the support of sending the PDN type notification to the UE that is associated with the subscriber. By default this feature is disabled.

To enable or disable:

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
       [ no ] notify-payload pdn-type-allowed
    end
```

NOTES:

- **notify-payload pdn-type-allowed**: Enables sending of PDN type notification in Notify Payload.
- **[no] notify-payload pdn-type-allowed**: Disables sending of PDN type notification in Notify Payload.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show crypto template tag

The following output displays the enabled PDN type notification for a subscriber.

```
[pdif]ePDG# show crypto template tag boston
|
|
   IKEv2 Notify Payload:
    Device Identity: Enabled[Default]
    PDN Type Allowed: Enabled
|
|
[pdif]ePDG#
```

show configuration

The following output displays the enabled PDN type notification for a subscriber.

```
pdif]ePDG# show configuration
|
|
    crypto template boston ikev2-dynamic
      authentication remote eap-profile eap1 second-phase eap-profile eap1
      ikev2-ikesa transform-set list ikesa-boston
      ikev2-ikesa rekey
      payload 1 match childsa match any
        ip-address-alloc static
        ipsec transform-set list tselsa-boston
        rekey keepalive
      #exit
      natt
      ikev2-ikesa policy error-notification
      notify-payload pdn-type-allowed
    #exit
|
|
End
```

clear epdg-service statistics

The **clear epdg-service statistics** command clears all the crypto ikev2 statistics.

show crypto statistics ikev2

After clearing, all the counters of IKEv2 statistics will be set to 0. The following is the sample show output after clear command.

```
[pdif]ePDG# show crypto statistics ikev2
…
…
…
Total IKEv2 Notify Statistics:
    COOKIE Notify Sent:                0 COOKIE Notify Rcvd:          0
    COOKIE Notify Match:               0 COOKIE Notify No Match:      0
    Multi Auth Supported:              0 Another Auth Follows:        0
    Device ID Req Sent:                0 Device ID Rsp Rcvd:          0
    Temporary Failure Retries:         0 PDN Type IPv4 Sent:          1
    PDN Type IPv6 Sent:                0
…
…
…
```

Bulk Statistics

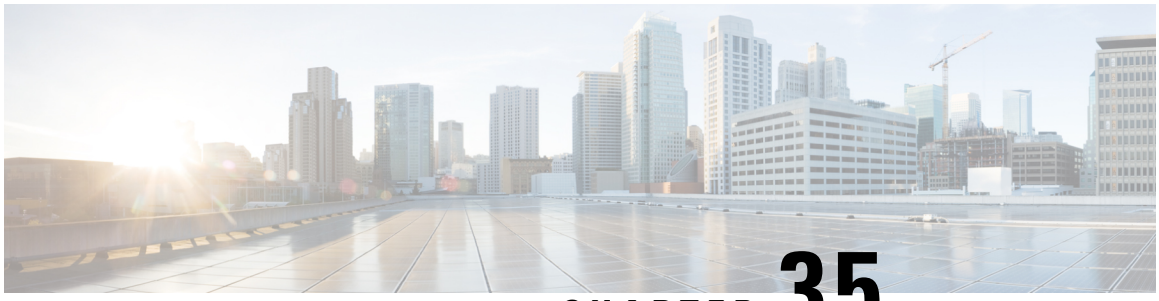
The following bulk statistics are added to the System schema as part of this feature:

System Schema

Following new counters are provided under the existing **show bulkstats variables system**.

Table 9: Bulk Statistics Varibales in the System Schema

Variables	Description
ikev2-notifpaysent-pdntype-ipv4	The total number of PDN type notification sent for IPv4 event records.
ikev2-notifpaysent-pdntype-ipv6	The total number of PDN type notification sent for IPv6 event records.



CHAPTER 35

MME Support on VPC-SI

Feature Summary and Revision History

Summary Data

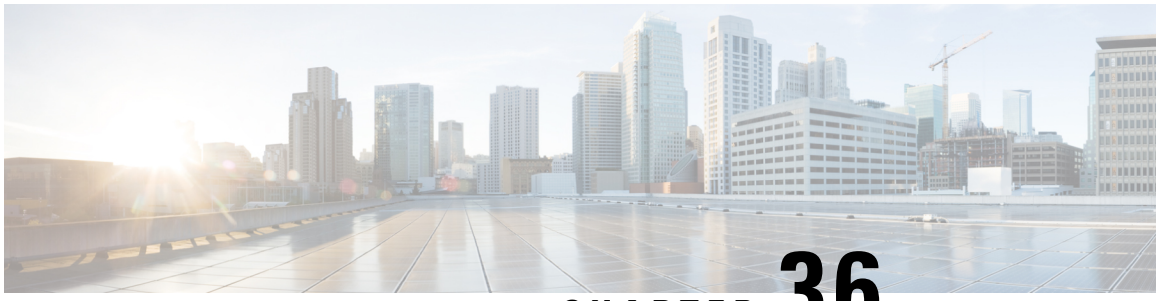
Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	VPC-SI
Feature Default	Disabled – License required to enable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable.

Revision History

Revision Details	Release
First introduced.	21.28.m14

Feature Description

MME supports VPC-SI with VMware ESXi 7.0.3



CHAPTER 36

NAT Port Chunk Hold Timer Support

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.28.m10

Feature Description

With the availability of the NAT Port Chunk Hold Timer feature in P-GW , a port chunk hold timer can be configured for many-to-one NAT IP Pools. When the last port from a port chunk is released, the chunk is moved from **Used** to **Hold** state and the Port Chunk Hold Timer is started. On the expiry of the Port Chunk Hold Timer, the port chunk is released and is made available for new sessions. If any packet is received that results into the port chunk being reused before the expiry of the Port Chunk Hold Timer then the port Chunk Hold Timer is stopped and a port from that port chunk is allocated.

Port chunk can be released in the following ways:

- When the last flow of the last port in the port chunk becomes idle due to timeout, the port chunk hold timer starts, and upon expiry of the port chunk hold timer, the port chunk is released.
- When a Subscriber is disconnected.

Release of a NAT IP happens after expiry of NAT Binding timer. This behavior remains same, irrespective of the Port Chunk Hold Timer feature.

How it Works

The following table summarizes the triggering of various timers for a single last flow using a Port chunk.

Table 10: Corresponding Timers in Seconds

Seconds	Timer
a	UDP idle timeout
b	TCP idle timeout
c	NAT Binding timeout
d	Mapping timeout
e	Port chunk hold timeout

Table 11: Triggers for Releasing NAT Port, Port Chunk, and NAT IP

Last Flow Protocol in the NAT Port Chunk	Release of NAT Port (NAT mapping) to the Chunk	Release of Port Chunk (when port-chunk-hold-timer is enabled)	Release of NAT IP from the REALM

UDP	Released after idle timeout of a seconds + Mapping timeout of "d" seconds	Release after the expiry of Port chunk hold timeout in "e" seconds (port chunk hold timer started after last NAT port release of the chunk) Total time to release the port chunk from the point when the UDP flow became inactive is (a + d + e) seconds	Released after NAT binding timer expiry
TCP (graceful)	In case TCP flow is closed upon receiving RST/FIN, then the NAT port is released after the flow is cleared. But the port is reusable for the configured NAT 2MSL timeout.	Released after the expiry of Port chunk hold timeout in "e" seconds (port chunk hold timer started after the last NAT port release of the chunk). 2 MSL and port chunk timer run in parallel. If 2MSL is > Port chunk hold timeout, then port is forced to Free state and port chunk is released. Total time to release port chunk after the last TCP flow gets cleared in Port chunk hold timeout "e" seconds.	Released after NAT binding timer expiry
TCP (open)	No FIN/RST sent; upon expiration of idle-timeout of "b" seconds + Mapping timeout of "d" seconds	Release after expiry of Port chunk hold timeout in "e" seconds (port chunk hold timer started after the last NAT port release of the chunk) Total time to release the port chunk from the point when the TCP flow became inactive is (b + d + e) seconds	Released after NAT binding timer expiry

Configuring Port Chunk Hold Timer

Use the following configuration to decouple NAT binding timer and port chunk hold timer separately.

The port chunk hold timer configuration applies to all NAT IP address in the NAT IP pool.

```
configure
   context context_name
      ip pool nat_pool_name { ip_address subnet_mask | ip_address/mask> |
range from_ip_address to_ip_address  }
     napt-users-per-ip-address users [ alert-threshold [ { pool-free |
pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] + ]
     [ max-chunks-per-user chunks] [ nat-binding-timer binding_timer [
port-chunk-hold-timer port-chunk-hold-timeout ] ]
     [ on-demand ] [ port-chunk-size size ] [ port-chunk-threshold threshold
 ] [ send-nat-binding-update ] [ srp-activate ] + ]
```

NOTES:

- **port-chunk-hold-timer** *[port-chunk-hold-timeout]*: Configures timeout in seconds after which a freed port chunk can be reused in a NAPT IP pool. If either the value is set to 0 or this is not configured, then

to maintain backward compatibility, port chunks are released based on the **nat-binding-timer**. The minimum value is 0 and the maximum value is 31556926. By default, the Port Chunk Hold Timer is disabled. You can enable the Port Chunk Hold Timer again with a nonzero value but less than a NAT binding timer value.

Note

- It is recommended to configure a NAT binding timer value while enabling the port chunk hold timer feature.
- If you disable the **nat-binding-timer** and configure the **port-chunk-hold timer**, the NAT IP address will not be freed, and all NAT port chunks will be released after the **port-chunk-hold timer** expires.
- Specify only lesser value for the **port-chunk-hold timer** than the NAT binding timeout value. If the port chunk hold timeout value is configured higher than the NAT binding timeout, the following CLI error appears.

```
"Failure: NAT port chunk hold timer must be less than
NAT binding timer."
```

- Do not configure lesser than 2MSL as the port chunk hold timer.
- Since Port Chunk Hold Timer value is lower than NAT Binding Timer, use of this feature will result into increased number of NAT Binding Records (NBR). Setting too low a value of this timer results into a high number of NBRs. While actual value depends on traffic profile of the subscribers, keeping a value of 300 seconds for Port Chunk Hold Timer when NAT Binding Timer is 1800 seconds should be acceptable for most deployments.

Modifying Port Chunk Hold Timer

Use the following configuration to modify a port chunk hold timer.

```
configure
   context context_name
      ip pool nat_pool_name [ nat-binding-timer binding_timer
port-chunk-hold-timer port_chunk_hold_timeout  ]
   exit
```

NOTES:

- **nat-binding-timer** *binding_timer* **port-chunk-hold-timer** *port_chunk_hold_timeout* : Specify a Port chunk hold timeout for modifying port chunk hold timer for the ip pool. As soon as the port chunk hold timer is modified for the ip pool, the new Port Chunk Timer uses the modified value for all subscribers.

Sample Configuration

The following configuration is a sample output.

```
[local]qvpc-si# configure
[local]qvpc-si(config)# context egress
```

```
[egress]qvpc-si(config-ctx)# ip pool pgw_nat_ps_int01 97.36.232.0 255.255.255.252
napt-users-per-ip-address 2 group-name pgw_nat_ps_int alert-threshold pool-free 20 clear
25 on-demand max-chunks-per-user 1 port-chunk-size 32256 nat-binding-timer 600
port-chunk-hold-timer 300
```

Downgrade Process

We recommend reconfiguring the ip pool CLI with the exclusion of the **port-chunk-hold-timer** CLI keyword because if you save the configuration with the **port-chunk-hold-timer** CLI keyword and downgrade when you reload with the same configuration file in the downgraded image, then the entire ip pool CLI gets ignored.

Monitoring and Troubleshooting

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

Show Commands and/or Outputs

This section provides information about the show CLI commands that are available in support of the feature.

show configuration

Use this **show configuration** CLI command to view the following field that is available in support of Port chunk Timer behaviour for many-to-one NAT feature:

- **port-chunk-hold-timer** : Displays timeout in seconds after which a freed port chunk can be reused in a NAPT IP pool.

Sample Output

```
[local]qvpc-si# show configuration
Config
  context egress
    ip pool ipv4-private 10.0.0.1 255.255.0.0 private 0 srp-activate group-name int41
alert-threshold group-available 20 clear 25
    ip pool ipv4-static 11.0.0.1 255.255.0.0 static
    ip pool pgw_nat_ps_int01 97.36.232.0 255.255.255.252 napt-users-per-ip-address 2
group-name pgw_nat_ps_int alert-threshold pool-free 20 clear 25 on-demand port-chunk-size
32256 nat-binding-timer 600 port-chunk-hold-timer 300
  exit
```

show ip pool nat-realm

Use this **show ip pool nat-realm** CLI command to view the following field that is available in support of Port chunk Timer behaviour for many-to-one NAT feature:

- **Port-chunk-hold-Timer in seconds**: Displays timeout in seconds after which a freed port chunk can be reused in a NAPT IP pool.

Sample output:

```
show ip pool nat-realm
```

```
Group: pgw_nat_ps_int
     Pool: pgw_nat_ps_int01       97.36.232.0      255.255.255.252
     Pool Status:       Good
     Pool Id: 3
        Type:            NAPT                    Priority:   0
        Group:                                   pgw_nat_ps_int
           Used:            0                     Free:       2

           Hold:            0                     Released:   0
           Limit Exceeded:  0                     Total Alloc Req: 0
           Total Rel Req:   2
              Recovered Alloc Req: 0          Alloc Req by Group:  2
  User-Plane Id: N/A
  Virtual-FE Id: N/A
  User-Plane Id: N/A
  Virtual-FE Id: N/A
  Vdu group name:
     Number of Users Per-IP: 2
     IP Sharing: Disabled
     Shared IP Size: n/a
     Allocation Mode: On-Demand
     Port Chunk Size: 32256
     Port Chunk Threshold: 100
     Maximum Number of Chunks per User: 1
     Minimum Number of Chunks per User: 0
     Nat-Binding-Timer: 600

     Send-Nat-Binding-Update: Disabled
     Nexthop Forwarding Address: Disabled
        Pool-Free Threshold:  20%                          Clear:  25%
        Pool-Used Threshold: Disabled                      Clear: Disabled
        Pool-Release Threshold: Disabled                   Clear: Disabled
        Pool-Hold Threshold: Disabled                      Clear: Disabled
        cip-local-pool-used Threshold: Disabled            Clear: Disabled
        cip-local-pool-in-use-addr Threshold: Disabled     Clear: Disabled
        Include-Network-Broadcast-Address: Disabled
        Port-chunk-hold-Timer in seconds: 300
             Group Summary:
             Group Used:                          0
             Group Free:                          2
             Group Hold:                          0
             Group Quarantine:                    0
             Group Released:                      0
             Group Effective Alarm Threshold %: Disabled
             Group Effective Clear Threshold %: Disabled
             Group Current Usage %:               0.00%
             Group Status:                        Good
```

show active-charging nat statistics

The **show active-charging nat statistics** displays the following output.

```
[local]qvpc-si# show active-charging nat statistics
Thursday March 09 23:30:21 EST 2023
NAT Realm Utilization:
----------------------
Realm Name:               pgw_nat_ps_int  Context:                          egress
Current IP Address-In-Use:           n/a  Total IP Address:                    2
Current Calls Using-Realm:           n/a  Current Port-Chunks Available:     n/a
Current Port-Chunks-In-Use:          n/a  Total Port-Chunks:                   4
Current Port-Chunks-On-hold     :    n/a
Port-Chunk size:                     n/a
Statistics:
```

```
  Total AAA alloc msgs sent:           0  Total AAA dealloc msgs sent:         0
  Total flows denied no IP:            0  Total flows denied no port:          0
  NAT44 flows denied no IP:            0  NAT44 flows denied no port:          0
  NAT64 flows denied no IP:            0  NAT64 flows denied no port:          0
  Total flows denied no memory:        0
  NAT44 flows denied no memory:        0  NAT64 flows denied no memory:        0
  Total bytes Transferred:             0  Total flows processed:               0
  NAT44 bytes Transferred:             0  NAT44 flows processed:               0
  NAT64 bytes Transferred:             0  NAT64 flows processed:               0
  Average TCP port usage:              0  Average UDP port usage:              0
  Average Others port usage:           0

Realm Name:             pgw_nat_ps_int01  Context:                         egress
Current IP Address-In-Use:               1  Total IP Address:                    2
Current Calls Using-Realm:               0  Current Port-Chunks Available:       3
Current Port-Chunks-In-Use:              0  Total Port-Chunks:                   4
Current Port-Chunks-On-hold     :        1
Total Reserved Port-Chunks:                                                      0
Current Reserved Port-Chunks-In-Use:                                             0
Current Available Reserved Port-Chunks:                                          0
Port-Chunk size:                     32256
Statistics:
  Total AAA alloc msgs sent:           0  Total AAA dealloc msgs sent:         0
  Total flows denied no IP:            0  Total flows denied no port:          0
  NAT44 flows denied no IP:            0  NAT44 flows denied no port:          0
  NAT64 flows denied no IP:            0  NAT64 flows denied no port:          0
  Total flows denied no memory:        0
  NAT44 flows denied no memory:        0  NAT64 flows denied no memory:        0
  Total bytes Transferred:            84  Total flows processed:               1
  NAT44 bytes Transferred:            84  NAT44 flows processed:               1
  NAT64 bytes Transferred:             0  NAT64 flows processed:               0
  Average TCP port usage:              0  Average UDP port usage:              1
  Average Others port usage:           0

Port-Chunks distribution:
Max no.of chunks used   Total no.of subscribers   Current no.of subscribers
---------------------   -----------------------   -------------------------
         1                         1                         1

Ports distribution:
Max no. of ports used   Total no. of subscribers
---------------------   -----------------------------------
         [0-8]                     1

Total Realms: 2
```

Bulk Statistics

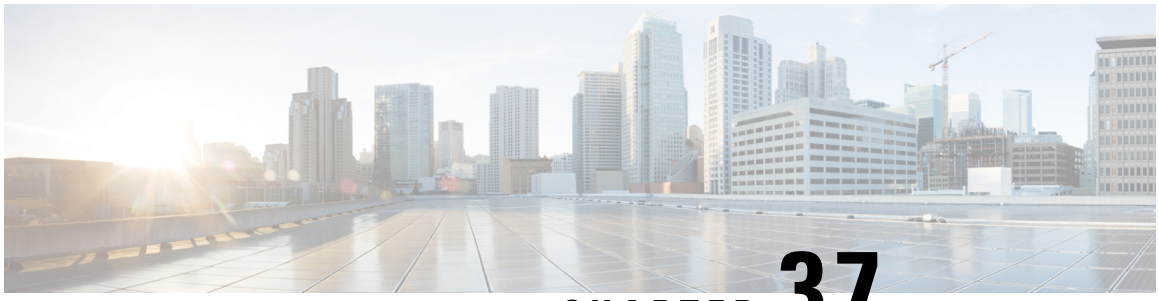
This section provides information on the bulk statistics schema.

NAT Realm Schema

The NAT Realm schema provides operational statistics that can be used for monitoring and troubleshooting the NAT Port chunk hold timer feature.

Table 12: Bulk Statistic Variables in the NAT Realm Schema

Variables	Description
nat-rlm-port-chunks-on-hold	The total number of port chunks on hold, which are collected per context and for each realm



CHAPTER 37

Port Number Behavior in EDR Module Configuration

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	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Reference Guide* • *ASR 5500 System Administration Guide* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide*

Revision History

Revision Details	Release
First Introduced.	2024.02.0 (21.28.m23)

Behavior Change

After Cisco SSH or SSL upgrade, the port number behavior has changed for the EDR-module configuration.

Previous Behavior: In the EDR-module configuration, the default SFTP port number "0" was selected automatically and connected to port 0 when colon was specified.

For example:

cdr transfer-mode push primary url sftp://root:starent@192.0.2.1:/root/EDR/ via local-context

New Behavior: The EDR-module configuration allows the new default SFTP port number "22" or disallow the port number without specifying a colon.

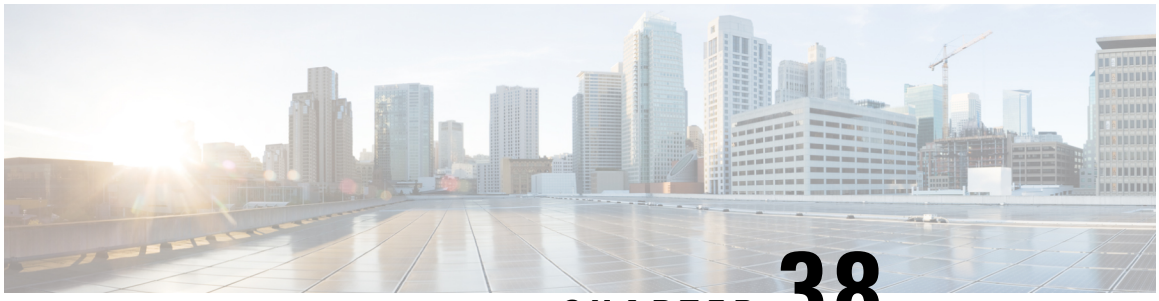
If colon is specified after host, the port number is mandatory. The default SFTP port number is 22. If colon is not specified after host, the port number need not be entered and the default SFTP port number is used.

For example:

cdr transfer-mode push primary url sftp://root:starent@192.0.2.1:22/root/EDR/ via local-context(with default SFTP port number)

cdr transfer-mode push primary url sftp://root:starent@192.0.2.1/root/EDR/ via local-context (without colon)

For more information about **cdr** command, see the EDR Module Configuration Mode Commands chapter in the *Command Line Interface Reference Guide*.



CHAPTER 38

Public Warning System Failure and Restart Indication Support on SBc Interface

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5000 • VPC-DI • VPC-SI
Feature Default	Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	Release
MME is enhanced to show two new failure message types. Session manager and MME manager facility stack are updated to handle the PWS failure and restart indications.	21.28

Feature Description

The MME uses the SBc interface, between the MME and the Cell Broadcast Center (CBC), for warning message delivery and control functions.

The MME supports a Commercial Mobile Alert System (CMAS)—SBc interface and underlying protocols. CBC sends Warning Messages over the SBc-AP interface and relays to all relevant eNodeBs over the S1-AP interface.

MME upon receiving Public Warning System (PWS) failure or restart indication starts a CBC transaction to notify MME on the failure or restart.

Note MME supports only up to 256 maximum elements in PWS Restart-TAI-List. If the eNodeB sends more than 256 elements, the PWS Restart Indication message does not get relayed to the CBC.

Session manager and MME manager facility stack are updated to handle the PWS failure and restart indications.

The CMAS functionality is enabled in the networks to provide warning notifications to subscribers.

Important A valid license key is required to enable the SBc interface. Contact your Cisco account representative for information on how to obtain a license.

How It Works

The MME accepts incoming SBc associations coming from multiple CBCs.

The MME is responsible for the delivery of the Warning Messages received from CBC to all relevant eNodeBs serving the given TAI list. In the absence of TAI list in the received Warning Message, MME sends the Warning Message to all connected eNodeBs.

The MME acknowledges to CBC when it has started distributing the Warning Message to all relevant eNodeBs. If a response is not received from any eNodeB, it shall not result in any exclusive error messaging to CBC.

Even if the MME node is experiencing congestion, Warning Messages are forwarded and not dropped.

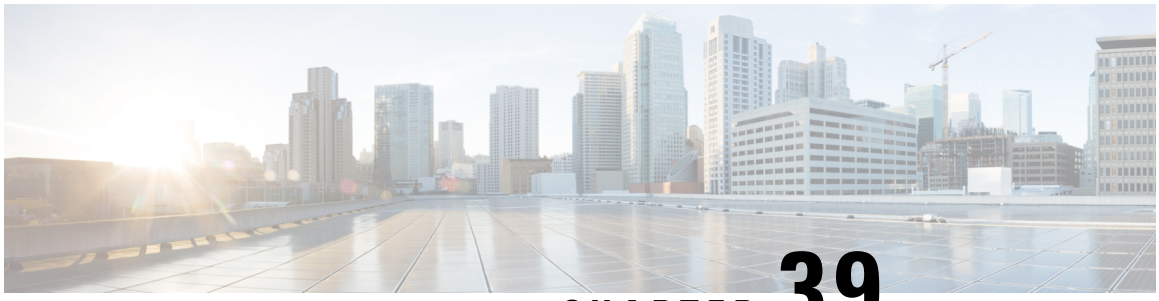
When connected to multiple CBCs, the uniqueness of Warning Messages as identified by Message Type, Message Identifier and Serial Number, must be ensured across these CBCs.

Warning Message Call Flows

In compliance with 3GPP TS 29.168 v15.1.0, the MME supports the following procedures:

- Write-Replace Warning Procedure
- Stop Warning Procedure
- Error Indication Procedure
- Write-Replace Warning Indication Procedure

- Stop Warning Indication Procedure
- PWS Failure Indication
- PWS Restart Indication



CHAPTER 39

Prioritizing IMEI over MAC Address

Revision History

Revision Details	Release
First introduced.	21.28.m22

Feature Changes

Previous Behavior: If IMEI was received in Create Session Request for a Wi-Fi call, the ePDG CDR encoded MAC address in the servedIMEISV field. The MAC address was given preference over IMEI and encoded in servedIMEISV. With this behavior, CDR processing was affected.

New Behavior: IMEI will be prioritized over MAC address and will be sent in the servedIMEISV field. The servedIMEIsv field in CDR is optional. If Create Session Request for a Wi-Fi call has both IMEI and MAC address, then IMEI is encoded in servedIMEIsv.

This behavior is configurable using the **gtpp prioritize-imei-over-mac-address** CLI in the GTPP Server Group Configuration mode. If the CLI is not configured, the existing behaviour will take effect.

Command Changes

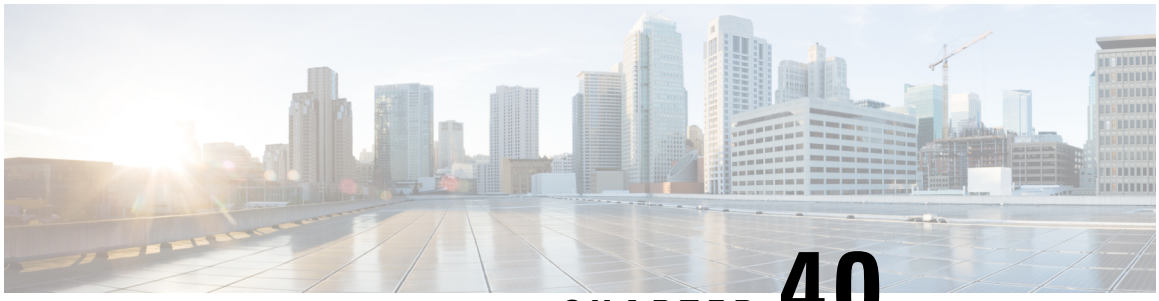
Use the following configuration to prioritize IMEI over MAC address and encode IMEI in the servedIMEISV field of the CDR. If IMEI is not available, the servedIMEISV field will not be present in the CDR.

```
configure
  context context_name
    gtpp group group_name
      [ default | no ] gtpp prioritize-imei-over-mac-address
      end
```

NOTES:

- **default | no**—Specify either one of the options to prioritize MAC over IMEI and encode it in servedIMEISV field. This is the existing behavior.

  If MAC is not available, then IMEI is encoded in the servedIMEISV field.



CHAPTER 40

Processing APCO IE on Unsupported Container ID

Feature Summary and Revision History

Summary Data

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

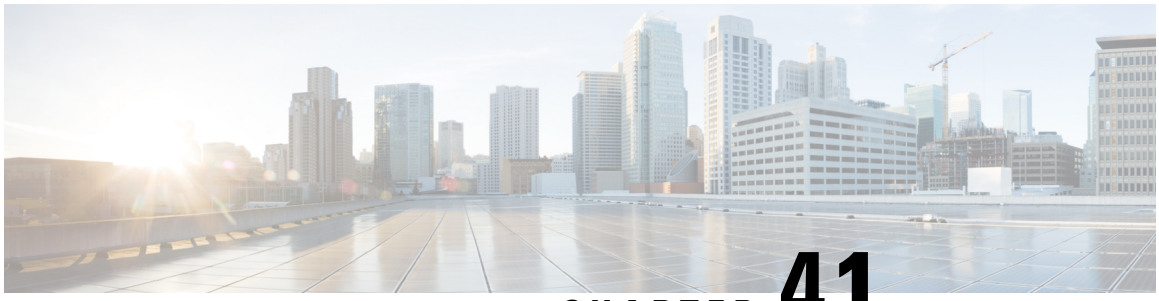
Revision History

Revision Details	Release
ePDG skips the unsupported container and continue parsing the next container in APCO.	21.28.m0

Feature Changes

Previous Behavior: ePDG stops parsing when it encounters an unknown container ID in Additional Protocol Configuration Options (APCO) in Create Session Response.

New Behavior: ePDG allows you to skip the unsupported container and continue parsing the next container in APCO.



CHAPTER 41

QCI67 Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *MME Administration Guide* • *Statistics and counters Reference*

Revision History

Revision Details	Release
Support is provided for additional QCI value 67.	21.28

Feature Description

MME supports the new standard Quality of Service Class Indentifier value (QCI) 67 in addition to the eixsting values 65, 66, 69 and 70.

Monitoring and Troubleshooting

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

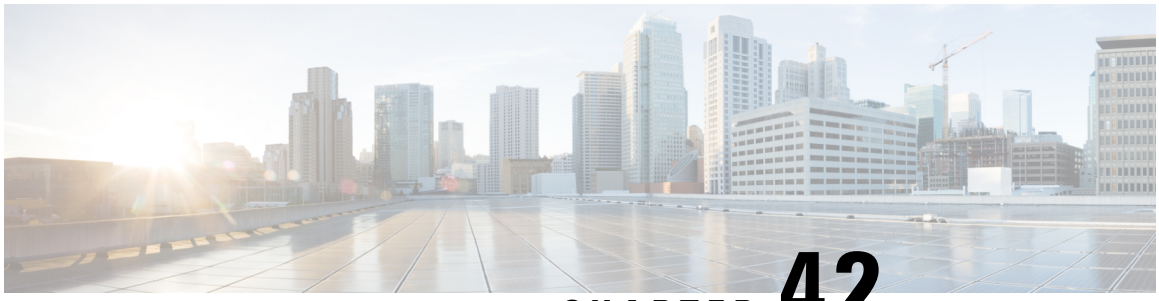
Show Commands and Output

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

show mme-service statistics

The output of this command displays the following field.

Field	Description
EPS QoS Not Accepted	The total number of ESM Bearer Allocate Reject messages sent, for bearer allocation failures, with the cause "EPS QoS Not Accepted".



CHAPTER 42

Recording the APN in the EDR Record

Feature Summary and Revision History

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

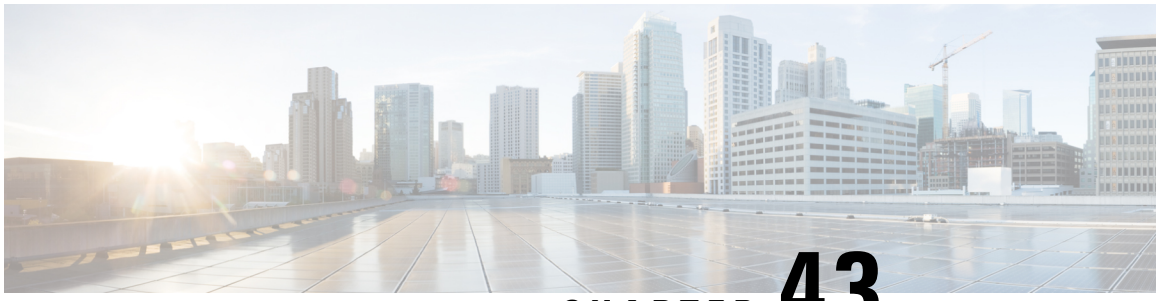
Revision History

Revision Details	Release
Recording the APN field in the EDR record	21.28.m10

Feature Changes

Previous Behavior: For 2G Gn or S4 calls, if the APN field contains special characters (newline (\n), comma(,), Double quotes(")), the APN field is printed without escape characters and does not get enclosed with double quotes.

New Behavior: For 2G Gn/S4 calls, if the APN field contains special characters (newline (\n), comma(,), Double quotes(")), the APN field gets enclosed with double quotes. If double quotes are found within the APN, then it precedes with another double quote.



CHAPTER 43

Reject Sessions from Blocked APGROUPNAME

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First Introduced.	• 21.28.mx • 21.28.m1

Feature Description

The SaMOG supports the configuration of a list of APGROUPNAME for which session authentication is to be blocked, and the rejection of incoming sessions (For example, AP group name) belongs to the configured APGROUPNAME block list.

The rejection of incoming sessions is applicable only for the combination of RADIUS Access-Request-based triggers, EoGRE user-plane, Diameter-based authentication with AAA on an STa interface, and GTPv2-based S2A interface.

Configuring APGROUPNAME List

Use the following commands to configure apgroupname-list under the samog context with blocked apgroupnames.

```
configure
   context context_name
     apgroupname-list aplistname1
        apgrp apgrpname1
   end
```

NOTES:

- **apgroupname-list**: Configures the APGROUPNAME list.

  Only 25 AP group names are allowed to be configured in the list. You can create a maximum of 10 AP group name lists per context.

  If the **apgroupname-list** is dis-associated for any specific samog-service, then AP group names under the list are considered as allowed for the session continuation.

- **apgrp**: Configures blocked apgroup names within the list.

Associate APGROUPNAME-list to SaMOG Service

Use the following configuration to associate the configured apgroupname-list with samog-service.

```
configure
   context context_name
   samog-service samog1
   associate apgroupname-list aplistname1 reject-call
   end
```

NOTES:

- **associate apgroupname-list**: Associates the configured apgroupname-list with samog-service.

Remove the APGROUPNAME List Configuration

Use the following configuration to remove the configured apgroupname-list with samog-service and allows the AP group names to establish session.

```
configure
  context context_name
    [ no ] apgroupname-listaplistname1
   end
```

NOTES:

- **no** : Removes the blocked APGROUPNAME list from SaMOG.

Remove the APGROUPNAME from APGROUPNAME-list

Use the following configuration to remove the APGROUPName from APGROUPNAME-list.

```
configure
  context context_name
    apgroupname-list  aplistname1
     [ no ] apgrp apgrpname1
   end
```

NOTES:

- **no** : Removes APGROUPNAME entry from APGROUPNAME list.

Dis-associate APGROUPNAME List to SaMOG Service

Use the following configuration to dis-associate the configured apgroupname-list from samog-service.

```
configure
  context context_name
  samog-service samog1
  [ no ] associate apgroupname-list reject-call
   end
```

NOTES:

- **no associate apgroupname-list reject-call**: Dis-associates APGROUPNAME list from the SaMOG and all the AP group names present in the list are allowed to establish session.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show samog-service name

Use the following command to verify the association of apgroupname-list.

Table 13: show samog-service name Command Output Description

Field	Description
Service Name :	
Associated APGROUPNAME List	Displays the associated APGROUP name list.

show apgroupname-list summary

You can verify the apgroupname-list configuration. The output of this command is enhanced to display the following field.

Table 14: show appgroupname-list summary Command Output Description

Field	Description
Context	Displays the context within which the apgroupname list is created.
Apgroupname-List	Displays the list name configured.

show apgroupname-list name

You can verify the apgroupname-list configuration. The output of this command is enhanced to display the following field.

Table 15: show appgroupname-list name aplistname Command Output Description

Field	Description
List name	Displays the list name.
Associated with SAMOGService	Displays the SAMOG service that the blocked APgroupname-list is associated with.
Service context	Displays the context within which blocked APgroupname-list is created.
Number of APGROUPNAMEs in list	Displays number of apgroupnames configured within the list.
List of APGROUPNAMEs in list	Displays a space separated list of names.

show config

Using the **show config** commnad you can view the associate apgroup-name list and apgroup-name lists.

Sample output:

```
[samog]asr5500# show config
config
  cli hidden
  tech-support test-commands encrypted password ***
  cli test-commands encrypted password ***
  :
samog-service samog1
```

```
  associate mrme-service mrme1
  associate cgw-service cgw1
  associate dhcp-service dhcp1 level system
  associate subscriber-map smap4g
  associate apgroupname-list aplistname1 reject-call
  timeout setup 120
  timeout absolute 600
  plmn id mcc 777 mnc 109
#exit

apgroupname-list aplistname1
  apgrp myapg1
  apgrp myapg2
  apgrp myapg3
  apgrp myapg4
  apgrp myapg5
  apgrp myapg6
#exit
```

show samog-service statistics name

Use the **show samog-service statistics name** command to verify the counter for blocked apgroupname. In the sample output, when samog-service performs UE initiated attach with Radius session triggered over EoGRE access type with Diameter-based authentication, and EPC connectivity over GTPv2 to P-GW from blocked apgroupname, the session gets rejected and the blocked counter value is incremented.

```
[samog]qvpc-di# show samog-service statistics name samog1
SaMOG statistics for Service: samog1
MRME Service Stats:
Session Stats:
  Total Attempted:                                    0
  Total Setup:                                        0
  Total Current:                                      0
  Total Released:                                     0
    Total Aborted:                                      0
    Total Disconnected:                                 0
      Disconnected locally:                             0
      Disconnected by UE:                               0
      Disconnected by NAS:                              0
      Disconnected by CGW:                              0
      Disconnected by AAA:                              0
Radius Message Stats:
  Total Start Req rcvd:                               0
  Total Start Req (Retransmitted) rcvd:               0
  Total Start Rsp sent:                               0
  Total Interim Updt rcvd:                            0
  Total Interim Updt (Retransmitted) rcvd:            0
  Total Interim Updt Rsp sent:                        0
  Total Stop Req rcvd:                                0
  Total Stop Req (Retransmitted) rcvd:                 0
  Total Stop Rsp sent:                                0
  Total Accounting On rcvd:                           0
  Total Accounting Off rcvd:                          0
  Total Access Req rcvd:                              0
  Total Access Req (Retransmitted) rcvd:              0
  Total Access Challenge sent:                        0
  Total Access Accept sent:                           0
  Total Access Reject sent:                           0
     Congestion control policy applied:               0
     No Policy Match:                                 0
  Total Unknown Req rcvd:                             0
  Total Send Failure:                                 0
  Total Discarded:                                    0
```

```
Mandatory Attr Missing:                          0
Start For Non-Existing Session:                  0
Interim For Non-Existing Session:                0
Stop For Non-Existing Session:                   0
Unknown Client:                                  0
Invalid Authenticator:                           0
Stale Packets:                                   0
Service Not Supported:                           0
No Resource:                                     0
Internal Error:                                  0
License Limit Exceeded:                          0
Service Limit Exceeded:                          0
Invalid Length:                                  0
Invalid EAP:                                     0
Pending server response:                         0
Congestion control policy applied:               0
Newcall policy applied:                           0
Blocked APGroupName:                             0
```

Bulk Statistics

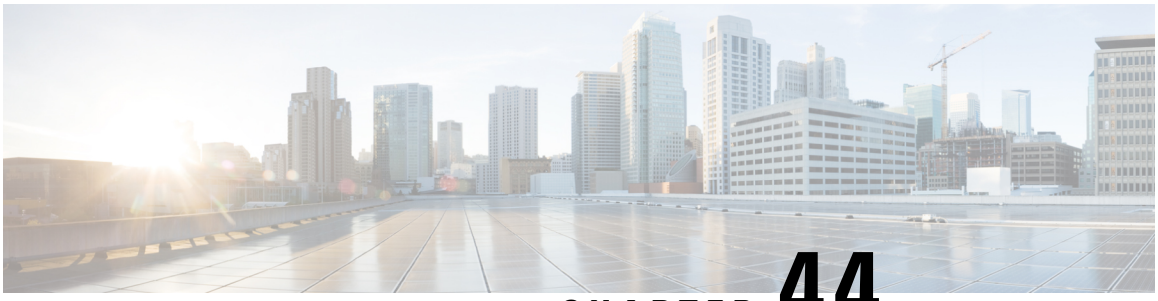
The following bulk statistics are added to the SaMOG schema as part of this feature:.

SaMOG Schema

The following bulks statistics included in the SaMOG schema to support this feature:

Table 16: Bulk Statistic Variables in the SaMOG Schema

Variables	Description
mrme-total-discard-blocked-apgroupname	Displays total number of sessions discarded due to blocked apgroupname.



CHAPTER 44

Send 5G User Location Information to SMF+PGW-c

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
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide*

Revision History

Revision Details	**Release**
First introduced.	21.28.m10

Feature Description

ePDG supports the 5G Cell ID feature to:

- Decode Geographic Location Types such as 135, 136 and 137 (NCGI, 5GS TAI, 5GS TAI and NCGI respectively), which are received in the 3GPP-User-Location-Info AVP of the Diameter EAP Answer (DEA) on the SWm interface from the AAA server.
- Upon receiving the Geographic Location Types 135,136 or 137, ePDG constructs the 5G ULI from the 3GPP-user-Location-Info AVP and sends the 5G ULI in the ULI IE of CreateSessionRequest, when the configuration to send the 5G ULI is enabled and the call is decided to be latched on to SMF+PGW-c.

Assumption

SMF+PGW-c can either decode the customized User Location Information IE received in the Create Session Request on the S2b interface or ignore the custom 5G ULI and proceed with the call.

How it Works

This section provides a call flow and procedure that explains the scenario of sending 5G ULI to SMF+PGW-c.

Call Flow

Figure 14: ePDG Setup Procedure Call Flow

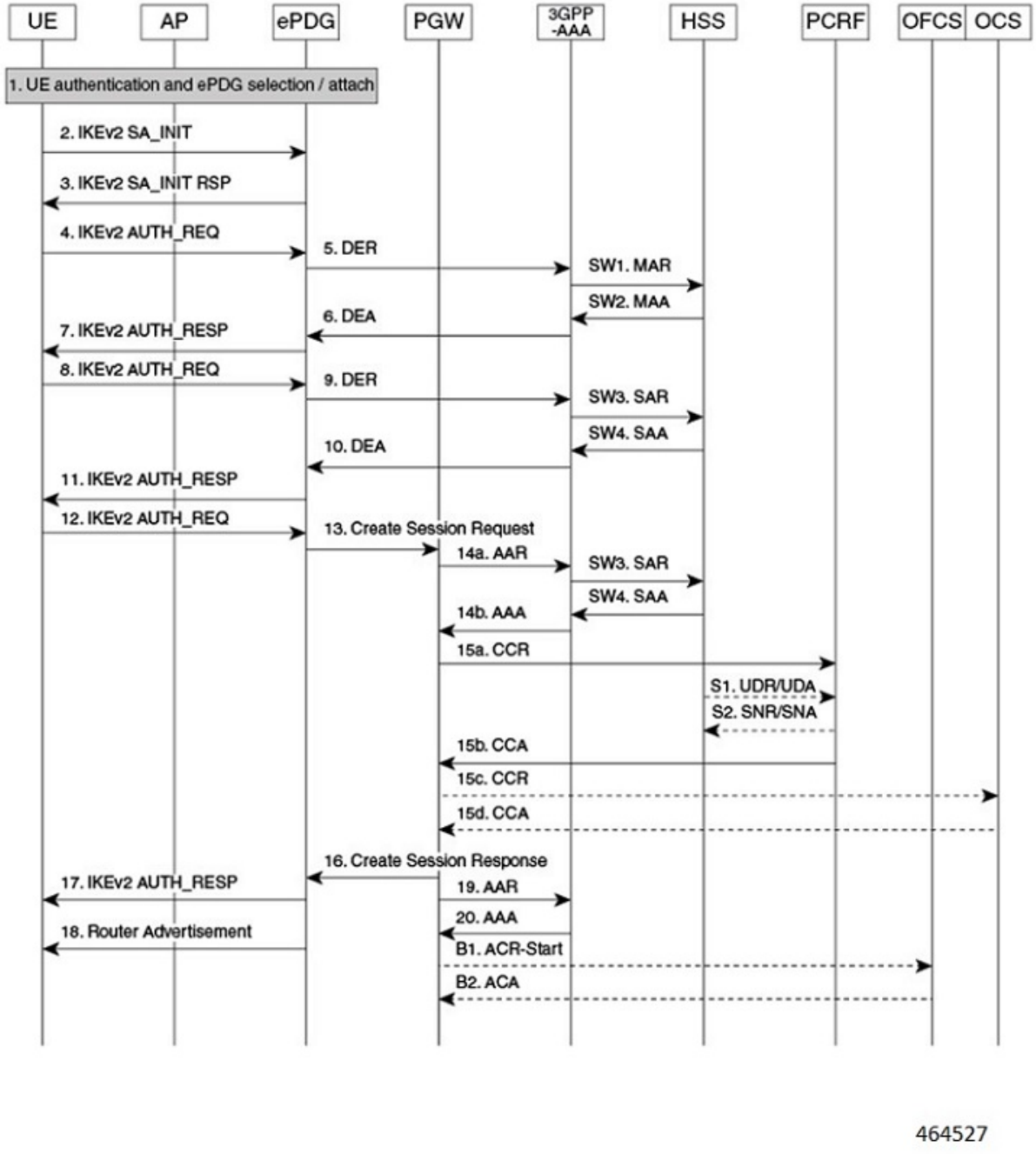


Table 17: ePDG Setup Procedure Call Flow Description

Step	Description
2.	The UE sends the IKE_SA_INIT message.
3.	The ePDG responds with the IKE_SA_INIT_RSP message.
4.	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.
5	The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN.
6.	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. The ePDG uses these parameters and the 5G NAS capability from the UE to determine if SMF+PGW-c or P-GW must be selected.

Step	Description
7.	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.
8.	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.
9.	The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA server.
10.	The AAA Server responds with DEA (Diameter EAP Answer). DEA contains 3GPP-User-Location-Information (ULI) for 5G if configured and available.
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.
13.	ePDG constructs 5G ULI and sends it in ULI IE of Create Session Request to the selected SMF+PGW-c upon the following conditions: • The 3GPP-User-Location-Information (ULI) for 5G is received. • The SMF+PGW-c is selected to latch on. • The **epdg-s2b-gtpv2 send 5g-uli** CLI for sending 5G ULI is enabled.
14 a through 16.	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-C receives PDU Session ID, it adds S-NSSAI in the APCO field of Create Session Response.

Step	Description
17.	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 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. **Note** If the UE does not support 5GC NAS but has a 5GS subscription, SMF+PGW-c is selected, and if interaction with UDM, Policy Control Function (PCF), and UPF is required, then SMF+PGW-c assigns PDU Session ID. The SMF+PGW-c does not provide any 5GS related parameters to the ePDG.
18.	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 Elements and AVP Support

This feature supports the following IE and AVPs based on TS 29.061, TS 29.274, and TS 38.413:

3GPP-User-Location-Information

With the existing 3GPP-User-Location-Information AVP 22, ePDG supports Geographic Location Type NCGI (135), 5GS TAI (136), and 5GS TAI & NCGI (137) as part of the 5G Cell ID feature.

5GS TAI and NCGI Formats on the SWm Interface

The Geographic Location Types 135, 136 and 137, 5GS TAI and NCGI are decoded as per subclause 9.3.3.11 in the 3GPP TS 38.413 and 9.3.1.7 in 3GPP TS 38.413. ePDG supports both lead and trail spare nibble padding formats for NCI through a CLI configurable option. By default ePDG considers NCI with lead spare nibble padding. If AAA server encodes with trail spare nibble padding, ePDG should be configured to support trail spare nibble padding for NCI. Refer the *Configuring ePDG to Enable NCI trail Spare Nibble Padding* section for more information.

Table 18: 5GS TAI format on the SWm interface

Octets	8	7	6	5	4	3	2	1
I	MCC digit 2				MCC digit 1			

i+1	MNC digit 1	MCC digit 3
i+2	MNC digit 3	MNC digit 2
i+3 to i+5	5G Tracking Area Code (TAC)	

Table 19: NCGI format with lead spare nibble padding of NCI on the SWm Interface

Octets	8	7	6	5	4	3	2	1
H	MCC digit 2				MCC digit 1			
h+1	MNC digit 1				MCC digit 3			
h+2	MNC digit 3				MNC digit 2			
h+3	spare				NCI (NR Cell Identifier)			
h+4 to h+7	NCI (NR Cell Identifier)							

Table 20: NCGI format with trail spare nibble padding of NCI on the SWm Interface

Octets	8	7	6	5	4	3	2	1
h	MCC digit 2				MCC digit 1			
h+1	MNC digit 1				MCC digit 3			
h+2	MNC digit 3				MNC digit 2			
h+3 to h+6	NCI (NR Cell Identifier)							
h+7	NCI (NR Cell Identifier)				Spare			

Table 21: PLMN format with 3 digit MNC for 5GS TAI and NCGI on the SWm interface

Octets	8	7	6	5	4	3	2	1
5	MCC digit 2				MCC digit 1			
6	MNC digit 1				MCC digit 3			
7	MNC digit 3				MNC digit 2			

Table 22: PLMN format with 2 digit MNC for 5GS TAI and NCGI on the SWm interface

Octets	8	7	6	5	4	3	2	1
5	MCC digit 2				MCC digit 1			
6	1111				MCC digit 3			
7	MNC digit 2				MNC digit 1			

Custom 5G User Location Information in ULI IE on the s2b Interface

The following formats describe the custom User Location Information IE sent in the Create Session Request on the S2b interface.

Figure 15: User Location Information IE in Create Session Request

	8	7	6	5	4	3	2	1
1	Type=86 (decimal)							
2 o 3	Length=n							
4	5G TAI	NCGI	Spare		Instance			
5	Extended Macro eNodeB ID	MacroeNBID	LAI	ECGI	TAI	RAI	SAI	CGI
a to a+6	CGI							
b to b+6	SAI							
c to c+6	RAI							
d to d+4	TAI							
e to e+6	ECGI							
f to f+4	LAI							
g to g+5	Macro eNodeB ID							
g to g+5	Extended Macro eNodeB ID							
h to h+7	NCGI							
i to i+5	5G TAI							
j to n+4	These octet(s) is/are present only if explicitly specified							
	To include NCGI and 5G TAI: 1. Set NCGI and 5G TAI fields. 2. Include NR Cell identity and 5G TAI in corresponding fields. 3.Length n=15							

474568

Figure 16: NCGI & 5GS TAI formats on the S2b Interface

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
h	MCC digit 2				MCC digit 1			
h+1	MNC digit 3				MCC digit 3			
h+2	MNC digit 2				MNC digit 1			
h+3	Spare				NCI(NR Cell Identifier)			
h+4 to h+7	NCI (NR Cell Identifier)							

NCGI Field

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
i	MCC digit 2				MCC digit 1			
i+1	MNC digit 3				MCC digit 3			
i+2	MNC digit 2				MNC digit 1			
i+3 to i+5	5G Tracking Area Code (TAC)							

5G TAI Field

474569

Configuring ePDG to Enable 5G Cell ID

Use the following configuration to enable or disable sending 5G ULI on the s2b interface:

```
configure
    call-control-profile profile_name
       [ remove ]  epdg-s2b-gtpv2 send 5g-uli
    end
```

NOTES:

- **epdg-s2b-gtpv2 send 5g-uli**: Enables sending of 5G ULI on the s2b interface.

Note ULI for 5G is sent only when ePDG decides to latch the call on SMF+PGW-C. Selection of PGW/SMF+PGW-C is enabled through the 5GIWK feature, which is a licensed feature.

- **remove epdg-s2b-gtpv2 send 5g-uli** : Disables sending of 5G ULI on the s2b interface.

Note If the ePDG receives a 4G TAI and/or ECGI, and if the **epdg-s2b-gtpv2 send uli** has been configured, the ePDG will include the ULI values in the CSReq message, irrespective of whether P-GW or SMF+PGW-C is chosen.

Configuring ePDG to Enable NCI trail Spare Nibble Padding

Use this command to enable or disable trail spare nibble format for NCI that is received in the 3GPP-User-Location-Info AVP of DEA (Diameter EAP Answer) on the SWm interface. By default, the leading spare nibble padding format is used for decoding.

```
configure
    call-control-profile profile_name
       [ remove ] epdg-swm receive nci-spare-nibble-trail
    end
```

NOTES:

- **receive**: Configures the AVP or message options in the receive direction.
- **nci-spare-nibble-trail**: Allows trailing spare nibble format of NCI. By default, the NCI is with the leading spare nibble.
- **remove**: Reverts the configuration for trailing spare nibble format of NCI to default.

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 Cell ID feature.

show configuration

The following **show configuration** command displays the configuration of sending 5g ULI and enabling trail spare nibble padding for NCI:

```
[pdif]asr5500# show configuration
:
:
  call-control-profile ccp1
    authenticate context pdif aaa-group swmgroup
    accounting mode gtpp
    epdg-s2b-gtpv2 send uli
    epdg-s2b-gtpv2 send 5g-uli
    epdg-s2b-gtpv2 send serving-network value uli
    epdg-s2b-gtpv2 send aaa-server-id
    epdg-swm receive nci-spare-nibble-trail
    vplmn-address allowed
    associate accounting-policy ap1
  #exit
```

show subscribers full epdg-service < service_name >

The **show subscribers full epdg-service** < *service_name* > displays the received 5G TAI and NCGI information.

```
ePDG# show subscribers full epdg-service epdg1
Monday November 14 18:46:23 IST 2022

Username: 0100000000000001@syfer.com     Status: Online/Active
  Access Type: epdg                      Network Type: IP
  Access Tech: Wireless LAN              Access Network Peer ID: n/a
  callid: 00004e22                       msid: 100000000000001
  Card/Cpu: 2/1                          Sessmgr Instance: 1
  state: Connected                       Peer address: 1.1.1.1
 :
 :
 :
  Downlink traffic-policing: Disabled
  Uplink traffic-policing: Disabled
  Downlink traffic-shaping: Disabled
  Uplink traffic-shaping: Disabled
  Radius Accounting Mode: access-flow-based auxiliary-flows
  Collapsed cscf subscribers: none

  3GPP User location Info:
     TAI     : MCC = 000        MNC = 000       TAC = 0x0
     ECGI    : MCC = 000        MNC = 000       ECI = 0x00000000
     5GS TAI : MCC = 789     MNC = 12        TAC = 0xabc00f
     NCGI    : MCC = 987        MNC = 123       NCI = 0x0edcb00876
  input pkts: 0                                   output pkts: 0
```

```
  input bytes: 0                                    output bytes: 0
  input bytes dropped: 0                            output bytes dropped: 0
  input pkts dropped: 0                             output pkts dropped: 0
  input pkts dropped due to lorc    : 0             output pkts dropped due to lorc    : 0

  input bytes dropped due to lorc   : 0
  in packet dropped suspended state: 0              out packet dropped suspended state: 0
```

show call-control-profile full name < call_control_profile >

The **show call-control-profile full name** *call_control_profile* command displays:

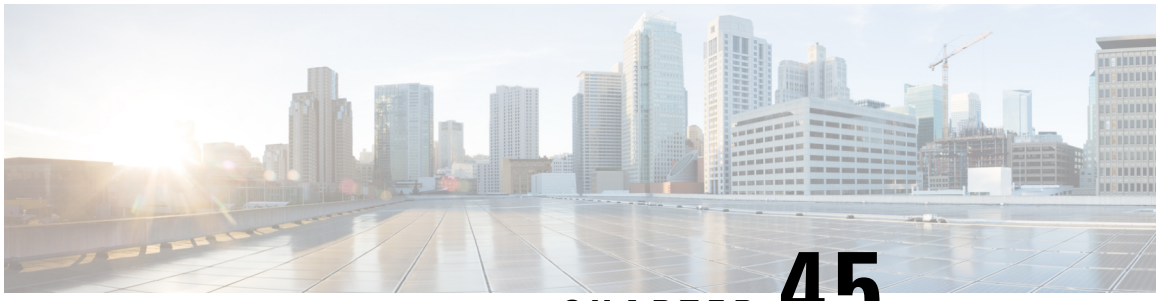
- Whether the configuration for sending 5G ULI is enabled or disabled
- NCI is received with lead or trail padding from AAA server

Sample Configuration:

```
ePDG# show call-control-profile full name ccp1
Monday November 14 18:44:54 IST 2022
Call Control Profile Name = ccp1
Authentication Context Name         : pdif
Authentication AAA Group Name       : swmgroup
Authentication Type                 : DIAMETER
:
:
:
ePDG S2b GTPv2 IE Options:
 Sending UE Local IP and UDP Port        : Disabled
 Sending AAA Server Id                   : Enabled
 Sending WLAN Location Information/TimeStamp  : Disabled
 Sending ULI                                  : Disabled
 Sending custom 5G ULI                   : Enabled
 Sending RAN NAS CAUSE                        : Disabled
 Sending RAN NAS CAUSE Internal Failures      : Disabled
 Sending ServingNetwork[Value ULI]            : Disabled
ePDG S2b GTPv2 Message Options:
ePDG SWm AVP Options:
       NCI with trail padding            : Enabled
ePDG Swm Message Options:
  Authorization and Authenticate Request      : Disabled:
      Triggers:
        Location Retrieval                    : Disabled

WLAN Access:
 P-CSCF Restoration                           : Enabled
 Piggybacking                                 : Disabled
Accounting Mode (SGW/SaMOG)                   : Gtpp
```

show call-control-profile full name < call_control_profile >



CHAPTER 45

Separate Counters for All EAP Type for Success and Failure Events

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Separate counters are added for all EAP type for success and failure events along with the KPI counters.	21.28

Feature Description

To overcome Device Authentication issues, separate counters are introduced for all Extensible Authentication Protocol (EAP) types such as EAP-AKA, EAP-SIM, EAP-PRIME, EAP-TLS, EAP-TTLS, and EAP-PEAP along with the KPI counters (Success/Failure/Drop/Request).

Limitations

The Separate Counters for All EAP Type for Success and Failure Events feature has the following limitations:

- Supports only EoGRE Access-Type . IP Access-Type is not supported.
- Supports only Radius Access-Request trigger type. DHCP, PMIP, and Accounting-based trigger types are not supported.
- Support is limited to GTPv2 based s2a interface.
- Statistics Recovery is not supported.
- Call flows are not affected. Only the counters are affected.
- The previous counter values are not retained after Session Recovery/Card migration/Upgrade and Downgrade. The counters are initialized to zero after Session Recovery/Card migration/Upgrade and Downgrade.

Monitoring and Troubleshooting

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

Show Commands and Output

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

show samog-service statistics

Table 23: show samog-service statistics

Field	Description
SaMOG Statistics for all services	
MRME Service Stats	
Session Stats	
Total Attempted	Total number of sessions attempted.
Total Setup	Total number of sessions setup.

Field	Description
Total Current	Total number of sessions that are currently active.
Total Released	Total number of sessions released
Total Aborted	Total number of sessions aborted.
Total Disconnected	
Disconnected locally	Total number of sessions that were disconnected locally.
Disconnected by UE	Total number of sessions that were disconnected by the UE.
Disconnected by NAS	Total number of sessions that were disconnected by NAS.
Disconnected by CGW	Total number of sessions that were disconnected CGW.
Disconnected by AAA	Total number of sessions that were disconnected by AAA.
Radius Message Stats	
Total Start Req rcvd	Total number of RADIUS start request message received.
Total Start Req (Retransmitted) rcvd	Total number of RADIUS retransmitted start request message received.
Total Start Rsp sent	Total number of RADIUS start response message sent.
Total Interim Updt rcvd	Total number of RADIUS interim update received.
Total Interim Updt (Retransmitted) rcvd	Total number of RADIUS retransmitted interim update received.
Total Interim Updt Rsp sent	Total number of RADIUS interim update response sent.
Total Stop Req rcvd	Total number of RADIUS stop request message received.
Total Stop Req (Retransmitted) rcvd	Total number of RADIUS retransmitted stop request message received.
Total Stop Rsp sent	Total number of RADIUS stop response sent.
Total Accounting On rcvd	Total number of accounting on message received.
Total Accounting Off rcvd	Total number of accounting off message received.
Total Access Req rcvd	Total number of access request message received.
Total Access Req (Retransmitted) rcvd	Total number of retransmitted access request message received.
Total Access Challenge sent	Total number of Access Challenge message sent.
Total Access Accept sent	Total number of Access Accept sent due to congestion policy.
Total Access Reject sent	Total number of Access Rejected sent due to congestion policy.

Field	Description
Congestion control policy applied	
Total Unknown Req rcvd	Total number of unknown requests received for congestion control policy.
Total Send Failure	Total number of congestion control policy sent that failed.
Total Discarded	Total number of congestion control policy discarded.
Mandatory Attr Missing	Total number of missing mandatory attributes.
Start For Non-Existing Session	Total number of start messages sent to non-existing sessions.
Interim For Non-Existing Session	Total number of interim messages sent to non-existing sessions.
Stop For Non-Existing Session	Total number of stop messages sent to non-existing sessions.
Unknown Client	Total number of unknown client.
Invalid Authenticator	Total number of authenticators that is invalid
Stale Packets	Total number of stale packets.
Service Not Supported	Total number of services that are not supported.
No Resource	Total number of resources that are not available.
Internal Error	Total number of internal errors that occurred.
License Limit Exceeded	Total number of license limit exceeded.
Service Limit Exceeded	Total number of license limit exceeded.
Invalid Length	Total number of call control profiles with invalid length.
Invalid EAP	Total number of call control profiles with invalid EAP.
Pending Server Response	Total number of call control profiles with server response pending.
Congestion control policy applied	Total number of congestion control policies applied.
No Policy Match	Total number of Access-Requests dropped due to non-availability of matching PLMN based local policy.
DHCP Message Stats	
DHCP Messages Discarded	Total number of DHCP messages discarded.
Max Size Exceeded	Total number of DHCP messages discarded due to the maximum size exceeded.
Non-Existing Session	Total number of DHCP messages discarded due to a non-existing session.
GiAddr Mismatch	Total number of DHCP messages due to a Gi address mismatch.

Field	Description
Unsupported HW Type or Length	Total number of DHCP messages due to an unsupported hardware type or length.
Stale Packets	Total number of DHCP messages discarded due to stale packets.
Service Not Supported	Total number of DHCP messages discarded due to an unsupported service.
Reauthorization Stats	
Attempts	Total number of reauthorization attempts.
Success	Total number of reauthorization succeeded.
Failure	Total number of reauthorization failure.
Reauthentication Stats	
Attempts	Total number of reauthentication attempts.
Success	Total number of reauthentication succeeded.
Failure	Total number of reauthentication failure.
Handoff Stats	
With Authentication	
Attempts	Total number of sessions attempted for handoff using authentication mechanism.
Success	Total number of sessions with successful handoff using authentication mechanism.
Failure	Total number of handoff failure sessions using authentication mechanism.
With Accounting Start	
Attempts	Total number of sessions attempted for handoff using accounting mechanism.
Success	Total number of sessions with successful handoff using accounting mechanism.
Failure	Total number of sessions with handoff failure using accounting mechanism.
With Accounting Interim	
Attempts	Total number of sessions attempted for handoff using accounting interim mechanism.
Success	Total number of sessions with successful handoff using accounting interim mechanism.

Field	Description
Failure	Total number of sessions with handoff failure using accounting inerim mechanism.
DHCP to DHCP Handoff Statistics	
Received	Total number of DHCP to DHCP handoff statistics received.
Accepted	Total number of DHCP to DHCP handoff statistics accepted.
Denied	Total number of DHCP to DHCP handoff statistics denied.
EAP Client Stats	
Initial Identity Msgs	
NAI Formats	
Root NAI	Total number of UE Identity that uses the root NAI format.
Decorated NAI	Total number of UE Identity that uses the decorated NAI format.
UE Identity formats	
IMSI Identity	Total number of UE Identity that uses an IMSI identity.
Fast Reauth	Total number of UE Identity that uses the fast reauth NAI format.
Pseudonym	Total number of UE Identity that uses the pseudonym NAI format.
Emergency	Total number of UE Identity that uses the emergency NAI format.
Unknown NAI	Total number of UE Identity that uses an NAI format that is unknown.
EAP type	
EAP-AKA	Total number of Extensible Authentication Protocol AKA.
EAP-SIM	Total number of Extensible Authentication Protocol SIM.
EAP-AKA'	Total number of Extensible Authentication Protocol AKA'.
EAP-TLS	Total number of Extensible Authentication Protocol TLS.
EAP-TTLS	Total number of Extensible Authentication Protocol TTLS.
EAP-PEAP	Total number of Extensible Authentication Protocol PEAP.
EAP Unsupported	Total number of Extensible Authentication Protocol that is unsupported. **Important** This counter has been removed in Release 18 and later.

Field	Description
EAP Other	Total number of Extensible Authentication Protocol MSCHAPv2/other. Total number of Extensible Authentication Protocol EAP-TLS or EAP-TTLS/MSCHAPv2.
Initial Non-Identity Msgs	
Total Requested	Total number of initial non-identity messages requested.
Total Rejected	Total number of initial non-identity messages rejected.
Invalid Len	Total number of initial non-identity messages with invalid length.
Invalid Code	Total number of initial non-identity messages with invalid code.
Id Mismatch	Total number of initial non-identity messages with ID mismatch.
Invalid NAI	Total number of initial non-identity messages with invalid NAI.
Invalid IMSI	Total number of initial non-identity messages with invalid IMSI number.
Total Dropped	Total number of initial non-identity messages that were dropped.
Invalid code	Total number of initial non-identity messages with invalid code.
EAP Server Stats	
Total Sent	Total number of EAP server status sent.
Total Received	Total number of EAP server status received.
Success	Total number of EAP server connections succeeded.
Request	Total number of EAP server requests sent.
Failure	Total number of EAP server requests failed.
Drop	Total number of EAP server requests dropped.
Total Received- AKA	Total number of EAP AKA received.
Success	Total number of EAP AKA connections succeeded.
Request	Total number of EAP AKA requested.
Failure	Total number of EAP AKA requests failed.
Drop	Total number of EAP AKA requests dropped.
Total Received- AKA'	Total number of EAP AKA' received.
Success	Total number of EAP AKA' connections succeeded.
Request	Total number of EAP AKA' requested.

Field	Description
Failure	Total number of EAP AKA' requests failed.
Drop	Total number of EAP AKA' requests dropped.
Total Received- SIM	Total number of EAP SIM received.
Success	Total number of EAP SIM connections succeeded.
Request	Total number of EAP SIM requested.
Failure	Total number of EAP SIM requests failed.
Drop	Total number of EAP SIM requests dropped.
Total Received- TLS	Total number of EAP TLS received.
Success	Total number of EAP TLS connections succeeded.
Request	Total number of EAP TLS requested.
Failure	Total number of EAP TLS requests failed.
Drop	Total number of EAP TLS requests dropped.
Total Received- TTLS	Total number of EAP TTLS received.
Success	Total number of EAP TTLS connections succeeded.
Request	Total number of EAP TTLS requested.
Failure	Total number of EAP TTLS requests failed.
Drop	Total number of EAP TTLS requests dropped.
Total Received- PEAP	Total number of EAP PEAP received.
Success	Total number of EAP PEAP connections succeeded.
Request	Total number of EAP PEAP requested.
Failure	Total number of EAP PEAP requests failed.
Drop	Total number of EAP PEAP requests dropped.
Total Discarded	Total number of EAP server requests discarded
Framed MTU	Total number of framed MTUs sent.
Non-EAP Session Stats	
Attempted	Total number of non-EAP sessions attempted.
AAA Rejects	Total number of non-EAP sessions rejected by AAA server or rejected during AAA auth response parsing in SaMOG (invalid attributes, missing mandatory AVPs etc.)

Field	Description
Pre-authentication Calls	
Success	Total number of non-EAP sessions successfully established during the pre-authentication phase.
Failure	Total number of non-EAP sessions failed to be created during the pre-authentication phase. Possible reasons: internal errors, missing pre-auth phase configs, missing ACL/pool/rulebase etc.
AAA Disconnect with IMSI	Total number of AAA disconnects with IMSI during the pre-authentication phase.
AAA Disconnect without IMSI	Total number of AAA disconnects without IMSI during pre-authentication phase.
AAA Disconnect timeout	Total number of AAA disconnects due to a timeout during the pre-authentication phase.
Authentication & Authorization Calls	
Success	Total number of non-EAP sessions successfully established after UE is authenticated and authorized by AAA (i.e. TAL phase, wherein AAA provides User Identity).
Failure	Total number of non-EAP sessions failed to be created after UE is authenticated and authorized by AAA (i.e. TAL phase, wherein AAA provides User Identity). Possible reasons are network type selection failure, PGW selection failure, multi-device demux failure, internal errors etc.
Abort	Total number of non-EAP sessions aborted specifically due to IPSG demux failure, when multiple devices of same user are connected.
PGW/GGSN Selection Stats	
IP Address	Total number of PGW/GGSN IP addresses resolved during PGW selection.
Hostname	
SNAPTR Procedure	
Success	Total number of Snaptr queries that are successful for the given hostname for PGW selection.
Failure	Total number of Snaptr queries that failed for the given hostname for PGW selection.
APN FQDN	
SNAPTR Procedure	
Success	Total number of Snaptr queries that are successful for given APN FQDN for PGW selection.

Field	Description
Failure	Total number of Snaptr queries that failed for a given APN FQDN for PGW selection
A/AAAA Procedure	
Success	Total number of A/AAAA queries that are successful for given APN FQDN for PGW selection.
Failure	Total number of A/AAAA queries that failed for a given APN FQDN for PGW selection.
Network Access Mode Stats	
Local Offload	Total number of sessions selected for local offload network access mode.
GTPv1	Total number of sessions selected with network access mode as GTPv1.
GTPv2	Total number of sessions selected with network access mode as GTPv2.
PMIP	Total number of sessions selected with network access mode as PMIP.
Local Offload Flow Stats	
GTPv1	Total number of local offload flows with network mode as GTPv1.
GTPv2	Total number of local offload flows with network mode as GTPv2.
PMIP	Total number of local offload flows with network mode as PMIP.
Disconnect Messages Stats	
Disconnect Messages Sent	Total number of disconnect messages sent.
Disconnect Response Received	Total number of disconnect responses received.
Disconnect Response Ack Received	Total number of disconnect response acknowledgement received.
Residual Session Removed	Total number of residual sessions removed.
Disconnect Response Nack Received	Total number of disconnect response acknowledgement received.
Unsupported Attribute	Total number of unsupported attribute.
Missing Attribute	Total number of missing attribute.
NAS Id Mismatch	Total number of mismatch in the NAS ID.
Invalid Request	Total number of invalid requests.
Unsupported Service	Total number of unsupported services.
Unsupported Extension	Total number of unsupported extensions.

Field	Description
Admin Prohibited	Total number of administration prohibited.
Session Context Not Found	Total number of session context not found.
Session Context Not Removable	Total number of session context not removable.
Resource Unavailable	Total number of unavailable resources.
CGW Service Stats	
Subscribers Total	
Active	Total number of active subscribers.
Setup	Total number of subscribers setup.
Released	Total number of subscribers released.
PDNs Total	
Active	Total number of PDN connections active.
Setup	Total number of PDN connections setup.
Released	Total number of PDN connections released.
Rejected	Total number of PDN connections rejected.
PDNs By PDN-Type	
IPv4 PDNs	
Active	Total number of IPv4 PDNs active.
Setup	Total number of IPv4 PDNs connected.
Released	Total number of IPv4 PDNs released.
Rejected	Total number of IPv4 PDNs rejected.
IPv6 PDNs	
Active	Total number of IPv6 PDNs active.
Setup	Total number of IPv6 PDNs connected.
Released	Total number of IPv6 PDNs released.
Rejected	Total number of IPv6 PDNs rejected.
IPv4v6 PDNs	
Active	Total number of IPv4v6 PDNs active.
Setup	Total number of IPv4v6 PDNs connected.

Field	Description
Released	Total number of IPv4v6 PDNs released.
Rejected	Total number of IPv4v6 PDNs rejected.
PDNs By Network-Type	
GTPv1 PDNs	
Active	Total number of current active GTPv1 PDN connections.
Setup	Total number of GTPv1 PDN connections created.
Released	Total number of GTPv1 PDN connections released.
Rejected	Total number of GTPv1 PDN connections rejected.
GTPv2 PDNs	
Active	Total number of current active GTPv2 PDN connections.
Setup	Total number of GTPv2 PDN connections created.
Released	Total number of GTPv2 PDN connections released.
Rejected	Total number of GTPv2 PDN connections rejected.
Gi Redirect PDNs	
Active	Total number of locally offloaded PDN (including Pre-authentication) calls that are currently active.
Setup	Total number of locally offloaded PDN (including Pre-authentication) calls setup on SaMOG after a chassis reboot.
Released	Total number of locally offloaded PDN (including Pre-authentication) calls released by the SaMOG service.
Rejected	Total number of locally offloaded PDN (including Pre-authentication) calls rejected by the SaMOG service.
PDNs Released By Reason	
MAG Ini	Total number of PDN connections released by MAG.
PGW Ini	Total number of PDN connections released by PGW.
DHCP Client Ini	Total number of PDN connections released by DHCP.
GGSN Ini	Total number of PDN connections released by GGSN.
GTPC Path Failure	Total number of PDN connections released because of GTPC path failure.
GTPU Path Failure	Total number of PDN connections released because of GTPU path failure.

Field	Description
GTPU Error Ind	Total number of PDN connections released because of GTPU Error Indication.
Local	Total number of PDN connections released Locally.
Other	Total number of PDN connections released by reason undefined.
PDNs Aborted By Reason	
IP Allocation Failure	Total number of PDN connections aborted due to an IP allocation failure.
Bearer Id Alloc Failure	Total number of PDN connections aborted due to a bearer ID allocation failure.
IPv6 Neighbor Discovery Statistics	
IPv6 RS Received	Total number of IPv6 Router Solicitation messages received.
IPv6 RS Dropped	Total number of IPv6 Router Solicitation messages dropped.
IPv6 RA Sent	Total number of IPv6 Router Advertisement messages sent.
Data Statistics Per Interface	
S2A-GTP Total Data Statistics	
Uplink	
Total Pkts	
IPv4 Pkts(IPv4)	Total number of IPv4 payload packets sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of IPv6 payload packets sent over the IPv4 GTP tunnel towards P-GW.
IPv6 Pkts(IPv4)	Total number of IPv4 payload packets sent over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of IPv6 payload packets sent over the IPv6 GTP tunnel towards P-GW.
Total Bytes	
IPv4 Bytes(IPv4)	Total number of IPv4 payload bytes sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Bytes(IPv6)	Total number of IPv6 payload bytes sent over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of IPv4 payload bytes sent over the IPv6 GTP tunnel towards P-GW.

Field	Description
IPv6 Bytes(IPv6)	Total number of IPv6 payload bytes sent over the IPv6 GTP tunnel towards P-GW.
Dropped Pkts	
IPv4 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were sent over the IPv4 GTP tunnel towards P-GW.
IPv6 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were sent over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were sent over the IPv6 GTP tunnel towards P-GW.
Dropped Bytes	
IPv4 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were sent over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were sent over the IPv6 GTP tunnel towards P-GW.
IPv6 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were sent over the IPv6 GTP tunnel towards P-GW.
Downlink	
Total Pkts	Total number of downlink packets sent on S2a Interface.
IPv4 Pkts(IPv4)	Total number of IPv4 payload packets received over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of IPv6 payload packets received over the IPv4 GTP tunnel towards P-GW.
IPv6 Pkts(IPv4)	Total number of IPv4 payload packets received over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of IPv6 payload packets received over the IPv6 GTP tunnel towards P-GW.
Total Bytes	
IPv4 Bytes(IPv4)	Total number of IPv4 payload bytes received over the IPv4 GTP tunnel towards P-GW.

Field	Description
IPv4 Bytes(IPv6)	Total number of IPv6 payload bytes received over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of IPv4 payload bytes received over the IPv6 GTP tunnel towards P-GW.
IPv6 Bytes(IPv6)	Total number of IPv6 payload bytes received over the IPv6 GTP tunnel towards P-GW.
Dropped Pkts	
IPv4 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were received over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were received over the IPv4 GTP tunnel towards P-GW.
IPv6 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were received over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were received over the IPv6 GTP tunnel towards P-GW.
Dropped Bytes	
IPv4 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were received over the IPv4 GTP tunnel towards P-GW.
IPv4 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were received over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were received over the IPv6 GTP tunnel towards P-GW.
IPv6 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were received over the IPv6 GTP tunnel towards P-GW.
S2A-PMIP Total Data Statistics	
Uplink	
Total Pkts	Total number of Uplink packets sent on S2a PMIP Interface.
Total Bytes	Total number of Uplink bytes sent on S2a PMIP Interface.
Dropped Pkts	Total number of Uplink packets dropped on S2a PMIP Interface.
Dropped Bytes	Total number of Uplink bytes dropped on S2a PMIP Interface.
Downlink	
Total Pkts	Total number of downlink packets sent on S2a PMIP Interface.
Total Bytes	Total number of downlink bytes sent on S2a PMIP Interface.

Field	Description
Dropped Pkts	Total number of downlink packets dropped on S2a PMIP Interface.
Dropped Bytes	Total number of downlink bytes dropped on S2a PMIP Interface.
Gn-U Total Data Statistics	
Uplink	
Total Pkts	Total number of Uplink packets sent on Gn-U Interface.
Total Bytes	Total number of Uplink data bytes sent on Gn-U Interface.
Dropped Pkts	Total number of Uplink packets dropped on Gn-U Interface.
Dropped Bytes	Total number of Uplink data bytes dropped on Gn-U Interface.
Downlink	
Total Pkts	Total number of Downlink packets sent on Gn-U Interface.
Total Bytes	Total number of Downlink data bytes sent on Gn-U Interface.
Dropped Pkts	Total number of Downlink packets dropped on Gn-U Interface.
Dropped Bytes	Total number of Downlink data bytes dropped on Gn-U Interface.
Data Statistics Per PDN-Type	
IPv4 PDNs	
Uplink	
Total Pkts	Total number of uplink packets sent for IPv4 PDNs.
Total Bytes	Total number of uplink bytes sent for IPv4 PDNs.
Downlink	
Total Pkts	Total number of downlink packets sent for IPv4 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv4 PDNs.
IPv6 PDN	
Uplink	
Total Pkts	Total number of uplink packets sent for IPv6 PDNs.
Total Bytes	Total number of uplink bytes sent for IPv6 PDNs.
Downlink	
Total Pkts	Total number of downlink packets sent for IPv6 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv6PDNs.

Field	Description
IPv4v6 PDNs	
Uplink v4	
Total Pkts	Total number of downlink packets sent for IPv4 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv4PDNs.
Downlink v4	
Total Pkts	Total number of downlink packets sent for IPv4 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv4 PDNs.
Uplink v6	
Total Pkts	Total number of downlink packets sent for IPv6 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv6 PDNs.
Downlink v6	
Total Pkts	Total number of downlink packets sent for IPv6 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv6 PDNs.
MIP AAA Authentication	
Attempts	Total number of sessions for MIP authentication attempts.
Success	Total number of successful MIP authentication sessions.
Total Failures	Total number of MIP authentication failures.
Actual Auth Failures	Total number of actual MIP Authentication failures.
Misc Auth Failures	Total number of Miscellaneous MIP Authentication failures.
Binding Updates Received	
Total Received	Total number of PMIPv6 PBUs received.
Total Accepted	Total number of PMIPv6 PBUs accepted.
Total Denied	Total number of PMIPv6 PBUs denied/failed during processing.
Total Discarded	Total number of PMIPv6 PBUs discarded or dropped.
Initial Binding Update Requests	
Received	Total number of initial binding update requests received.
Accepted	Total number of initial binding update requests accepted.
Denied	Total number of initial binding update requests denied.

Field	Description
Refresh Binding Update Requests	
Received	Total number of PMIPv6 PBUs received for renew.
Accepted	Total number of PMIPv6 PBUs for renew accepted.
Denied	Total number of PMIPv6 PBUs for renew denied/failed during processing.
DeReg Requests	
Received	Total number of PMIPv6 PBUs received for Deregistration.
Accepted	Total number of PMIPv6 PBUs for Deregistration accepted.
Denied	Total number of PMIPv6 PBUs for deregistration denied.
Handoff Requests	
Received	Total number of PMIPv6 PBUs received for Handoff.
Accepted	Total number of PMIPv6 PBUs for Handoff accepted.
Denied	Total number of PMIPv6 PBUs for handoff denied.
DHCP Discover Handoff Stats	
Received	Total number of DHCP Discover messages received during handoff.
Accepted	Total number of DHCP Discover messages accepted during handoff.
Denied	Total number of DHCP Discover messages denied during handoff.
Binding Acknowledgements Sent	
Total	Total number of PMIPv6 PBAs sent.
Accepted Reg	Total number of PMIPv6 PBAs sent accepting registrations and renew.
Accepted DeReg	Total number of PMIPv6 Deregistration PBUs accepted sending PBAs.
Denied	Total number of PMIPv6 PBUs denied sending PBAs.
Send Error	Total number of PMIPv6 PBAs failed to send.
Binding Update Deny Reasons	
Insufficient Resource	Total number of PMIPv6 PBUs rejected with insufficient resources.
Mismatched ID	Total number of PMIPv6 PBUs rejected for mismatch in ID.
MN Auth Failure	Total number of PMIPv6 PBUs rejected for MN Authentication failure.
Admin Prohibited	Total number of PMIPv6 PBUs rejected for Administratively Prohibited reason.

Field	Description
Msg ID Required	Total number of PMIPv6 PBUs rejected for Message ID Required.
DAD Failed	Total number of PMIPv6 PBUs rejected for requested Home Address allocation failure.
Not Home Subnet	Total number of PMIPv6 PBUs rejected for address allocation failure from address pool.
Sequence Out Of Window	Total number of PMIPv6 PBUs rejected for incorrect sequence number.
Reg Type Change Disallowed	Total number of PMIPv6 PBUs rejected for renews.
Unspecified Reason	Total number of PMIPv6 PBUs rejected for other reasons.
Service-Authorization Failed	Total number of PMIPv6 PBUs rejected for authorization failure.
Proxy Reg Not Enabled	Total number of PMIPv6 PBUs rejected when proxy registrations are not enabled.
Timestamp Mismatch	Total number of PMIPv6 PBUs rejected when timestamp in PBU is incorrect.
Timestamp Lower Than Expected	Total number of PMIPv6 PBUs rejected when timestamp in PBU is in past.
Missing MN-ID Option	Total number of PMIPv6 PBUs rejected when MN NAI Extension is missing.
Missing HNP Option	Total number of PMIPv6 PBUs rejected when Home Network Prefix Extension is missing.
Missing Access Tech Option	Total number of PMIPv6 PBUs rejected when Access Tech Type Extension is missing.
Missing Handoff Ind Option	Total number of PMIPv6 PBUs rejected when Handoff Indicator is missing.
Not Authorized For HNP	Total number of PMIPv6 PBUs rejected when Requested Home Address Prefix is not authorized.
Not LMA For Mobile	Total number of PMIPv6 PBUs rejected when LMA for Mobile is incorrect.
Not Authorized For Proxy Reg	Total number of PMIPv6 PBUs rejected when Proxy registrations are not allowed.
BCE Prefix Do Not Match	Total number of PMIPv6 PBUs rejected when requested Prefix session is not found.
GRE Key Option Required	Total number of PMIPv6 PBUs rejected when GRE key option is not found.
MCOA Unknown CoA	Total number of PMIPv6 PBUs rejected when Care of Address is incorrect.
Update Denied - Insufficient Resource Reasons	
No Session Manager	Total number of Binding Update Request Denied because of no Session Manager is available.

Field	Description
No Memory	Total number of Binding Update Request Denied because of no Memory available.
Session Manager Rejected	Total number of Binding Update Request Denied because of Session Manager Rejection.
Input-Q Exceeded	Total number of Binding Update Request Denied because of Input queue size is exceeded.
Simul Bindings Exceeded	Total number of Binding Update Request Denied because of number of simultaneous Binding Updates exceeded.
Address Alloc Failed	Total number of Binding Update Request Denied because of address allocation failed.
Update Denied - Admin Prohibited Reasons	
MN-AAA Auth Option Missing	Total number of PMIPv6 PBUs denied due to MN AAA Authentication mobility option missing.
H-bit Not Set	Total number of PMIPv6 PBUs are denied due to H (Home Registration)-Bit not set.
Invalid MN-AAA Option SPI	Total number of PMIPv6 PBUs denied due to invalid MN-AAA Authentication mobility option.
Invalid MN-HA Option SPI	Total number of PMIPv6 PBUs are denied due to invalid MN-HA Authentication mobility option.
Congestion Control Denied	Total number of PMIPv6 PBUs denied due to overload congestion control.
Policy Rejected	Total number of PMIPv6 PBUs are denied due to policy rejection.
HoA Not Authorized	Total number of PMIPv6 PBUs are denied as Home Address is not authorized.
No Permission	Total number of PMIPv6 PBUs denied with no permission.
Bad Request	Total number of PMIPv6 PBUs denied due to bad request.
Binding Updates Discard Reasons	
Congestion Discarded	Total number of PMIPv6 PBUs discarded due to overload congestion.
Checksum Error	Total number of PMIPv6 PBUs discarded due to checksum errors.
Initial Auth Pending	Total number of PMIPv6 PBUs are discarded due to initial authentication pending.
Session Not Found	Total number of PMIPv6 PBU denied and discarded due to session not found.
HAMGR Not Ready	Total number of PMIPv6 PBUs discarded as HAMgr is not ready.

Field	Description
Decode Failure	Total number of PMIPv6 PBUs discarded due to failure to decode.
Invalid Buffer Length	Total number of PMIPv6 PBUs discarded due to invalid buffer length.
Revocation Pending	Total number of PMIPv6 PBUs discarded due to revocation pending for the session.
Binding Revocation	
Sent	Total number of PMIPv6 Binding Revocations sent.
Retries Sent	Total number of PMIPv6 Binding Revocation retries sent.
Ack Rcvd	Total number of PMIPv6 Binding Revocation Ack Messages received.
Not Acknowledged	Total number of PMIPv6 Binding Revocation Ack Timeouts.
Rcvd	Total number of PMIPv6 Binding Revocations received.
Ack Sent	Total number of PMIPv6 Binding Revocation Ack sent.
Sent Revocation Trigger Reasons	
Unspecified	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Unspecified (0).
Administrative Reason	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Administrative Reason (1).
Inter-MAG Handoff-Same ATT	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Inter-MAG Handover - same Access Type (2).
Inter-MAG - Unknown Handoff	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Inter-MAG Handover - Unknown (4).
Inter-MAG Handoff-Diff ATT	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Inter-MAG Handover - different Access Type (3).
Per-Peer Policy	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Per-Peer Policy (128).
Revoking Node Local Policy	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Revoking Mobility Node Local Policy (129).
User Initiated Session Term	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason User-Initiated Session(s) Termination (5).
Access Network Session Term	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Access Network Session(s) Termination (6).
Out-of Sync BCE State	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Possible Out-of-Sync BCE State (7).

Field	Description
Unknown	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason other than defined values.
Received Revocation ACK Status	
Success	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as success (0).
Partial-Success	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as partial success (1).
Binding-Does-Not-Exist	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Binding Does NOT Exist (128).
No IPv4-HoA-Bind	Total number of Binding Revocation Acknowledgements (BRA) received with Status Code as IPv4 Home Address Option Required (129).
Global-Revoc-Not-Authorized	Total number of Binding Revocation Acknowledgements (BRA) received with Status Code as Global Revocation NOT Authorized (130).
Revoc-MN-ID-Required	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revoked Mobile Nodes Identity Required (131).
Revoc-Failed-MN-Attached	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revocation Failed - MN is Attached (132).
Trigger-Not-Supported	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revocation Trigger NOT Supported (133).
Proxy-Bind-Rev-Not-Supported	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Proxy Binding Revocation NOT Supported (135).
Revoc-Func-Not-Supported	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revocation Function NOT Supported (134).
Unknown	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code other than defined values.
Binding Revocation ACK Discarded	
Total	Total number of received Binding Revocation Acknowledgements(BRA) discarded.
Session Not Found	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to corresponding Session Not Found for the BRA.
Badly Formed Request	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Badly Formed message.
Decode Error	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Decode failure.

Field	Description
Checksum Error	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Checksum Error.
Invalid Message Type	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Invalid Message Type.
HAMGR Not Ready	Total number of received Binding Revocation Acknowledgements (BRA) discarded due to HAMGR Not Ready to process requests (recovering).
Matching Request Not Found	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to matching revocation request not found.
Invalid Buffer Length	Total number of received Binding Revocation Acknowledgements (BRA) discarded due to Invalid Buffer Length found while decoding the message.
PMIPv6 Data Statistics	
Tunnel Data Received	
Total Packets	
IPv4 GRE(IPv4)	Total number of IPv4 data packets received on IPv4 GRE tunnel.
IPv4 GRE(IPv6)	Total number of IPv6 data packets received on IPv4 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 data packets received on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 data packets received on IPv6 GRE tunnel.
Total Bytes	
IPv4 GRE(IPv4)	Total bytes of IPv4 bytes received on IPv6 GRE tunnel.
IPv4 GRE(IPv6)	Total bytes of IPv4 bytes received on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 bytes received on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 bytes received on IPv6 GRE tunnel.
Total Errors	
Protocol Type Error	Total number of data packets received on IPv6 GRE tunnel with invalid next header.
Invalid Pkt Length	Total number of data packets received on IPv6 GRE tunnel with invalid length.
No Session Foun	Total number of data packets received on IPv6 GRE tunnel for which binding is not found at SaMOG based on CoA address.
Tunnel Data Sent	
Total Packets	

Field	Description
IPv4 GRE(IPv4)	Total number of IPv4 data packets sent on IPv4 GRE tunnel.
IPv4 GRE(IPv6)	Total number of IPv6 data packets sent on IPv4 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 data packets sent on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 data packets sent on IPv6 GRE tunnel.
Total Bytes	
IPv4 GRE(IPv4)	Total bytes of IPv4 bytes sent on IPv4 GRE tunnel.
IPv4 GRE(IPv6)	Total bytes of IPv6 bytes sent on IPv4 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 bytes sent on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 bytes sent on IPv6 GRE tunnel.
EoGRE Data Statistics	
Tunnel Data Received	
Total Packets	
IPv4 EoGRE(IPv4)	Total number of IPv4 payload packets received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
IPv4 EoGRE(IPv6)	Total number of IPv6 payload packets received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv6 EoGRE(IPv4)	Total number of IPv4 payload packets received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv6 payload packets received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
Total Bytes	
IPv4 EoGRE(IPv4)	Total number of IPv4 payload bytes received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
IPv4 EoGRE(IPv6)	Total number of IPv6 payload bytes received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv6 EoGRE(IPv4)	Total number of IPv4 payload bytes received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv6 payload bytes received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
Total Errors	
Drop Error	Total number of Data Packets dropped on EoGRE Tunnel.

Field	Description
Dest MAC Violation	Total number of destination MAC address in the packet received over the EoGRE tunnel that does not match with SaMOG's virtual MAC, broadcast, or multicast address.
Tunnel Data Sent	
Total Packets	Total number of IPv4 payload packets sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
IPv4 EoGRE(IPv4)	Total number of IPv6 payload packets sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv4 EoGRE(IPv6)	Total number of IPv4 payload packets sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv4)	Total number of IPv6 payload packets sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv4 payload packets sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
Total Bytes	Total number of data bytes sent on the EoGRE tunnel.
IPv4 EoGRE(IPv4)	Total number of IPv4 payload bytes sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
IPv4 EoGRE(IPv6)	Total number of IPv6 payload bytes sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv6 EoGRE(IPv4)	Total number of IPv4 payload bytes sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv6 payload bytes sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)

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

Table 24:

Field	Description
System Statistics	
Active GTPv2 PDNs	Total number of active GTPv2 PDN sessions received.
GTPv2 Sessions	Total number of GTPv2 sessions received.
EAP Session Statistics	
Attempted	Total number of EAP sessions attempted.
Success	Total number of EAP sessions succeeded.

Field	Description
Failure	Total number of failed EAP sessions.
Current	Total number of active EAP sessions.
S2A Statistics	
Create Session Request TX	Total number of Create Session Request sessionstransmitted on S2A interface.
Create Session Response Accept RX	Total number of create session response accept messages received based on S2A interface.
Create Bearer Request RX	Total number of Create bearer Request messages received.
Create Bearer Response Accept TX	Total number of Create Bearer Response Accept sessions transmitted.
Delete Session Request TX	Total number of Delete session requests transmitted.
Delete Session Response Accept RX	Total number of Delete session responses received.
Delete Bearer Request RX	Total number of Delete Bearer request messages received.
Delete Bearer Response Accept TX	Total number of Delete Bearer response messages tansmitted.
Diameter Authentication Statistics	
DER TX	Total number of DER messages transmitted.
DEA Accept RX	Total number of DEA Accept messages received.
RAR RX	Total number of RAR messages received.
RAA TX	Total number of RAA messages transmitted.
ASR RX	Total number of ASA messages received.
ASA TX	Total number of ASA messages transmitted.
STR TX	Total number of STR messages transmitted.
STA RX	Total number of STA messages received.
DHCPv6 Statistics	
IPV6 RA TX	Total number of IPV6 RA messages transmitted.
DHCP Statistics	
DHCP Sessions Active	Total number of active DHCP sessions.
DHCP Sessions Setup	Total number of DHCP sessions set up.
DHCP Sessions Released	Total number of DHCP session released.

Field	Description
DHCP DISCOVER RX	Total number of DHCP discover messages received.
DHCP OFFER TX	Total number of DHCP offer messages transmitted.
DHCP REQUEST RX	Total number of DHCP request messages received.
DHCP ACK TX	Total number of DHCP acknowledgment messages transmitted.
DHCP NAK TX	Total number of DHCP NAK messages transmitted.
RADIUS Accounting Statistics	
Accounting-Request TX	Total number of RADIUS accounting request DHCP messages transmitted.
Accounting-Response RX	Total number of RADIUS accounting response messages reeceived..
Accounting-Start TX	Total number of RADIUS accounting start messages transmitted.
Accounting-Stop TX	Total number of RADIUS accounting stop messsages transmitted.
Accounting-Request Timeout	Total number of RADIUS accounting request messages that are timedout.

show subscribers samog-only full

Table 25: show subscribers samog-only full Command Output Descriptions

Field	Description
EAP-Method	Indicates the Extensible Authentication Protocol (EAP) method. The Possible values are: - EAP-AKA - EAP-SIM - EAP-AKA-PRIME - EAP-TLS - EAP-TTLS - EAP-PEAP **Note** The EAP-Method already displays EAP-AKA, EAP-SIM, EAP-AKA-PRIME. Now this show command is extended to display EAP-TLS, EAP-TTLS, EAP-PEAP.

Bulk Statistics

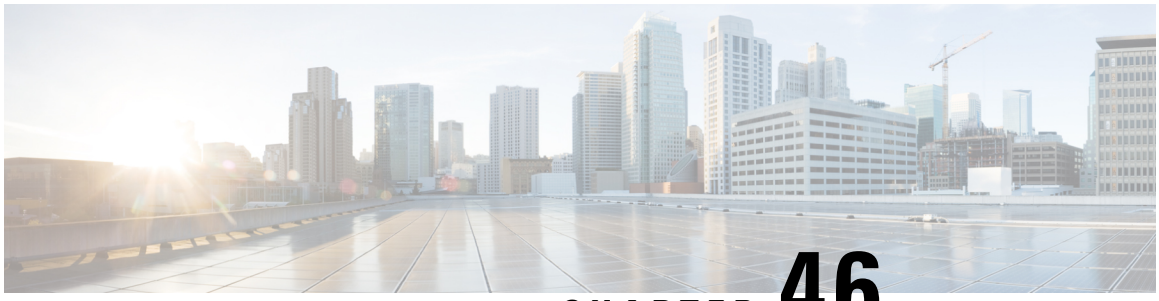
The following bulk statistics are added to the SaMOG schema as part of this feature:

SaMOG Schema

Table 26: Bulk Statistics Varibales in the SaMOG Schema

Variables	Description
mrme-eap-rxmobile-eap-tls	Total number of EAP TLS received.
mrme-eap-rxmobile-eap-ttls	Total number of EAP TTLS received.
mrme-eap-rxmobile-eap-peap	Total number of EAP PEAP received.
mrme-eap-rxmobile-eap-aka-total-rcvd	Total number of EAP-AKA received.
mrme-eap-rxmobile-eap-aka-success	Total number of EAP-AKA connections succeeded.
mrme-eap-rxmobile-eap-aka-challenge	Total number of EAP-AKA challenges received.
mrme-eap-rxmobile-eap-aka-failure-rcvd	Total number of EAP AKA requests failed.
mrme-eap-rxmobile-eap-aka-msgs-from-svr-discarded	Total number of EAP-AKA messages from server that are discarded.
mrme-eap-rxmobile-eap-aka-prime-total-rcvd	Total number of EAP-AKA' received.
mrme-eap-rxmobile-eap-aka-prime-success	Total number of EAP-AKA' connections succeeded.
mrme-eap-rxmobile-eap-aka-prime-challenge	Total number of EAP-AKA' challenges received.
mrme-eap-rxmobile-eap-aka-prime-failure-rcvd	Total number of EAP AKA' requests failed.
mrme-eap-rxmobile-eap-aka-prime-msgs-from-svr-discarded	Total number of EAP-AKA' messages from server that are discarded.
mrme-eap-rxmobile-eap-sim-total-rcvd	Total number of EAP-SIM received.
mrme-eap-rxmobile-eap-sim-success	Total number of EAP-SIM connections succeeded.
mrme-eap-rxmobile-eap-sim-challenge	Total number of EAP-SIM challenges received.
mrme-eap-rxmobile-eap-sim-failure-rcvd	Total number of EAP SIM requests failed.
mrme-eap-rxmobile-eap-sim-msgs-from-svr-discarded	Total number of EAP-SIM messages from server that are discarded.
mrme-eap-rxmobile-eap-tls-total-rcvd	Total number of EAP-TLS received.
mrme-eap-rxmobile-eap-tls-success	Total number of EAP-TLS connections succeeded.
mrme-eap-rxmobile-eap-tls-challenge	Total number of EAP-TLS challenges received.
mrme-eap-rxmobile-eap-tls-failure-rcvd	Total number of EAP TLS requests failed.
mrme-eap-rxmobile-eap-tls-msgs-from-svr-discarded	Total number of EAP-TLS messages from server that are discarded.

Variables	Description
mrme-eap-rxmobile-eap-ttls-total-rcvd	Total number of EAP-TTLS received.
mrme-eap-rxmobile-eap-ttls-success	Total number of EAP-TTLS connections succeeded.
mrme-eap-rxmobile-eap-ttls-challenge	Total number of EAP-TTLS challenges received.
mrme-eap-rxmobile-eap-ttls-failure-rcvd	Total number of EAP TTLS requests failed.
mrme-eap-rxmobile-eap-ttls-msgs-from-svr-discarded	Total number of EAP-TLS messages from server that are discarded.
mrme-eap-rxmobile-eap-peap-total-rcvd	Total number of EAP-PEAP received.
mrme-eap-rxmobile-eap-peap-success	Total number of EAP-PEAP connections succeeded.
mrme-eap-rxmobile-eap-peap-challenge	Total number of EAP-PEAP challenges received.
mrme-eap-rxmobile-eap-peap-failure-rcvd	Total number of EAP PEAP requests failed.
mrme-eap-rxmobile-eap-peap-msgs-from-svr-discarded	Total number of EAP-PEAP messages from server that are discarded.



CHAPTER 46

Support for DH group 5 Encryption under IKESA and IPSEC Transform Set

Feature Summary and Revision History

Summary Data

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

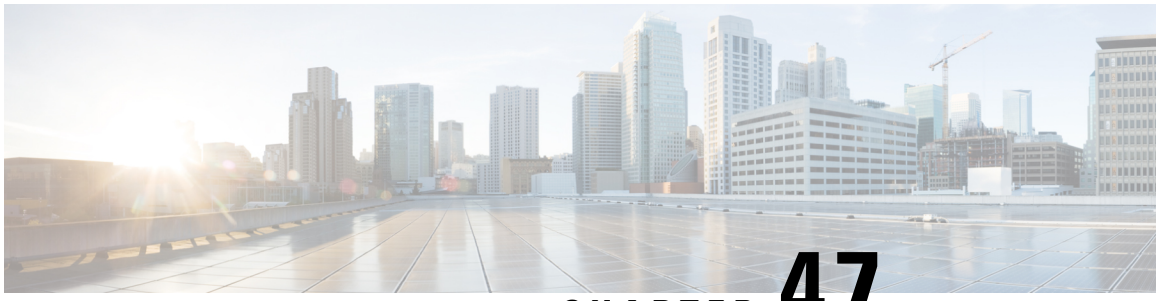
Revision History

Revision Details	**Release**
ePDG supports Default DH group in non-trusted builds.	21.28.m7
ePDG supports Default DH group in trusted builds.	21.28.m5
First introduced.	21.17.12

Feature Changes

In earlier StarOS releases to be in compliant with network security, DH group 5 algorithm was identified as deprecated one and removed for trusted builds from 21.12.x onwards. In the StarOS 21.17.12 release, to support VoWiFi services for IPhone subscribers, ePDG supports DH group 5 algorithm for trusted builds and this DH group 5 algorithm can be configured under both IKESA and IPSEC transform set.

In the StarOS 21.28.5 and later releases, the default DH group for trusted builds in the **ikesa transform-set** is set as group 14. However, only in StarOS 21.28.5 and 21.28.m7 releases, the depreciated DH group 5 is available to configure as non-default configuration.



CHAPTER 47

Subscriber Session Continuation at SaMOG During Wi-Fi Frequency Band Change

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Support is added for the Subscriber session continuation during the Wi-Fi fequency band change.	21.28

Feature Description

SaMOG must continue with the existing subscriber session while accounting stop and accounting start originates in the same Access Point during Wi-Fi frequency band change. Subscriber session has to continue so that intra RG handover occurs seamlessly during Wi-Fi frequency band change and the existing subscriber session continues.

Limitations

The Subscriber Session Continuation at SaMOG during Wi-Fi Freqency Band Change feature has the following limitations:

- Supports only EoGRE Access-Type . IP Access-Type is not supported.
- Supports only Radius Access-Request trigger type. DHCP, PMIP, and Accounting-based trigger types are not supported.
- Support is limited to GTPv2 based s2a interface.

Monitoring and Troubleshooting

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

Show Commands and Output

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

show samog-service statistics

Table 27: show samog-service statistics

Field	Description
SaMOG Statistics for all services	
MRME Service Stats	
Session Stats	
Total Attempted	Total number of sessions attempted.
Total Setup	Total number of sessions setup.
Total Current	Total number of sessions that are currently active.
Total Released	Total number of sessions released

Field	Description
Total Aborted	Total number of sessions aborted.
Total Disconnected	
Disconnected locally	Total number of sessions that were disconnected locally.
Disconnected by UE	Total number of sessions that were disconnected by the UE.
Disconnected by NAS	Total number of sessions that were disconnected by NAS.
Disconnected by CGW	Total number of sessions that were disconnected CGW.
Disconnected by AAA	Total number of sessions that were disconnected by AAA.
Radius Message Stats	
Total Start Req rcvd	Total number of RADIUS start request message received.
Total Start Req (Retransmitted) rcvd	Total number of RADIUS retransmitted start request message received.
Total Start Rsp sent	Total number of RADIUS start response message sent.
Total Interim Updt rcvd	Total number of RADIUS interim update received.
Total Interim Updt (Retransmitted) rcvd	Total number of RADIUS retransmitted interim update received.
Total Interim Updt Rsp sent	Total number of RADIUS interim update response sent.
Total Stop Req rcvd	Total number of RADIUS stop request message received.
Total Stop Req (Retransmitted) rcvd	Total number of RADIUS retransmitted stop request message received.
Total Stop Rsp sent	Total number of RADIUS stop response sent.
Total Accounting On rcvd	Total number of accounting on message received.
Total Accounting Off rcvd	Total number of accounting off message received.
Total Access Req rcvd	Total number of access request message received.
Total Access Req (Retransmitted) rcvd	Total number of retransmitted access request message received.
Total Access Challenge sent	Total number of Access Challenge message sent.
Total Access Accept sent	Total number of Access Accept sent due to congestion policy.
Total Access Reject sent	Total number of Access Rejected sent due to congestion policy.
Congestion control policy applied	
Total Unknown Req rcvd	Total number of unknown requests received for congestion control policy.

Field	Description
Total Send Failure	Total number of congestion control policy sent that failed.
Total Discarded	Total number of congestion control policy discarded.
Mandatory Attr Missing	Total number of missing mandatory attributes.
Start For Non-Existing Session	Total number of start messages sent to non-existing sessions.
Interim For Non-Existing Session	Total number of interim messages sent to non-existing sessions.
Stop For Non-Existing Session	Total number of stop messages sent to non-existing sessions.
Unknown Client	Total number of unknown client.
Invalid Authenticator	Total number of authenticators that is invalid
Stale Packets	Total number of stale packets.
Service Not Supported	Total number of services that are not supported.
No Resource	Total number of resources that are not available.
Internal Error	Total number of internal errors that occurred.
License Limit Exceeded	Total number of license limit exceeded.
Service Limit Exceeded	Total number of license limit exceeded.
Invalid Length	Total number of call control profiles with invalid length.
Invalid EAP	Total number of call control profiles with invalid EAP.
Pending Server Response	Total number of call control profiles with server response pending.
Congestion control policy applied	Total number of congestion control policies applied.
No Policy Match	Total number of Access-Requests dropped due to non-availability of matching PLMN based local policy.
DHCP Message Stats	
DHCP Messages Discarded	Total number of DHCP messages discarded.
Max Size Exceeded	Total number of DHCP messages discarded due to the maximum size exceeded.
Non-Existing Session	Total number of DHCP messages discarded due to a non-existing session.
GiAddr Mismatch	Total number of DHCP messages due to a Gi address mismatch.
Unsupported HW Type or Length	Total number of DHCP messages due to an unsupported hardware type or length.
Stale Packets	Total number of DHCP messages discarded due to stale packets.

Field	Description
Service Not Supported	Total number of DHCP messages discarded due to an unsupported service.
Reauthorization Stats	
Attempts	Total number of reauthorization attempts.
Success	Total number of reauthorization succeeded.
Failure	Total number of reauthorization failure.
Reauthentication Stats	
Attempts	Total number of reauthentication attempts.
Success	Total number of reauthentication succeeded.
Failure	Total number of reauthentication failure.
Handoff Stats	
With Authentication	
Attempts	Total number of sessions attempted for handoff using authentication mechanism.
Success	Total number of sessions with successful handoff using authentication mechanism.
Failure	Total number of handoff failure sessions using authentication mechanism.
With Accounting Start	
Attempts	Total number of sessions attempted for handoff using accounting mechanism.
Success	Total number of sessions with successful handoff using accounting mechanism.
Failure	Total number of sessions with handoff failure using accounting mechanism.
With Accounting Interim	
Attempts	Total number of sessions attempted for handoff using accounting interim mechanism.
Success	Total number of sessions with successful handoff using accounting interim mechanism.
Failure	Total number of sessions with handoff failure using accounting inerim mechanism.
DHCP to DHCP Handoff Statistics	
Received	Total number of DHCP to DHCP handoff statistics received.

Field	Description
Accepted	Total number of DHCP to DHCP handoff statistics accepted.
Denied	Total number of DHCP to DHCP handoff statistics denied.
EAP Client Stats	
Initial Identity Msgs	
NAI Formats	
Root NAI	Total number of UE Identity that uses the root NAI format.
Decorated NAI	Total number of UE Identity that uses the decorated NAI format.
UE Identity formats	
IMSI Identity	Total number of UE Identity that uses an IMSI identity.
Fast Reauth	Total number of UE Identity that uses the fast reauth NAI format.
Pseudonym	Total number of UE Identity that uses the pseudonym NAI format.
Emergency	Total number of UE Identity that uses the emergency NAI format.
Unknown NAI	Total number of UE Identity that uses an NAI format that is unknown.
EAP type	
EAP-AKA	Total number of Extensible Authentication Protocol AKA.
EAP-SIM	Total number of Extensible Authentication Protocol SIM.
EAP-AKA'	Total number of Extensible Authentication Protocol AKA'.
EAP-TLS	Total number of Extensible Authentication Protocol TLS.
EAP-TTLS	Total number of Extensible Authentication Protocol TTLS.
EAP-PEAP	Total number of Extensible Authentication Protocol PEAP.
EAP Unsupported	Total number of Extensible Authentication Protocol that is unsupported. **Important** This counter has been removed in Release 18 and later.
EAP Other	Total number of Extensible Authentication Protocol MSCHAPv2/other. Total number of Extensible Authentication Protocol EAP-TLS or EAP-TTLS/MSCHAPv2.
Initial Non-Identity Msgs	
Total Requested	Total number of initial non-identity messages requested.
Total Rejected	Total number of initial non-identity messages rejected.

Field	Description
Invalid Len	Total number of initial non-identity messages with invalid length.
Invalid Code	Total number of initial non-identity messages with invalid code.
Id Mismatch	Total number of initial non-identity messages with ID mismatch.
Invalid NAI	Total number of initial non-identity messages with invalid NAI.
Invalid IMSI	Total number of initial non-identity messages with invalid IMSI number.
Total Dropped	Total number of initial non-identity messages that were dropped.
Invalid code	Total number of initial non-identity messages with invalid code.
EAP Server Stats	
Total Sent	Total number of EAP server status sent.
Total Received	Total number of EAP server status received.
Success	Total number of EAP server connections succeeded.
Request	Total number of EAP server requests sent.
Failure	Total number of EAP server requests failed.
Drop	Total number of EAP server requests dropped.
Total Received- AKA	Total number of EAP AKA received.
Success	Total number of EAP AKA connections succeeded.
Request	Total number of EAP AKA requested.
Failure	Total number of EAP AKA requests failed.
Drop	Total number of EAP AKA requests dropped.
Total Received- AKA'	Total number of EAP AKA' received.
Success	Total number of EAP AKA' connections succeeded.
Request	Total number of EAP AKA' requested.
Failure	Total number of EAP AKA' requests failed.
Drop	Total number of EAP AKA' requests dropped.
Total Received- SIM	Total number of EAP SIM received.
Success	Total number of EAP SIM connections succeeded.
Request	Total number of EAP SIM requested.
Failure	Total number of EAP SIM requests failed.

Field	Description
Drop	Total number of EAP SIM requests dropped.
Total Received- TLS	Total number of EAP TLS received.
Success	Total number of EAP TLS connections succeeded.
Request	Total number of EAP TLS requested.
Failure	Total number of EAP TLS requests failed.
Drop	Total number of EAP TLS requests dropped.
Total Received- TTLS	Total number of EAP TTLS received.
Success	Total number of EAP TTLS connections succeeded.
Request	Total number of EAP TTLS requested.
Failure	Total number of EAP TTLS requests failed.
Drop	Total number of EAP TTLS requests dropped.
Total Received- PEAP	Total number of EAP PEAP received.
Success	Total number of EAP PEAP connections succeeded.
Request	Total number of EAP PEAP requested.
Failure	Total number of EAP PEAP requests failed.
Drop	Total number of EAP PEAP requests dropped.
Total Discarded	Total number of EAP server requests discarded
Framed MTU	Total number of framed MTUs sent.
Non-EAP Session Stats	
Attempted	Total number of non-EAP sessions attempted.
AAA Rejects	Total number of non-EAP sessions rejected by AAA server or rejected during AAA auth response parsing in SaMOG (invalid attributes, missing mandatory AVPs etc.)
Pre-authentication Calls	
Success	Total number of non-EAP sessions successfully established during the pre-authentication phase.
Failure	Total number of non-EAP sessions failed to be created during the pre-authentication phase. Possible reasons: internal errors, missing pre-auth phase configs, missing ACL/pool/rulebase etc.

Field	Description
AAA Disconnect with IMSI	Total number of AAA disconnects with IMSI during the pre-authentication phase.
AAA Disconnect without IMSI	Total number of AAA disconnects without IMSI during pre-authentication phase.
AAA Disconnect timeout	Total number of AAA disconnects due to a timeout during the pre-authentication phase.
Authentication & Authorization Calls	
Success	Total number of non-EAP sessions successfully established after UE is authenticated and authorized by AAA (i.e. TAL phase, wherein AAA provides User Identity).
Failure	Total number of non-EAP sessions failed to be created after UE is authenticated and authorized by AAA (i.e. TAL phase, wherein AAA provides User Identity). Possible reasons are network type selection failure, PGW selection failure, multi-device demux failure, internal errors etc.
Abort	Total number of non-EAP sessions aborted specifically due to IPSG demux failure, when multiple devices of same user are connected.
PGW/GGSN Selection Stats	
IP Address	Total number of PGW/GGSN IP addresses resolved during PGW selection.
Hostname	
SNAPTR Procedure	
Success	Total number of Snaptr queries that are successful for the given hostname for PGW selection.
Failure	Total number of Snaptr queries that failed for the given hostname for PGW selection.
APN FQDN	
SNAPTR Procedure	
Success	Total number of Snaptr queries that are successful for given APN FQDN for PGW selection.
Failure	Total number of Snaptr queries that failed for a given APN FQDN for PGW selection
A/AAAA Procedure	
Success	Total number of A/AAAA queries that are successful for given APN FQDN for PGW selection.

Field	Description
Failure	Total number of A/AAAA queries that failed for a given APN FQDN for PGW selection.
Network Access Mode Stats	
Local Offload	Total number of sessions selected for local offload network access mode.
GTPv1	Total number of sessions selected with network access mode as GTPv1.
GTPv2	Total number of sessions selected with network access mode as GTPv2.
PMIP	Total number of sessions selected with network access mode as PMIP.
Local Offload Flow Stats	
GTPv1	Total number of local offload flows with network mode as GTPv1.
GTPv2	Total number of local offload flows with network mode as GTPv2.
PMIP	Total number of local offload flows with network mode as PMIP.
Disconnect Messages Stats	
Disconnect Messages Sent	Total number of disconnect messages sent.
Disconnect Response Received	Total number of disconnect responses received.
Disconnect Response Ack Received	Total number of disconnect response acknowledgement received.
Residual Session Removed	Total number of residual sessions removed.
Disconnect Response Nack Received	Total number of disconnect response acknowledgement received.
Unsupported Attribute	Total number of unsupported attribute.
Missing Attribute	Total number of missing attribute.
NAS Id Mismatch	Total number of mismatch in the NAS ID.
Invalid Request	Total number of invalid requests.
Unsupported Service	Total number of unsupported services.
Unsupported Extension	Total number of unsupported extensions.
Admin Prohibited	Total number of administration prohibited.
Session Context Not Found	Total number of session context not found.
Session Context Not Removable	Total number of session context not removable.
Resource Unavailable	Total number of unavailable resources.
CGW Service Stats	

Field	Description
Subscribers Total	
Active	Total number of active subscribers.
Setup	Total number of subscribers setup.
Released	Total number of subscribers released.
PDNs Total	
Active	Total number of PDN connections active.
Setup	Total number of PDN connections setup.
Released	Total number of PDN connections released.
Rejected	Total number of PDN connections rejected.
PDNs By PDN-Type	
IPv4 PDNs	
Active	Total number of IPv4 PDNs active.
Setup	Total number of IPv4 PDNs connected.
Released	Total number of IPv4 PDNs released.
Rejected	Total number of IPv4 PDNs rejected.
IPv6 PDNs	
Active	Total number of IPv6 PDNs active.
Setup	Total number of IPv6 PDNs connected.
Released	Total number of IPv6 PDNs released.
Rejected	Total number of IPv6 PDNs rejected.
IPv4v6 PDNs	
Active	Total number of IPv4v6 PDNs active.
Setup	Total number of IPv4v6 PDNs connected.
Released	Total number of IPv4v6 PDNs released.
Rejected	Total number of IPv4v6 PDNs rejected.
PDNs By Network-Type	
GTPv1 PDNs	
Active	Total number of current active GTPv1 PDN connections.

Field	Description
Setup	Total number of GTPv1 PDN connections created.
Released	Total number of GTPv1 PDN connections released.
Rejected	Total number of GTPv1 PDN connections rejected.
GTPv2 PDNs	
Active	Total number of current active GTPv2 PDN connections.
Setup	Total number of GTPv2 PDN connections created.
Released	Total number of GTPv2 PDN connections released.
Rejected	Total number of GTPv2 PDN connections rejected.
Gi Redirect PDNs	
Active	Total number of locally offloaded PDN (including Pre-authentication) calls that are currently active.
Setup	Total number of locally offloaded PDN (including Pre-authentication) calls setup on SaMOG after a chassis reboot.
Released	Total number of locally offloaded PDN (including Pre-authentication) calls released by the SaMOG service.
Rejected	Total number of locally offloaded PDN (including Pre-authentication) calls rejected by the SaMOG service.
PDNs Released By Reason	
MAG Ini	Total number of PDN connections released by MAG.
PGW Ini	Total number of PDN connections released by PGW.
DHCP Client Ini	Total number of PDN connections released by DHCP.
GGSN Ini	Total number of PDN connections released by GGSN.
GTPC Path Failure	Total number of PDN connections released because of GTPC path failure.
GTPU Path Failure	Total number of PDN connections released because of GTPU path failure.
GTPU Error Ind	Total number of PDN connections released because of GTPU Error Indication.
Local	Total number of PDN connections released Locally.
Other	Total number of PDN connections released by reason undefined.
PDNs Aborted By Reason	
IP Allocation Failure	Total number of PDN connections aborted due to an IP allocation failure.

Field	Description
Bearer Id Alloc Failure	Total number of PDN connections aborted due to a bearer ID allocation failure.
IPv6 Neighbor Discovery Statistics	
IPv6 RS Received	Total number of IPv6 Router Solicitation messages received.
IPv6 RS Dropped	Total number of IPv6 Router Solicitation messages dropped.
IPv6 RA Sent	Total number of IPv6 Router Advertisement messages sent.
Data Statistics Per Interface	
S2A-GTP Total Data Statistics	
Uplink	
Total Pkts	
IPv4 Pkts(IPv4)	Total number of IPv4 payload packets sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of IPv6 payload packets sent over the IPv4 GTP tunnel towards P-GW.
IPv6 Pkts(IPv4)	Total number of IPv4 payload packets sent over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of IPv6 payload packets sent over the IPv6 GTP tunnel towards P-GW.
Total Bytes	
IPv4 Bytes(IPv4)	Total number of IPv4 payload bytes sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Bytes(IPv6)	Total number of IPv6 payload bytes sent over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of IPv4 payload bytes sent over the IPv6 GTP tunnel towards P-GW.
IPv6 Bytes(IPv6)	Total number of IPv6 payload bytes sent over the IPv6 GTP tunnel towards P-GW.
Dropped Pkts	
IPv4 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were sent over the IPv4 GTP tunnel towards P-GW.

Field	Description
IPv6 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were sent over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were sent over the IPv6 GTP tunnel towards P-GW.
Dropped Bytes	
IPv4 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were sent over the IPv4 GTP tunnel towards P-GW.
IPv4 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were sent over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were sent over the IPv6 GTP tunnel towards P-GW.
IPv6 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were sent over the IPv6 GTP tunnel towards P-GW.
Downlink	
Total Pkts	Total number of downlink packets sent on S2a Interface.
IPv4 Pkts(IPv4)	Total number of IPv4 payload packets received over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of IPv6 payload packets received over the IPv4 GTP tunnel towards P-GW.
IPv6 Pkts(IPv4)	Total number of IPv4 payload packets received over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of IPv6 payload packets received over the IPv6 GTP tunnel towards P-GW.
Total Bytes	
IPv4 Bytes(IPv4)	Total number of IPv4 payload bytes received over the IPv4 GTP tunnel towards P-GW.
IPv4 Bytes(IPv6)	Total number of IPv6 payload bytes received over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of IPv4 payload bytes received over the IPv6 GTP tunnel towards P-GW.
IPv6 Bytes(IPv6)	Total number of IPv6 payload bytes received over the IPv6 GTP tunnel towards P-GW.
Dropped Pkts	

Field	Description
IPv4 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were received over the IPv4 GTP tunnel towards P-GW.
IPv4 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were received over the IPv4 GTP tunnel towards P-GW.
IPv6 Pkts(IPv4)	Total number of dropped IPv4 payload packets that were received over the IPv6 GTP tunnel towards P-GW.
IPv6 Pkts(IPv6)	Total number of dropped IPv6 payload packets that were received over the IPv6 GTP tunnel towards P-GW.
Dropped Bytes	
IPv4 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were received over the IPv4 GTP tunnel towards P-GW.
IPv4 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were received over the IPv4 GTP tunnel towards P-GW.
IPv6 Bytes(IPv4)	Total number of dropped IPv4 payload bytes that were received over the IPv6 GTP tunnel towards P-GW.
IPv6 Bytes(IPv6)	Total number of dropped IPv6 payload bytes that were received over the IPv6 GTP tunnel towards P-GW.
S2A-PMIP Total Data Statistics	
Uplink	
Total Pkts	Total number of Uplink packets sent on S2a PMIP Interface.
Total Bytes	Total number of Uplink bytes sent on S2a PMIP Interface.
Dropped Pkts	Total number of Uplink packets dropped on S2a PMIP Interface.
Dropped Bytes	Total number of Uplink bytes dropped on S2a PMIP Interface.
Downlink	
Total Pkts	Total number of downlink packets sent on S2a PMIP Interface.
Total Bytes	Total number of downlink bytes sent on S2a PMIP Interface.
Dropped Pkts	Total number of downlink packets dropped on S2a PMIP Interface.
Dropped Bytes	Total number of downlink bytes dropped on S2a PMIP Interface.
Gn-U Total Data Statistics	
Uplink	
Total Pkts	Total number of Uplink packets sent on Gn-U Interface.

Field	Description
Total Bytes	Total number of Uplink data bytes sent on Gn-U Interface.
Dropped Pkts	Total number of Uplink packets dropped on Gn-U Interface.
Dropped Bytes	Total number of Uplink data bytes dropped on Gn-U Interface.
Downlink	
Total Pkts	Total number of Downlink packets sent on Gn-U Interface.
Total Bytes	Total number of Downlink data bytes sent on Gn-U Interface.
Dropped Pkts	Total number of Downlink packets dropped on Gn-U Interface.
Dropped Bytes	Total number of Downlink data bytes dropped on Gn-U Interface.
Data Statistics Per PDN-Type	
IPv4 PDNs	
Uplink	
Total Pkts	Total number of uplink packets sent for IPv4 PDNs.
Total Bytes	Total number of uplink bytes sent for IPv4 PDNs.
Downlink	
Total Pkts	Total number of downlink packets sent for IPv4 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv4 PDNs.
IPv6 PDN	
Uplink	
Total Pkts	Total number of uplink packets sent for IPv6 PDNs.
Total Bytes	Total number of uplink bytes sent for IPv6 PDNs.
Downlink	
Total Pkts	Total number of downlink packets sent for IPv6 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv6PDNs.
IPv4v6 PDNs	
Uplink v4	
Total Pkts	Total number of downlink packets sent for IPv4 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv4PDNs.
Downlink v4	

Field	Description
Total Pkts	Total number of downlink packets sent for IPv4 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv4 PDNs.
Uplink v6	
Total Pkts	Total number of downlink packets sent for IPv6 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv6 PDNs.
Downlink v6	
Total Pkts	Total number of downlink packets sent for IPv6 PDNs.
Total Bytes	Total number of downlink bytes sent for IPv6 PDNs.
MIP AAA Authentication	
Attempts	Total number of sessions for MIP authentication attempts.
Success	Total number of successful MIP authentication sessions.
Total Failures	Total number of MIP authentication failures.
Actual Auth Failures	Total number of actual MIP Authentication failures.
Misc Auth Failures	Total number of Miscellaneous MIP Authentication failures.
Binding Updates Received	
Total Received	Total number of PMIPv6 PBUs received.
Total Accepted	Total number of PMIPv6 PBUs accepted.
Total Denied	Total number of PMIPv6 PBUs denied/failed during processing.
Total Discarded	Total number of PMIPv6 PBUs discarded or dropped.
Initial Binding Update Requests	
Received	Total number of initial binding update requests received.
Accepted	Total number of initial binding update requests accepted.
Denied	Total number of initial binding update requests denied.
Refresh Binding Update Requests	
Received	Total number of PMIPv6 PBUs received for renew.
Accepted	Total number of PMIPv6 PBUs for renew accepted.
Denied	Total number of PMIPv6 PBUs for renew denied/failed during processing.
DeReg Requests	

Field	Description
Received	Total number of PMIPv6 PBUs received for Deregistration.
Accepted	Total number of PMIPv6 PBUs for Deregistration accepted.
Denied	Total number of PMIPv6 PBUs for deregistration denied.
Handoff Requests	
Received	Total number of PMIPv6 PBUs received for Handoff.
Accepted	Total number of PMIPv6 PBUs for Handoff accepted.
Denied	Total number of PMIPv6 PBUs for handoff denied.
DHCP Discover Handoff Stats	
Received	Total number of DHCP Discover messages received during handoff.
Accepted	Total number of DHCP Discover messages accepted during handoff.
Denied	Total number of DHCP Discover messages denied during handoff.
Binding Acknowledgements Sent	
Total	Total number of PMIPv6 PBAs sent.
Accepted Reg	Total number of PMIPv6 PBAs sent accepting registrations and renew.
Accepted DeReg	Total number of PMIPv6 Deregistration PBUs accepted sending PBAs.
Denied	Total number of PMIPv6 PBUs denied sending PBAs.
Send Error	Total number of PMIPv6 PBAs failed to send.
Binding Update Deny Reasons	
Insufficient Resource	Total number of PMIPv6 PBUs rejected with insufficient resources.
Mismatched ID	Total number of PMIPv6 PBUs rejected for mismatch in ID.
MN Auth Failure	Total number of PMIPv6 PBUs rejected for MN Authentication failure.
Admin Prohibited	Total number of PMIPv6 PBUs rejected for Administratively Prohibited reason.
Msg ID Required	Total number of PMIPv6 PBUs rejected for Message ID Required.
DAD Failed	Total number of PMIPv6 PBUs rejected for requested Home Address allocation failure.
Not Home Subnet	Total number of PMIPv6 PBUs rejected for address allocation failure from address pool.
Sequence Out Of Window	Total number of PMIPv6 PBUs rejected for incorrect sequence number.

Field	Description
Reg Type Change Disallowed	Total number of PMIPv6 PBUs rejected for renews.
Unspecified Reason	Total number of PMIPv6 PBUs rejected for other reasons.
Service-Authorization Failed	Total number of PMIPv6 PBUs rejected for authorization failure.
Proxy Reg Not Enabled	Total number of PMIPv6 PBUs rejected when proxy registrations are not enabled.
Timestamp Mismatch	Total number of PMIPv6 PBUs rejected when timestamp in PBU is incorrect.
Timestamp Lower Than Expected	Total number of PMIPv6 PBUs rejected when timestamp in PBU is in past.
Missing MN-ID Option	Total number of PMIPv6 PBUs rejected when MN NAI Extension is missing.
Missing HNP Option	Total number of PMIPv6 PBUs rejected when Home Network Prefix Extension is missing.
Missing Access Tech Option	Total number of PMIPv6 PBUs rejected when Access Tech Type Extension is missing.
Missing Handoff Ind Option	Total number of PMIPv6 PBUs rejected when Handoff Indicator is missing.
Not Authorized For HNP	Total number of PMIPv6 PBUs rejected when Requested Home Address Prefix is not authorized.
Not LMA For Mobile	Total number of PMIPv6 PBUs rejected when LMA for Mobile is incorrect.
Not Authorized For Proxy Reg	Total number of PMIPv6 PBUs rejected when Proxy registrations are not allowed.
BCE Prefix Do Not Match	Total number of PMIPv6 PBUs rejected when requested Prefix session is not found.
GRE Key Option Required	Total number of PMIPv6 PBUs rejected when GRE key option is not found.
MCOA Unknown CoA	Total number of PMIPv6 PBUs rejected when Care of Address is incorrect.
Update Denied - Insufficient Resource Reasons	
No Session Manager	Total number of Binding Update Request Denied because of no Session Manager is available.
No Memory	Total number of Binding Update Request Denied because of no Memory available.
Session Manager Rejected	Total number of Binding Update Request Denied because of Session Manager Rejection.
Input-Q Exceeded	Total number of Binding Update Request Denied because of Input queue size is exceeded.

Field	Description
Simul Bindings Exceeded	Total number of Binding Update Request Denied because of number of simultaneous Binding Updates exceeded.
Address Alloc Failed	Total number of Binding Update Request Denied because of address allocation failed.
Update Denied - Admin Prohibited Reasons	
MN-AAA Auth Option Missing	Total number of PMIPv6 PBUs denied due to MN AAA Authentication mobility option missing.
H-bit Not Set	Total number of PMIPv6 PBUs are denied due to H (Home Registration)-Bit not set.
Invalid MN-AAA Option SPI	Total number of PMIPv6 PBUs denied due to invalid MN-AAA Authentication mobility option.
Invalid MN-HA Option SPI	Total number of PMIPv6 PBUs are denied due to invalid MN-HA Authentication mobility option.
Congestion Control Denied	Total number of PMIPv6 PBUs denied due to overload congestion control.
Policy Rejected	Total number of PMIPv6 PBUs are denied due to policy rejection.
HoA Not Authorized	Total number of PMIPv6 PBUs are denied as Home Address is not authorized.
No Permission	Total number of PMIPv6 PBUs denied with no permission.
Bad Request	Total number of PMIPv6 PBUs denied due to bad request.
Binding Updates Discard Reasons	
Congestion Discarded	Total number of PMIPv6 PBUs discarded due to overload congestion.
Checksum Error	Total number of PMIPv6 PBUs discarded due to checksum errors.
Initial Auth Pending	Total number of PMIPv6 PBUs are discarded due to initial authentication pending.
Session Not Found	Total number of PMIPv6 PBU denied and discarded due to session not found.
HAMGR Not Ready	Total number of PMIPv6 PBUs discarded as HAMgr is not ready.
Decode Failure	Total number of PMIPv6 PBUs discarded due to failure to decode.
Invalid Buffer Length	Total number of PMIPv6 PBUs discarded due to invalid buffer length.
Revocation Pending	Total number of PMIPv6 PBUs discarded due to revocation pending for the session.
Binding Revocation	

Field	Description
Sent	Total number of PMIPv6 Binding Revocations sent.
Retries Sent	Total number of PMIPv6 Binding Revocation retries sent.
Ack Rcvd	Total number of PMIPv6 Binding Revocation Ack Messages received.
Not Acknowledged	Total number of PMIPv6 Binding Revocation Ack Timeouts.
Rcvd	Total number of PMIPv6 Binding Revocations received.
Ack Sent	Total number of PMIPv6 Binding Revocation Ack sent.
Sent Revocation Trigger Reasons	
Unspecified	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Unspecified (0).
Administrative Reason	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Administrative Reason (1).
Inter-MAG Handoff-Same ATT	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Inter-MAG Handover - same Access Type (2).
Inter-MAG - Unknown Handoff	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Inter-MAG Handover - Unknown (4).
Inter-MAG Handoff-Diff ATT	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Inter-MAG Handover - different Access Type (3).
Per-Peer Policy	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Per-Peer Policy (128).
Revoking Node Local Policy	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Revoking Mobility Node Local Policy (129).
User Initiated Session Term	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason User-Initiated Session(s) Termination (5).
Access Network Session Term	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Access Network Session(s) Termination (6).
Out-of Sync BCE State	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason Possible Out-of-Sync BCE State (7).
Unknown	Total number of Binding Revocation Indications(BRI) sent with Revocation Trigger Reason other than defined values.
Received Revocation ACK Status	
Success	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as success (0).

Field	Description
Partial-Success	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as partial success (1).
Binding-Does-Not-Exist	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Binding Does NOT Exist (128).
No IPv4-HoA-Bind	Total number of Binding Revocation Acknowledgements (BRA) received with Status Code as IPv4 Home Address Option Required (129).
Global-Revoc-Not-Authorized	Total number of Binding Revocation Acknowledgements (BRA) received with Status Code as Global Revocation NOT Authorized (130).
Revoc-MN-ID-Required	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revoked Mobile Nodes Identity Required (131).
Revoc-Failed-MN-Attached	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revocation Failed - MN is Attached (132).
Trigger-Not-Supported	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revocation Trigger NOT Supported (133).
Proxy-Bind-Rev-Not-Supported	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Proxy Binding Revocation NOT Supported (135).
Revoc-Func-Not-Supported	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code as Revocation Function NOT Supported (134).
Unknown	Total number of Binding Revocation Acknowledgements(BRA) received with Status Code other than defined values.
Binding Revocation ACK Discarded	
Total	Total number of received Binding Revocation Acknowledgements(BRA) discarded.
Session Not Found	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to corresponding Session Not Found for the BRA.
Badly Formed Request	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Badly Formed message.
Decode Error	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Decode failure.
Checksum Error	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Checksum Error.
Invalid Message Type	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to Invalid Message Type.
HAMGR Not Ready	Total number of received Binding Revocation Acknowledgements (BRA) discarded due to HAMGR Not Ready to process requests (recovering).

Field	Description
Matching Request Not Found	Total number of received Binding Revocation Acknowledgements(BRA) discarded due to matching revocation request not found.
Invalid Buffer Length	Total number of received Binding Revocation Acknowledgements (BRA) discarded due to Invalid Buffer Length found while decoding the message.
PMIPv6 Data Statistics	
Tunnel Data Received	
Total Packets	
IPv4 GRE(IPv4)	Total number of IPv4 data packets received on IPv4 GRE tunnel.
IPv4 GRE(IPv6)	Total number of IPv6 data packets received on IPv4 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 data packets received on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 data packets received on IPv6 GRE tunnel.
Total Bytes	
IPv4 GRE(IPv4)	Total bytes of IPv4 bytes received on IPv6 GRE tunnel.
IPv4 GRE(IPv6)	Total bytes of IPv4 bytes received on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 bytes received on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 bytes received on IPv6 GRE tunnel.
Total Errors	
Protocol Type Error	Total number of data packets received on IPv6 GRE tunnel with invalid next header.
Invalid Pkt Length	Total number of data packets received on IPv6 GRE tunnel with invalid length.
No Session Foun	Total number of data packets received on IPv6 GRE tunnel for which binding is not found at SaMOG based on CoA address.
Tunnel Data Sent	
Total Packets	
IPv4 GRE(IPv4)	Total number of IPv4 data packets sent on IPv4 GRE tunnel.
IPv4 GRE(IPv6)	Total number of IPv6 data packets sent on IPv4 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 data packets sent on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 data packets sent on IPv6 GRE tunnel.
Total Bytes	

Field	Description
IPv4 GRE(IPv4)	Total bytes of IPv4 bytes sent on IPv4 GRE tunnel.
IPv4 GRE(IPv6)	Total bytes of IPv6 bytes sent on IPv4 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv4 bytes sent on IPv6 GRE tunnel.
IPv6 GRE(IPv4)	Total number of IPv6 bytes sent on IPv6 GRE tunnel.
EoGRE Data Statistics	
Tunnel Data Received	
Total Packets	
IPv4 EoGRE(IPv4)	Total number of IPv4 payload packets received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
IPv4 EoGRE(IPv6)	Total number of IPv6 payload packets received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv6 EoGRE(IPv4)	Total number of IPv4 payload packets received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv6 payload packets received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
Total Bytes	
IPv4 EoGRE(IPv4)	Total number of IPv4 payload bytes received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
IPv4 EoGRE(IPv6)	Total number of IPv6 payload bytes received over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv6 EoGRE(IPv4)	Total number of IPv4 payload bytes received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv6 payload bytes received over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
Total Errors	
Drop Error	Total number of Data Packets dropped on EoGRE Tunnel.
Dest MAC Violation	Total number of destination MAC address in the packet received over the EoGRE tunnel that does not match with SaMOG's virtual MAC, broadcast, or multicast address.
Tunnel Data Sent	
Total Packets	Total number of IPv4 payload packets sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).

Field	Description
IPv4 EoGRE(IPv4)	Total number of IPv6 payload packets sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv4 EoGRE(IPv6)	Total number of IPv4 payload packets sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv4)	Total number of IPv6 payload packets sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv4 payload packets sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
Total Bytes	Total number of data bytes sent on the EoGRE tunnel.
IPv4 EoGRE(IPv4)	Total number of IPv4 payload bytes sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport).
IPv4 EoGRE(IPv6)	Total number of IPv6 payload bytes sent over the IPv4 GRE tunnel (EoGRE tunnel with v4 transport)
IPv6 EoGRE(IPv4)	Total number of IPv4 payload bytes sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)
IPv6 EoGRE(IPv6)	Total number of IPv6 payload bytes sent over the IPv6 GRE tunnel (EoGRE tunnel with v6 transport)

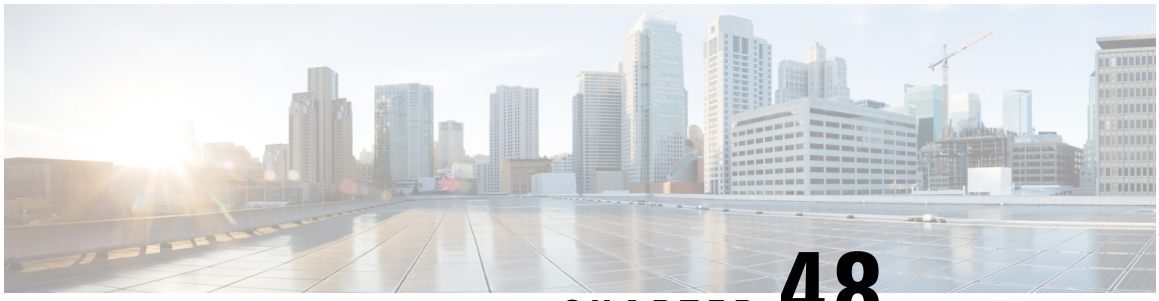
show samog-service statistics plmn mcc <mcc1> mnc <mnc1>

Table 28:

Field	Description
System Statistics	
Active GTPv2 PDNs	Total number of active GTPv2 PDN sessions received.
GTPv2 Sessions	Total number of GTPv2 sessions received.
EAP Session Statistics	
Attempted	Total number of EAP sessions attempted.
Success	Total number of EAP sessions succeeded.
Failure	Total number of failed EAP sessions.
Current	Total number of active EAP sessions.
S2A Statistics	
Create Session Request TX	Total number of Create Session Request sessionstransmitted on S2A interface.

Field	Description
Create Session Response Accept RX	Total number of create session response accept messages received based on S2A interface.
Create Bearer Request RX	Total number of Create bearer Request messages received.
Create Bearer Response Accept TX	Total number of Create Bearer Response Accept sessions transmitted.
Delete Session Request TX	Total number of Delete session requests transmitted.
Delete Session Response Accept RX	Total number of Delete session responses received.
Delete Bearer Request RX	Total number of Delete Bearer request messages received.
Delete Bearer Response Accept TX	Total number of Delete Bearer response messages tansmitted.
Diameter Authentication Statistics	
DER TX	Total number of DER messages transmitted.
DEA Accept RX	Total number of DEA Accept messages received.
RAR RX	Total number of RAR messages received.
RAA TX	Total number of RAA messages transmitted.
ASR RX	Total number of ASA messages received.
ASA TX	Total number of ASA messages transmitted.
STR TX	Total number of STR messages transmitted.
STA RX	Total number of STA messages received.
DHCPv6 Statistics	
IPV6 RA TX	Total number of IPV6 RA messages transmitted.
DHCP Statistics	
DHCP Sessions Active	Total number of active DHCP sessions.
DHCP Sessions Setup	Total number of DHCP sessions set up.
DHCP Sessions Released	Total number of DHCP session released.
DHCP DISCOVER RX	Total number of DHCP discover messages received.
DHCP OFFER TX	Total number of DHCP offer messages transmitted.
DHCP REQUEST RX	Total number of DHCP request messages received.
DHCP ACK TX	Total number of DHCP acknowledgment messages transmitted.
DHCP NAK TX	Total number of DHCP NAK messages transmitted.

Field	Description
RADIUS Accounting Statistics	
Accounting-Request TX	Total number of RADIUS accounting request DHCP messages transmitted.
Accounting-Response RX	Total number of RADIUS accounting response messages reeceived..
Accounting-Start TX	Total number of RADIUS accounting start messages transmitted.
Accounting-Stop TX	Total number of RADIUS accounting stop messsages transmitted.
Accounting-Request Timeout	Total number of RADIUS accounting request messages that are timedout.



CHAPTER 48

TMSI Based NRI Container IE

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* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
TMSI based NRI container IE in LUR message over SGs interface is supported.	21.28

Feature Description

MME supports Temporary Mobile Subscriber Identity (TMSI) based Network Resource Identifier (NRI) container IE in the Location Update Request (LUR) message over SGs interface. The UE sends this IE through the Combined Attach or Tracking Area Update (TAU) Request message. After the IE gets received, it gets parsed, processed, and sent through the SGs interface to the Visitor Location Register (VLR) in the LUR message.

How it Works

UE sends IE value to MME through S1Ap interface. The value is sent either in the Combined Attach or the TAU request. Now, MME sends the value in the LUR message to the VLR.

If UE does not send TMSI based NRI container in the Combined Attach or the TAU Request message, and if MME determines that the serving VLR changed for UE, MME includes the non-broadcasted Location Area Indentifier (LAI) in the old LAI field of the LUR message. Using the below mentioned configurations, the non-broadcasted LAI can be configured, which will be included in LUR message if serving VLR changed for the UE.

Table 29: LUR Content Based on the TMSI Based NRI Container IE Value and Serving VLR Change

Sl. No	IEs present in the Combined Attach or TAU message	MME deducts change in serving VLR	Resultant LUR content	Non-braodcast LAI CLI Content used
1	TMSI-based NRI container IE, old LAI IE	yes	TMSI-based NRI container IE, old LAI	No
		No	TMSI-based NRI container IE, old LAI	No
2	TMSI-based NRI container IE, no old LAI IE	Yes	TMSI-based NRI container IE	No
		No	TMSI-based NRI container IE	No
3	No TMSI-based NRI container IE, old LAI IE	Yes	Non-broadcast LAI For more information, refer the Note.	Yes
		No	Old LAI	No
4	No TMSI-based NRI container IE, no old LAI IE	Yes	Non-broadcast LAI For more information, refer the Note.	Yes
		No	No IE	No

Note Sending the 'Non-broadcast LAI' in Location Update Request (LUR) applies to TAU scenarios where the MME can detect VLR changes. This doesn't apply to attach scenarios because the MME lacks prior VLR context due to detachment.

Configuring NonBroadcast LAI

Use the following configuration to configure nonbroadcast lai.

```
configure
  context context_name
    sgs-service service_name
      [ no ] lai non-bradcast mcc mcc_id mnc mnc_id lac lac_id
  end
```

NOTES:

- **no**: Removes the nonbroadcast LAI configuration.
- **lai non-broadcast**: Specifies the Location Area Identity (LAI), not assigned to any area.
- **mcc** *mcc_id*: Configures the mobile country code (MCC). mcc_id is a 3-digit number between 000 to 999.
- **mnc** *mnc_id*: Configures the mobile network code (MNC). mnc_id is a 2- or 3-digit number between 00 to 999.
- **lac** *lac_id*: Configures the location area code (LAC). lac_id is an integer from 0 to 65535.

Monitoring and Troubleshooting

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

Show Commands and Output

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

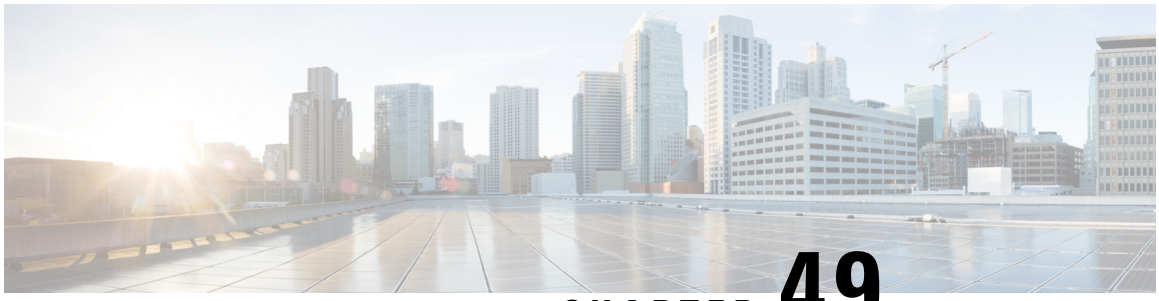
show sgs-service all

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

Table 30: show sgs-service all Command Output Descriptions

Field	Description
Non-Broadcast LAI	

Field	Description
MCC	Displays the configured MCC value.
MNC	Displays the configured MNC value.
LAC	Displays the configured LAC value.



CHAPTER 49

TEID Collision with ULI Change

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
TEID collision with ULI change feature is enhanced to verify only MCC is checked during TEID collision on P-GW, SAEGW, and GGSN services.	21.28.m4
With this release, P-GW and GGSN configuration to reject a Tunnel Endpoint Identifier (TEID) collision request with ULI change feature is supported.	21.6.13

Revision Details	Release
First introduced.	Pre 21.2

Feature Description

During Tunnel Endpoint Identifier (TEID) collision scenario, P-GW or GGSN allocates a TEID to a home subscriber. In case of a stale session, in an S-GW or SGSN, the same TEID that is allocated by P-GW or GGSN, is allocated to a roaming subscriber. Then, S-GW sends BRCmd, DBCmd, and MBR messages to P-GW. SGSN sends the Update PDP Context message to P-GW. Due to the same TEID allocation to both the home subscriber and the roaming subscriber, and P-GW having no information on duplicate TEID allocation, P-GW accepts the request. The duplicate use of same TEID leads to the billing for the home subscriber for the data that is used by the roaming subscriber.

To eliminate this scenario, TEID Collision with User Location Information (ULI) change feature is introduced. With this feature, you can configure P-GW and GGSN to reject a request when TEID collision occurs.

TEID Collisions with ULI change feature allows comparison with only Mobile Country Code (MCC) instead of comparison of mcc+mnc. This functionality supports the MOCN scenario on P-GW, SAEGW, and GGSN.

How It Works

The following section provides an overview of the TEID Collision with ULI change feature.

Architecture

For 4G calls, you can configure the TEID Collision with ULI Change feature through CLI in pgw-service in P-GW. For 3G calls, you can configure this feature through CLI in ggsn-service in GGSN. This feature works in the following way for P-GW and GGSN:

- For a home user equipment (UE) in P-GW, a request is rejected if the mobile country code and mobile network code (mcc_mnc) information in ULI differs from the ULI information available in the session for the UE on P-GW. The request is for one of the following messages:
  - Bearer Resource Command
  - Modify Bearer Request
  - Delete Bearer Command
- For a home UE in GGSN, a request is rejected if the mobile country code and mobile network code information in ULI differs from the ULI information available in the session for the UE on GGSN. The request is for the following message:
  - Update PDP context

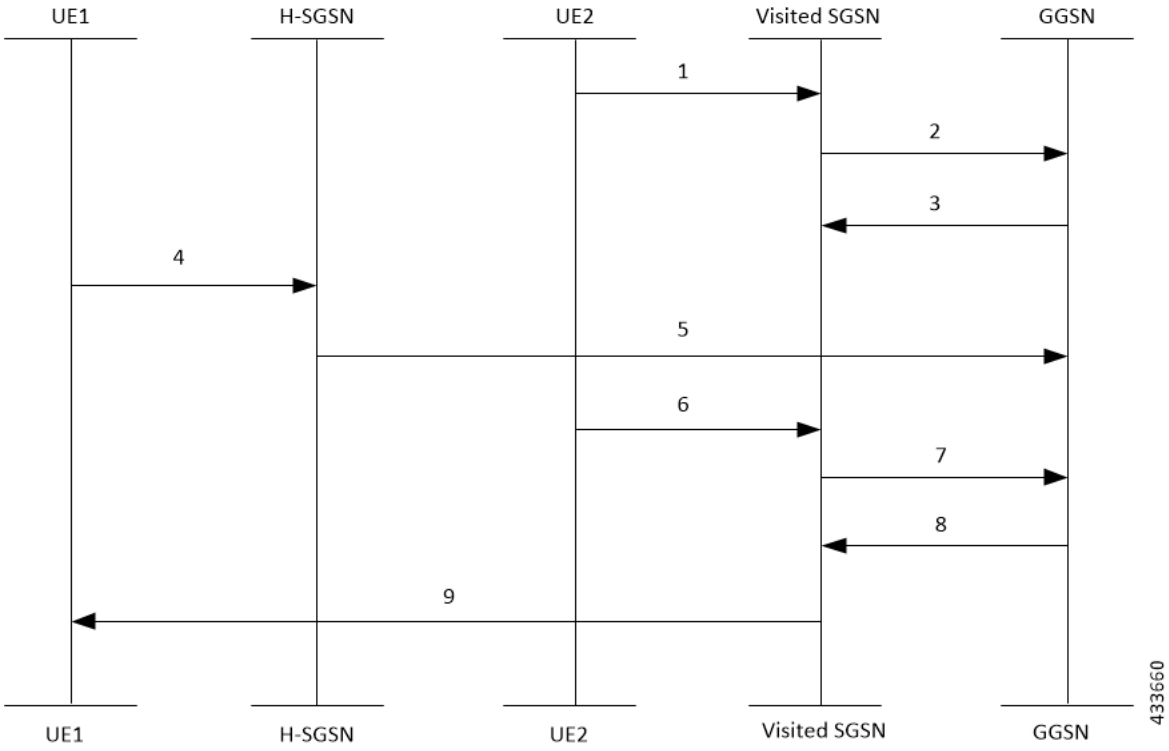
Call Flows

Following call flows show the handling of TEID collision with the ULI change for both P-GW and GGSN.

TEID Collision with ULI Change on GGSN Configuration

Following call flow shows the handling of TEID Collision with ULI Change on GGSN:

Figure 17: GTPC-Based TEID Collision Detection as per ULI Change



The call flow steps are listed below:

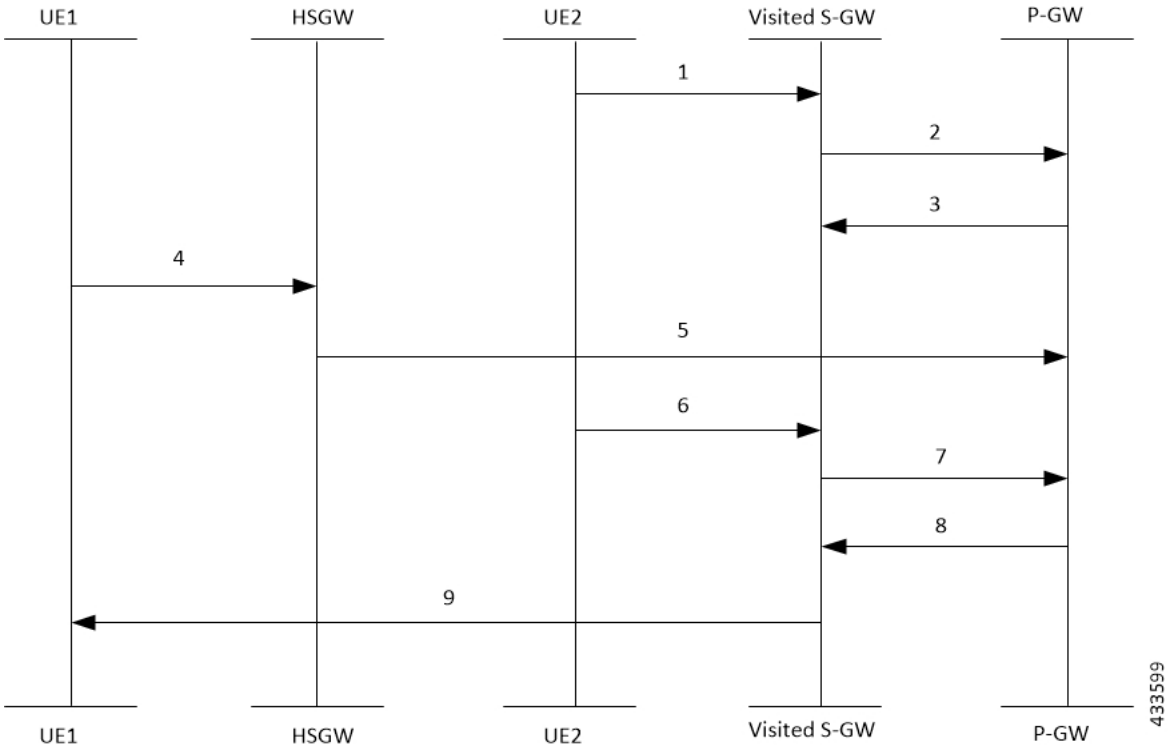
1. When a call is received from roaming subscriber, UE2 attempts to connect to GGSN through visited SGSN.
2. Roaming UE is allocated a TEID-x by the GGSN.
3. After the UE2 disconnects from the network, the session closes on GGSN. However, this session still continues on the visited SGSN.
4. The home UE attach happens on GGSN through home SGSN.
5. GGSN allocates the same TEID-x that was earlier assigned on GGSN.
6. Roaming UE returns to the GGSN. As the session on visited SGSN still exists, same TEID-x is used from visited SGSN.
7. If the TEID Collision with ULI Change feature is enabled at GGSN and the UE1 is in the home PLMN (as in Step 4), all the control requests (GTPv1-C) are processed at GGSN to check for a TEID-based collision as per the ULI change.
8. GGSN checks for MCC only of the ULI against the PLMN-List of the GGSN-Service. If there is no match, GGSM rejects the request. For example, for a HOME UE in GGSN, if the mcc in ULI information differs from PLMN list of the message, the request will be rejected

9. In case of a match, the request is sent for further processing.

TEID Collision with ULI Change for P-GW Configuration

Following call flow shows the handling of TEID Collision with ULI Change on P-GW:

Figure 18: EGTPC-Based TEID Collision Detection as per ULI Change



The call flow steps are listed below:

1. When a call is received from roaming subscriber, UE2 attempts to connect to P-GW through visited S-GW.
2. Roaming UE is allocated a TEID-x by the P-GW.
3. After the UE2 disconnects from the network, the session closes on P-GW. However, this session still continues on the visited S-GW.
4. The home UE attach happens on P-GW through home S-GW.
5. P-GW allocates the same TEID-x that was earlier assigned on P-GW.
6. Roaming UE returns to the P-GW. As the session on visited S-GW still exists, same TEID-x is used from visited S-GW.
7. If the TEID Collision with ULI Change feature is enabled at P-GW and the UE1 is in the home PLMN (as in Step 4), all the control requests (GTPv2-C) are processed at P-GW to check for a TEID-based collision as per the ULI change.
8. P-GW checks only MCC of the ULI against the PLMN-LIST of the PGW-Service. If there is no match, P-GW rejects the request.

9. In case of a match, the request is sent for further processing.

Configuring TEID Collision with ULI Change

This section provides information on the configuration of CLI command to reject a request in a TEID collision scenario on P-GW and GGSN.

Configuring TEID Collision with ULI Change on GGSN

Use the following configuration commands to configure P-GW to reject a request when TEID collision occurs.

```
configure
  context context_name
    ggsn-service service_name
      [ default | no ] gtpc update-pdp-resp reject uli-mismatch mcc-only

         end
```

NOTES:

- **default**: Resets the command to it its default setting—Disabled.
- **no**: Disables the GTPC parameters.
- **update-pdp-resp reject**: Updates the PDP Response reject options.
- **uli-mismatch**: Rejects the update PDP request message if the ULI is not part of the home PLMN session.
- **mcc-only**: Sends update PDP response with NON_EXISTENT (CC 192) cause code if MCC that is received in update PDP request does not match to the HOME PLMN.

Configuring TEID Collision with ULI Change on P-GW

Use the following configuration commands to configure P-GW to reject a request when TEID collision occurs.

```
configure
  context context_name
    pgw-service service_name
      [ default | no ] egtp bearer-req reject uli-mismatch mcc-only
        end
```

Notes:

- **default**: Resets the command to it its default setting—Disabled.
- **no**: Disables the GTPC parameters.
- **bearer-req**: Performs configuration related to handling a Bearer Request.
- **reject**: Shows the Bearer Request reject options.
- **uli-mismatch**: Sends Bearer response with CONTEXT_NOT_FOUND (CC 64) cause code if the ULI that is received in Bearer request does not match with the ULI of the existing session.

- **mcc-only**: Sends Bearer Response with CONTEXT_NOT_FOUND (CC 64) cause code if the ULI with MCC that is received in Bearer request does not match with the MCC of the existing session.

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

This section provides information about show commands and the fields that are introduced in support of TEID Collision with ULI Change.

show egtpc statistics

The output of this show command has been modified to display the following fields for TEID Collision with ULI Change:

- Modify Bearer Request
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Retrans RX
  - Discarded
  - No Rsp RX
- Modify Bearer Response
  - Total TX
  - Initial TX
  - Accepted
  - Denied
  - Retrans TX
  - Total RX
  - Initial RX
  - Accepted
  - Denied
  - Discarded
- Bearer Resource Command

- Total TX
- Initial TX
- Retrans TX
- Total RX
- Initial RX
- Retrans RX
- Discarded
- No Rsp RX

- Bearer Resource Failure Indication
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Discarded

- Delete Bearer Command
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Discarded

- Modify Bearer Request Without MME S11u TEID:
  - Local teid Mismatch:
    - Remote teid Mismatch
    - GnGp Call MBReq rejected FTEID absent
    - Tun Remote TEID Updated
    - Teid Collision with uli mismatch for BRcmd
    - Teid Collision with uli mismatch for DBCmd

show gtpc statistics

The output of this show command has been modified to display the following fields for TEID Collision with ULI Change:

- Update PDP Context RX
- Update PDP Context TX

show pgw-service name

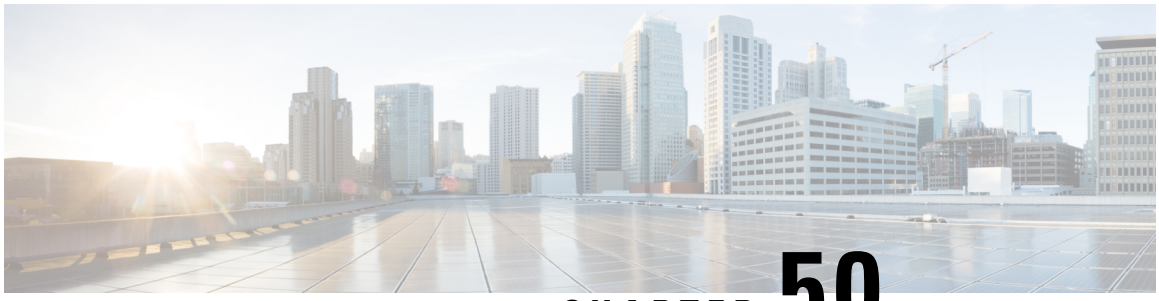
The output of this show command has been modified to display the following fields for TEID Collision ULI Change with only MCC mismatch:

```
EGTP Bearer Request with Context Not Found cause if MCC mismatch : Enabled
EGTP Bearer Request with Context Not Found cause if MCC mismatch : Disabled
```

show ggsn-service name ggsn-service | more

The output of this show command has been modified to display the following fields for TEID Collision ULI Change with only MCC mismatch:

```
GTPC Update PDP Response with Non Existent cause if IMSI mismatch : Enabled
  GTPC Update PDP Response with Non Existent cause if ULI mismatch : Enabled
  GTPC Update PDP Response with Non Existent cause if MCC mismatch : Enabled
```



CHAPTER 50

Security Enhancement

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	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

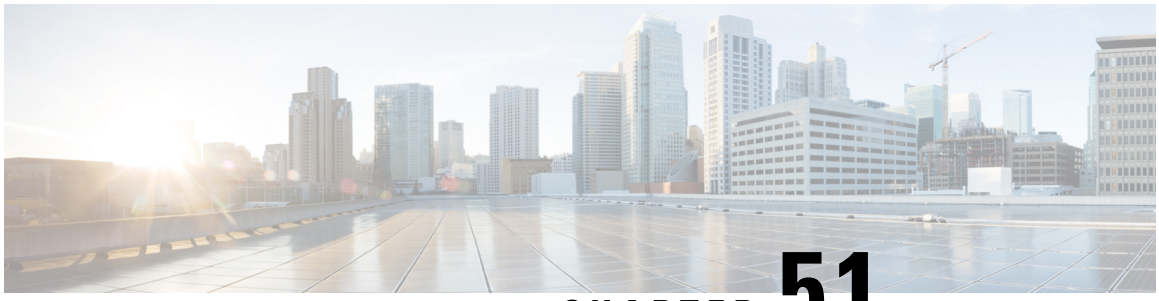
Revision History

Revision Details	Release
Password storage enhancement for non-trusted builds.	21.28.m6
First Introduced.	21.28.1

Feature Description

During upgrade or downgrade, it is recommended to use the compatible configuration files to avoid lockout. The configuration files saved from a new non-trusted build will not work on older builds (trusted or regular). The Admin password is stored as one way hash on non-trusted builds.

Customer Impact: If there is any saved configuration using new build there will be a possible impact during downgrade activities.



CHAPTER 51

SMS over NAS Messages on SGd Interface

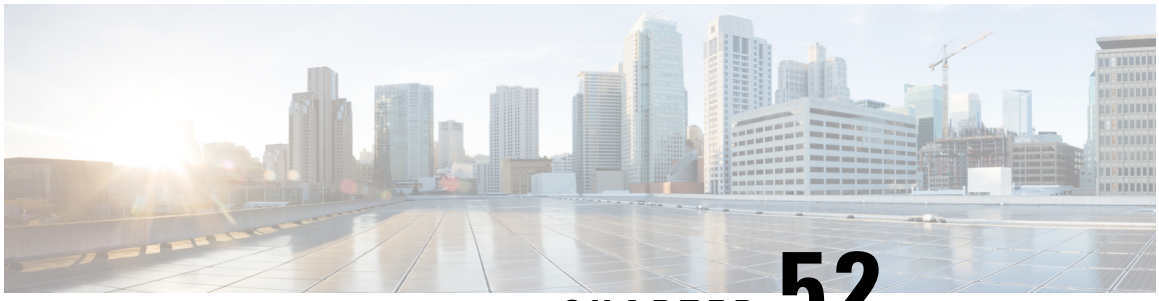
Revision History

Revision Details	Release
First Introduced.	21.28.m18

Feature Description

MME LI supports intercepting of Short Messaging Service (SMS) over NAS messages on the SGd Interface.

For more information, contact your Cisco account representative.



CHAPTER 52

Updating TAC ID to S-GW on Delete Session Request in Attach over Attach Case

Feature Summary and Revision History

Summary Data

Summary Data

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

Revision History

Revision History

Revision Details	Release
Configuration added to configure the MME to send old TAC Id in delete session request for old sessions.	21.28.m7

Feature Changes

Previous Behavior: While processing an Attach Over Attach Request, the MME sends a **delete-session-request** to the subscriber with the TAC Id received in Attach Request, as opposed to the last visited TAC Id.

New Behavior: A new CLI **oldtac-dsr-attach-over-attach** under mme-service is added to send old TAC Id in Delete Session Request. The subsequent Create Session Request is sent with the new TAC Id and the Detach Request Delete Session Request is sent with the new TAC Id received in the second attach.

Note The **oldtac-dsr-attach-over-attach** CLI will configure the MME to send old TAC Id in delete session request for old sessions in attach over attach scenario.

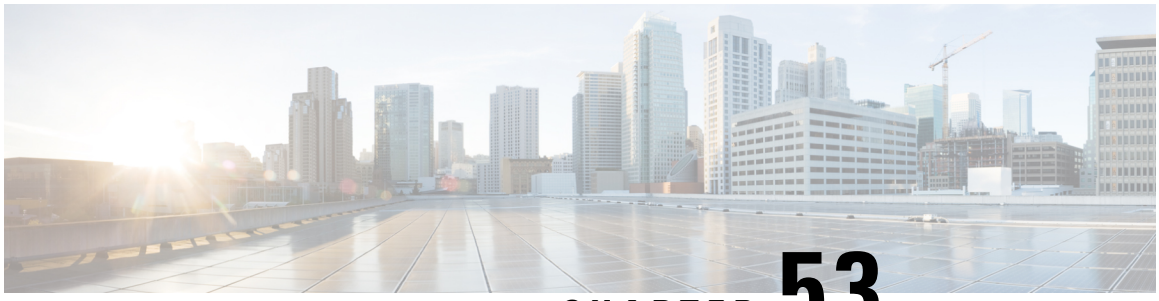
Command Changes

Use the following commands to configure the MME to send the old TAC Id in Delete Session Request for old sessions in attach over attach scenario.

```
configure
  context context_name
       mme-service service_name
       [ no ] oldtac-dsr-attach-over-attach
       exit
    exit
```

NOTES:

- **oldtac-dsr-attach-over-attach**: Sends old TAC Id in Delete Session Request for old sessions in attach over attach scenario. By default, it is disabled.
- **no**: Disables the CLI **oldtac-dsr-attach-over-attach**.



CHAPTER 53

UE-Usage-Type Based P-GW or SMF+PGW-C Selection

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500-DPC2 • VPC-DI
Feature Default	**UUT-based P-GW Selection without 5G Interworking:** Disabled - License not Required. **UUT-based PGW/SMF+PGW-C Selection with 5G Interworking:**Disabled - Existing 5G License to be Enabled.
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 select PGW/SMF+PGW-C based on the UE-Usage-Type with 5G Interworking.	21.28.6
ePDG is enhanced to select P-GW based on the UE-Usage-Type Without 5G Interworking.	21.28.5

UE-Usage-Type Based P-GW or SMF+PGW-C Selection

Feature Description

The Cisco ePDG supports selection of P-GW based on the allocated **UE-Usage-Type** (UUT) of the subscriber. **UE-Usage-Type** is stored in the HSS (Home Subscriber Server) within the subscription information of the UE. Each UE can have no more than one **UE-Usage-Type**. This functionality of selecting P-GW based on **UE-Usage-Type** is used to latch the subscribers to different cores by assigning an appropriate UE-Usage-Type value.

There is no change in the fallback mechanism, priority, and preference order of selection based on various criteria between AAA provided IP, DNS, and Static as in the existing P-GW selection, and same is applicable to UUT associated P-GWs.

AVP Support

This feature supports the **UE-Usage-Type** AVP with type Unsigned32 in the Diameter EAP Answer (DEA) message. This value indicates the usage characteristics of an UE that enables the selection of a specific Dedicated Core Network (DCN). The allowed value of **UE-Usage-Type** is in the range 0–255.

P-GW Selection based on UE-Usage-Type

The ePDG considers **UE-Usage-Type** AVP from the AAA/CPAR in the Diameter EAP Answer (DEA) message for the selection of P-GW to which the session has to be latched.

Note Subscribers not associated with any **UE-Usage-Type** are treated as per the current implementation. They will not be assigned any default **UE-Usage-Type** value.

To select the P-GW to be latched on based on the UE-Usage-Type:

- Enable the **UE-Usage-Type** feature through the CLI without **5G Interworking** and ensure that **UE-Usage-Type** AVP is received for a subscriber from the AAA server in the DEA (Diameter EAP Answer).

When the feature is enabled and **UE-Usage-Type** AVP is received from the AAA or CPAR in the DEA message, the ePDG uses the S-NAPTR procedure with the **x-s2b-gtp+ue-<uut value>** service parameter in the following scenarios:

- AAA provided FQDN based PGW selection

- APN-FQDN based PGW selection
- Local FQDN based PGW selection

The following process happens:

- ePDG first initiates the SNAPTR query against the AAA provided PGW-ID(FQDN) or Local FQDN or APN-FQDN to the server, to get the PGW IP address.
- The DNS server returns the NAPTR Resource Records (RRs) with “s” flag.
- RRs with service-parameter **x-3gpp-pgw: x-s2b-gtp+ue-<uut value1>** are considered by the ePDG to match one of the uut-value with the received **UE-Usage-Type** value.

Fallback Mechanism for UE-Usage-Type P-GW Selection

From DNS responses, if ePDG selects the P-GW based on the service parameter **x-s2b-gtp+ue-<uut-value1>.<uut-value2>.<uut-value3>** , where one of the UUT value in the Service parameter of the received DNS records matches with the **UE-Usage-Type** value received from AAA for a subscriber, the following selection order applies:

1. If DNS response has records for the given UUT, ePDG selects the P-GW. If none of the selected P-GWs are not reachable, fallback to static P-GW selection works based on local configuration, with the given UUT.
2. If DNS response has no matching UUT records, but has P-GW records without UUT, then ePDG ignores the P-GW list and fallback based on local configuration.
3. If the DNS query fails, or there are no PGW records matching with the given UUT value, or DNS is not reachable then, ePDG fallback to static P-GW selection based on the local configuration. The appropriate DNS-related failures get incremented.

In case of Local Static selection:

- If P-GW with the matching UUT value is configured, that will be considered
- If weight is defined, then, the Weight algorithm similar to the existing P-GW selection is applied to UUT-based selection.
- If no weight is configured, P-GW is selected in a round robin manner.
- If no P-GW with subscriber’s UUT is configured, but configured with P-GWs without UUT, or different UUTs, then ePDG ignores the P-GW lists and P-GW selection fails, a call gets terminated with appropriate disconnect reasons.

Limitations

This feature has the following limitations:

- The P-GW selection based on **UE-Usage-Type** (UUT) support is limited only to GTPv2 based s2b interface. All the three PDN types are supported including the IPv4, IPv6 and IPv4v6.
- ePDG does not send the value of **UE-Usage-Type** to P-GW in the Create Session Request.
- ePDG considers only the UUTs received in DEA message and not in any other diameter messages.

- This feature is not supported for Emergency calls. P-GW selection for emergency calls is as per the current implementation.

Configuring ePDG to Select P-GW based on the UE-Usage-Type

Use the following configuration commands to enable or disable the UE-Usage-Type.

```
configure
    context context_name
       epdg-service service_name
           [ no ] pgw-selection ue-usage-type
           end
```

NOTES:

- **pgw-selection ue-usage-type** : Enables P-GW selection based on the UE-Usage-Type.
- **no pgw-selection ue-usage-type** : Disables P-GW selection based on the UE-Usage-Type.

  By default, the P-GW selection based on the **UE-Usage-Type** feature is disabled. If **UE-Usage-Type** is not enabled or not associated with the subscriber, then the Gateway selection is performed as per the existing implementation.

Configuring Local P-GW with a Specific UE-Usage-Type

Use the following configuration command to configure the P-GW with a specific UE-Usage-Type (UUT).

Note A single P-GW can serve multiple UE-Usage-Type and single UE-Usage-Type can be served by multiple P-GW.

```
configure
    apn-profile apn_name
       pgw-address ip_address ue-usage-type value
       end
```

NOTES:

- **pgw-address** *ip_address* **ue-usage-type** *value*: Configures the UE-Usage-Type for the gateway service.

  The UE-Usage-Type integer value must be 1–255. If the P-GW is configured in either primary or secondary mode, then you cannot configure more than two IPs for the P-GW regardless of the **UE-Usage-Type**.

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 PGW selection based on **UE-Usage-Type** feature.

show epdg-service name *service-name*

If the **UE-Usage-Type** feature is enabled the **show epdg-service name** *service-name* CLI command displays the following output with the status:

```
Service name:  epdg1
  Context: pdif
  Bind: Done
  Max Sessions : 100000
  IP address: 111.111.11.2           UDP Port : 500
   Crypto-template: boston
  Reporting Action:
    Event Record: Enabled
  Service State: Started              Service Id: 6
  EGTP service : egtp-epdg-egress-v4
  MAG service : n/a
  MAG context : n/a
  PLMN Id:    MCC:242 , MNC:002
  Setup Timeout (sec) : 60
  dns-pgw context: pdif
  dns-pgw selection : weight,topology
  fqdn: n/a
  pgw-selection agent-info error-handling: terminate
  pgw-selection 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
  vendor-specific-attr pcscf-server-req: Private Extension
  Username MAC Address Stripping : Disabled
  QCI QOS Mapping Table : epdg_mapping
  Username MAC Address Validate : Enabled Failure-handling : Continue
  Newcall Policy : None
  Duplicate precedence in TFT - Allowed
  IP Fragment-Chain Timeout : 5 sec and Max OOO Fragment : 45
  EBI :
    Allowed Range 10 to 13
  Username MAC Address Delimiter - colon-or-NAI-Label
  Subscriber Map : map1
  AAA Send Framed-MTU Size : Disabled
  Data Buffering           : Enabled
  PDN-type IPv6 Path-MTU   : Enabled
  GTPC Overload Control Profile : None
  GTPC Load Control Profile: None
  LTE Emergency Profile: emergency
  Timeout Idle                      : Disabled
  Suppress International Roamer Handover : Disabled
  5G Interworking                   : Disabled
```

show configuration

The output of this command includes the following information:

```
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 statistics ue-usage-type

The **show epdg-service statistics ue-usage-type** command displays relevant counters for UUT based P-GW selection performed at the context level. This command is available as part of SSD.

Table 31: show epdg-service statistics ue-usage-type Command Output Descriptions

Field	Description
UUT Preferred PGW: The number of times that P-GW based on UE-Usage-Type is preferred.	
DNS Provided PGW	Number of times the P-GW selected from DNS responses for the given UE-Usage-Type.
Locally Configured PGW	Number of times the P-GW selected from local ePDG configuration for the given UE-Usage-Type.
AAA Provided PGW IP	Number of times the P-GW selected from AAA server provided IP attribute.
PGW not available reasons: Provides counters on how many times the UUT based P-GW selection is failed due to P-GW is not locally configured.	
No local PGW with matching UUT	The number of times that P-GW selection failed due to missing configuration.
Total Number of PGW Fallback: Fallback related counters for P-GW provided by AAA, DNS, and local configuration, for the associated UUT. In general, an attempt will be considered as fallback, after failed to connect first P-GW.	
PGW Fallback Attempted	Total number of UE-Usage-Type based P-GW fallback attempted when P-GW must be selected based on UUT.
PGW Fallback Success	Number of times session connected to P-GW, selected through fallback algorithm.
PGW Fallback Failure	Number of times session unable to connect to P-GW, selected through fallback algorithm.
Alternate PGW not found	Number of times where attempts to all P-GW is failed, and there are no alternate P-GW available further to attempt for a session to connect.

Field	Description
Local PGW resolution : Fallback related counters for total number of P-GW based on UE-Usage-Type provided by the local configuration. These counters are incremented when the previous attempt of P-GW is failed and the next fallback attempt of P-GW for the associated UE-Uage-Type is based on the local configuration.	
PGW Fallback Attempted	Total number of local UE-Usage-Type based P-GW fallback attempted when P-GW must be selected based on UUT.
PGW Fallback Success	Number of times session connected to local UE-Usage-Type based P-GW, selected through fallback algorithm.
PGW Fallback Failure	Number of times session unable to connect to local UE-Usage-Type based P-GW, selected through fallback algorithm.
Alternate PGW not found	Number of times where attempts to local UE-Usage-Type based P-GW failed, and there are no alternate P-GW available further to attempt for a session to connect.
DNS-related Failures	
DNS server not reachable	Number of times there are no response from DNS for the associated UE-Usage-Type.
No resource records	Number of times DNS server responded with no resource records for the associated UE-Usage-Type.
No matching PGW service params	Number of times DNS server responded with no P-GW, serving the requested UUT, in the resource records, when P-GW must be selected based on UUT for the session.
DNS PGW list exhausted	Increments when all the P-GW, provided by DNS, serving the given UUT, response is failed to connect.

Similarly, to view all the above mentioned counter details for a specific service in ePDG, use the **show epdg-service statistics name** *service-name* **ue-usage-type** command.

clear epdg-service statistics ue-usage-type

The **clear epdg-service statistics ue-usage-type** command clears statistics at context level.

clear epdg-service statistics name *service-name* ue-usage-type

The **clear epdg-service statistics name** *service-name* **ue-usage-type** command clears statistics at service level.

Bulk Statistics

This section provides bulk statistics variables supported for **UE-Usage-Type** in the ePDG schema.

show bulkstats variables epdg

Use the **show bulkstats variables epdg** command to view UE-Usage-Type related variables.

Bulk Statistics Variables	Description

uut-pgw-preferred	Number of times P-GW preferred based on UE-Usage-Type.
uut-pgw-dns-selected	Number of times the P-GW selected from DNS responses for the given UE-Usage-Type.
uut-pgw-local-selected	Number of times the P-GW selected from local epdg configuration for the given UE-Usage-Type.
uut-pgw-aaa-selected	Number of times the P-GW selected from AAA server provided IP attribute.
PGW not available reasons:	
uut-no-local-pgw-selected	The number of times that P-GW selection failed due to missing configuration.
Total Number of PGW Fallback:	
uut-pgw-fallback-attempted	Total number of UE-Usage-Type based P-GW fallback attempted when P-GW must be selected based on UUT.
uut-pgw-fallback-success	Number of times session connected to P-GW, selected through fallback algorithm.
uut-pgw-fallback-failed	Number of times session unable to connect to P-GW, selected through fallback algorithm.
uut-pgw-fallback-noalt-pgw	Number of times where attempts to all P-GW is failed, and there are no alternate P-GW available further to attempt for a session to connect.
Local PGW resolution:	
uut-local-pgw-fallback-attempted	Total number of local UE-Usage-Type based P-GW fallback attempted when P-GW must be selected based on UUT.
uut-local-pgw-fallback-success	Number of times session connected to local UE-Usage-Type based P-GW, selected through fallback algorithm.
uut-local-pgw-fallback-failed	Number of times session unable to connect to local UE-Usage-Type based P-GW, selected through fallback algorithm.
uut-local-pgw-fallback-noalt-pgw	Number of times where attempts to local UE-Usage-Type based P-GW failed, and there are no alternate P-GW available further to attempt for a session to connect.
DNS Related Failures:	

uut-dns-server-notreachable	Number of times there are no response from DNS for the associated UE-Usage-Type.
uut-dns-no-resourcerecords	Number of times DNS server responded with no resource records for the associated UE-Usage-Type,
uut-dns-no-matching-pgw-service	Number of times DNS server responded with no P-GW, serving the requested UUT, in the resource records, when P-GW must be selected based on UUT for the session.
uut-dns-pgw-list-exhausted	Increments when all the P-GW, provided by DNS, serving the given UUT, response is failed to connect.

P-GW or SMF+PGW-C Selection Based on UE-Usage-Type with 5G Interworking

Feature Description

ePDG supports handling of 4G and 5G Capable User Equipment (UE) for VoWIFI functionality along with **Interworking-5G** subscription data provided by HSS/AAA.

With **Interworking-5G** enabled on ePDG, for a seamless handover with NR, customer requests ePDG to select PGW/ SMF+PGW-C based on **UE-Usage-Type** for both initial attach and handover scenarios. ePDG determines the type of gateway PGW/SMF+PGW-C based on the existing **Interworking-5G** decision matrix. For more information on decision matrix, see the Selecting P-GW or SMF+PGW-C Based on UE-Usage-Type, on page 292.

When both **UE-Usage-Type** and **Interworking-5G** features are enabled and if the subscriber is allocated with **UE-Usage-Type** in the subscriber profile stored in HSS, ePDG determines the gateway type as PGW/SMF+PGW-C using the **Interworking-5G** decision matrix.

Based on the selected gateway type and UUT values (if received from AAA), ePDG either applies the appropriate DNS service parameter to select the gateway from the DNS responses received or selects the gateway serving the UUT through local configuration.

Upon enabling **UE-Usage-Type** feature with the **Interworking-5G** feature disabled, the selection of P-GW would be as per current implementation. For more information, refer P-GW Selection based on UE-Usage-Type, on page 278.

License Requirements

Existing **Interworking-5G** license shall be used to enable **Interworking-5G** feature, no separate license would be required for **UE-Usage-Type** Interworking with 5G feature.

For more details, see the *License Requirements* section in the ePDG Interworking with SMF+P-GW-IWK Support chapter .

How it Works

The gateway selection between PGW/SMF+PGW-C with the help of the AVP **UE-Usage-Type** happens in the following way:

- The CLI commands implemented under epdg-service for both **UE-Usage-Type** and **Interworking-5G** (licensed feature) features should be enabled for UUT **Interworking-5G** functionality.
- The existing CLI to configure SMF+PGW-C with the associated,**UE-Usage-Type** under APN profile shall be enhanced to be supported in ePDG as well. Same SMF+PGW-C IP can be configured to service more than one **UE-Usage-Type**. More than one SMF+PGW-C can be associated with a particular **UE-Usage-Type**. The valid range for **UE-Usage-Type** is 1-255.

Note Range 1-255 is as per current implementation, by MME. As per the standard, the range is 0–255, where the range 0–127 is reserved.

- If the **UE-Usage-Type** feature is not enabled, ePDG will not consider **UE-Usage-Type**, received in DEA, for the selection of PGW/SMF+PGW-C.
- Subscribers not associated with any **UE-Usage-Type**, would be treated as per the existing **Interworking-5G** implementation. Such subscribers with no UUT value from AAA, would not be assigned any default **UE-Usage-Type** value.
- Upon enabling both the features (**Interworking-5G** and **UE-Usage-Type**), ePDG uses the existing decision matrix to decide whether to latch on SMF+PGW-C/PGW. If the **UE-Usage-Type** is received from the AAA, then ePDG shall use this **UE-Usage-Type** and compare it against the **UE-Usage-Type** provided by DNS or local configuration based on the selection mechanism and select PGW or SMF+PGW-C serving the specific **UE-Usage-Type**.
- If the selected gateway is PGW, ePDG does not share either PDU session ID to SMF+PGW-C or S-NSSAI, PLMNID to UE, which remains the same as per the existing implementation.
- If the **UE-Usage-Type** is not received or if both **UE-Usage-Type** and **Interworking-5G** features are not enabled, the subscriber will be treated as per the current implementation.
- If the selected PGW/SMF+PGW-C IP is provided by the AAA server, then ePDG assumes that the provided PGW or SMF+PGW-C serves the **UE-Usage-Type** of the connecting UE and ePDG does not validate the same.
- Based on the decision matrix:
  - If the ePDG decides the selected gateway type as SMF+PGW-C, then DNS records with the service parameter **x-3gpp-pgw:x-s2b-gtp+nc-smf+ue-<value>** shall be filtered.
  - If the ePDG decides the selected gateway type as PGW then DNS records with the service parameter **x-3gpp-pgw:x-s2b-gtp+ue-<value>** shall be filtered.
- If PGW/SMF+PGW-C is selected, e-PDG shall use the S-NAPTR procedure in the following scenarios:
  - AAA provided FQDN-based PGW/ SMF+PGW-C selection.
  - APN-FQDN based PGW/SMF+PGW-C selection.
  - Local FQDN-based PGW/SMF+PGW-C selection.

The service parameters used are **x-3gpp-pgw:x-s2b-gtp+ue-<value>** for PGW and **x-3gpp-pgw:x-s2b-gtp+nc-smf+ue-<value>** for SMF+PGW-C.

- ePDG will first initiate the S-NAPTR query against AAA provided FQDN or Local FQDN or APN-FQDN to DNS server to get the PGW/SMF+PGW-C IP address. DNS server shall return NAPTR Resource Records (RRs), which should be fed to a filter where only RRs having one of the UUT value matching the UUT associated with the subscriber, shall be considered by ePDG. When there are more than one matching PGWs/ SMF+PGW-Cs, priority and weight will be applied to choose the PGW/ SMF+PGW-C as per the existing implementation. The service parameters used are **x-3gpp-pgw: x-s2b-gtp+ue-<value1>.<value2>…** for PGW and **x-3gpp-pgw: x-s2b-gtp+nc-smf+ue-<value1>. <value2>…** for SMF+PGW-Cs.
- If the DNS query fails or there is no matching DNS record for the given UUT or DNS provided PGW/SMF+PGW-C is not reachable or DNS provided the SMF+PGW-C list is exhausted, ePDG shall fallback to locally configured SMF+PGW-C with matching UUT from AAA, based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons. ePDG will not select DNS records without **UE-Usage-Type** in the service parameter, when the **UE-Usage-Type** feature is enabled.
- For static PGW/SMF+PGW-C selection with **UE-Usage-Type**, if PGW/SMF+PGW-C is not configured with the matching UUT or configured PGWs or SMF+PGW-Cs without UUT or different UUTs, ePDG ignores the other locally configured PGWs/SMF+PGW-Cs. The ePDG shall fallback to other PGW selection mechanism like DNS or AAA provided IP, based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons.
- In local configuration, under APN-profile, if the PGW/SMF+PGW-C is configured in primary/secondary mode, you cannot define more than two IPs (Prim/Sec) for the PGW/SMF+PGW-C. The **UE-Usage-Type** configured along with primary and secondary mode shall be the same or unique and you cannot configure multiple sets of **UE-Usage-Type** in primary/secondary mode under the same APN profile.

Call Flows

Following call flow discusses the process and call flow of SMF+PGW-C gateway selection when both **UE-Usage-Type** and **Interworking-5G** are enabled.

Figure 19: Call Flow of P-GW/SMF Gateway Selection

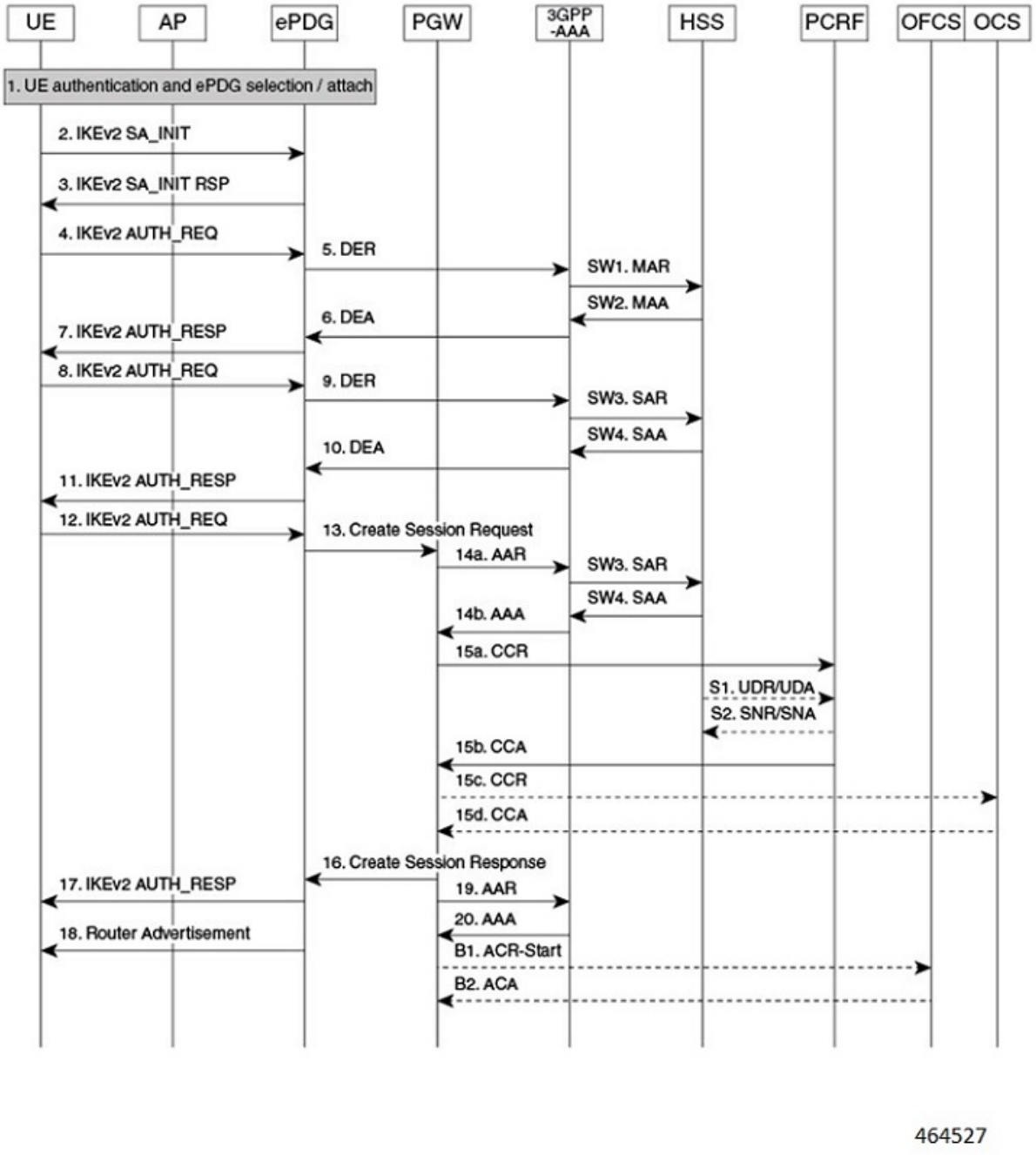


Table 32: Call Flow Description

Step	Description
1.	The UE sends the IKE_SA_INIT message.

Step	Description
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 the N1_MODE_CAPABILITY Notify payload.
4.	During the IKEv2 tunnel establishment procedure, the 5GC NAS capable UE shall indicate its support of 5GC NAS in IKEv2. The UE allocates a PDU Session ID and includes this in IKEv2 to the ePDG.
5.	UEs mobility restriction parameters related to 5GS or indication of support for interworking with 5GS for this APN or both are obtained by ePDG as part of the reply from the HSS via 3GPP AAA Server. These parameters and the 5G NAS support indicator from the UE, may be used by ePDG to determine if PGW/SMF+PGW-C should be selected.
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.	ePDG shall select PGW/SMF+PGW-C based on the existing decision matrix. If **UE-Usage-Type** is enabled and associated with the subscriber profile, that is, ePDG receives **UE-Usage-Type** value from AAA in DEA (Diameter EAP Answer), this parameter shall be used by ePDG and compare it with the **UE-Usage-Type** received from DNS server or local configuration.

Step	Description
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.
13.	If the UE supports 5G NAS and the PDN connection is not restricted to interworking with 5GS by user subscription, then ePDG shall send the 5GS Interworking Indication and the PDU Session ID to SMF+PGW-C and it does not carry any additional elements to indicate the **UE-Usage-Type** of the subscriber. If the SMF+PGW-C supports more than one S-NSSAI and the APN is valid for more than one S-NSSAI, the SMF+PGW-C selects one S-NSSAI. If the UE does not support 5GC NAS but has 5GS subscription, and a SMF+PGW-C is selected and interaction with UDM, PCF and UPF is required, the SMF+PGW-C assigns PDU Session ID. The SMF+PGW-C shall not provide any 5GS related parameters to the UE.
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+PGW-C 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.
16.	The SMF+PGW-C assigns a S-NSSAI to be associated with the PDN connection. The SMF+PGW-C sends the S-NSSAI to ePDG together with a PLMN ID that the S-NSSAI relates to. If the UE does not support 5GC NAS but has 5GS subscription, and a SMF+PGW-C is selected and interaction with UDM, PCF and UPF is required, the SMF+PGW-C assigns PDU Session ID. The SMF+PGW-C shall not provide any 5GS related parameters to the UE.
17.	The IKEv2 Authentication Response message, the ePDG sends S-NSSAI and PLMN ID to the UE, if the same is received from SMF+PGW-C.

Limitations

Some of the known limitations of this feature are as follows:

- This feature is not applicable to emergency calls.

- ePDG will not send the value of **UE-Usage-Type** to PGW/SMF+PGW-C in CreateSessionRequest.
- ePDG would provide support for AVP's (**UE-Usage-Type** /Interworking5GS-Indicator/Core-Network-Restrictions) received only in DEA message and not in any other diameter messages.
- The scope of this feature is limited to GTPv2 based S2b/S2b-C interface only.

Use Cases

If both **UE-Usage-Type** and **Interworking-5G** features are enabled and **UE-Usage-Type** is associated for the subscriber, ePDG would either compare it with the locally configured **UE-Usage-Type** or with the **UE-Usage-Type** value received from DNS service parameter based on the local configuration.

Feature Enabled/ Disabled	UUT Reeived from AAA	Core-Network-Restriction	Interworking-5GS-Indicator	N1 Mode	DNS Selection	Static Selection
UUT & IWK5G	No	5GC Allowed	Subscribed/Not Subscribed	0 or 1	ePDG selects SMF+PGW-C with service parameter **x-3gpp-pgw: x-s2b-gtp+nc-smf, without +ue<value>**.	ePDG selects SMF+PGW-C address configured without UUT.
UUT & IWK5G	Received from AAA and matches with DNS/local config: e.g.:130.	5GC Allowed	Subscribed/Not Subscribed	0 or 1	ePDG selects SMF+PGW-C with service parameter **x-3gpp-pgw: ~~x-s2b-gtp+nc-smf+ue-130~~**.	ePDG selects SMF+PGW-C address configured with UUT 130.
UUT & IWK5G	Received from AAA and matches with DNS/local config: e.g.:130.	5GC Not Allowed	Subscribed/Not Subscribed	0 or 1	ePDG selects PGW with service parameter **x-3gpp-pgw: x-s2b-gtp+ue-130**.	ePDG selects PGW address configured with UUT 130.

Feature Enabled/ Disabled	UUT Reeived from AAA	Core-Network-Restriction	Interworking-5GS-Indicator	N1 Mode	DNS Selection	Static Selection
UUT & IWK5G	Received from AAA and does not match with DNS/Local config e.g.: 150.	5GC Allowed	Subscribed/Not Subscribed	0 or 1	If the local fallback is applicable, based on local configuration or PDN-GW-Allocation-Type received from AAA, ePDG falls back to local selection of SMF+PGW-C based on UUT 150 if configured, else the call would be dropped.	Call would be dropped, only if no other fallback mechanism is applicable.
UUT or IWK5G disabled or both disabled	UUT associated e.g.: 130	Restricted/Not Restricted	Subscribed/Not Subscribed	0 or 1	ePDG selects PGW/ SMF+PGW-C as per current implementation.	ePDG selects PGW/ SMF+PGW-C as per current implementation.

Selecting P-GW or SMF+PGW-C Based on UE-Usage-Type

- If ePDG decides to choose SMF+PGW-C based on the decision matrix, then ePDG shall use the below service parameters in case if the selection mechanism is DNS.

  Service Parameters: x-3gpp-pgw:x-s2b-gtp+nc-smf+ue-<ue usage type>

  Or

  Service Parameters: x-3gpp-pgw:x-s2b-gtp+ue-<ue usage type>+nc-smf

  Or

  Service Parameters: x-3gpp-pgw:x-s2b-gtp+ue-<ue usage type1>.<ue usage type2>..+nc-smf

- If ePDG decides to choose PGW based on the decision matrix, then ePDG shall use the below service parameters in case if the selection mechanism is DNS.

  Service Parameters: x-3gpp-pgw:x-s2b-gtp+ue-<ue usage type>

  Or

  Service Parameters: x-3gpp-pgw:x-s2b-gtp+ue-<ue usage type1>.<ue usage type2>

Figure 20: P-GW or SMF+PGW-C Based on a UE-Usage-Type Decision Matrix Table

Scenario	UE 5GC NAS Capability	Core-Network-Restrictions	Interworking-5GS APN-Configuration	ePDG Policy	Service tag for selection of DNS records by ePDG	5GSIWKI	5GCNRS	5GCNRI	PGW or SMF
							Rel-15: N/A Rel-16 Values below		
	From UE	From HSS				+On S2b/S2b-c			
1-2	Yes or No	Not Included	Not Included	No	x-s2b-gtp+ue-<uut>	0	1	0	PGW
3	No	Not Included	SUBSCRIBED	Operator Policy (NOTE1) (NOTE3)	x-s2b-gtp+nc-smf+ue-<uut> (default) x-s2b-gtp+ue-<uut>	0	1	1	SMF (Default) PGW
4	Yes	Not Included	SUBSCRIBED	Operator Policy (NOTE3)	x-s2b-gtp+nc-smf+ue-<uut>	1	1	1	SMF PGW
5	No	Not Included	NOT SUBSCRIBED	Operator Policy (NOTE 1) (NOTE 2) (NOTE 3)	x-s2b-gtp+nc-smf+ue-<uut> (default) x-s2b-gtp+ue-<uut>	0	1	0	SMF (Default) PGW
6	Yes	Not Included	NOT SUBSCRIBED	Operator Policy (NOTE 2) (NOTE 3)	x-s2b-gtp+nc-smf+ue-<uut> (default) x-s2b-gtp+ue-<uut>	0	1	0	SMF (Default) PGW
7-12	Yes or No	5GC not allowed	SUBSCRIBED or NOT SUBSCRIBED or Not Included	No	x-s2b-gtp+ue-<uut>	0	1	0	PGW
13	No	5GC allowed	SUBSCRIBED	Operator Policy (NOTE1) (NOTE 3)	x-s2b-gtp+nc-smf+ue-<uut> (default) x-s2b-gtp+ue-<uut>	0	1	1	SMF (Default) PGW
14	Yes	5GC allowed	SUBSCRIBED	Operator Policy (NOTE3	x-s2b-gtp+nc-smf+ue-<uut>	1	1	1	SMF PGW
15-16	No	5GC allowed	NOT SUBSCRIBED or Not Included	Operator Policy (NOTE 1) (NOTE 2) (NOTE 3)	x-s2b-gtp+nc-smf+ue-<uut> (default) x-s2b-gtp+ue-<uut>	0	1	0	SMF (Default) PGW
17-18	Yes	5GC allowed	NOT SUBSCRIBED or Not Included	Operator Policy (NOTE 2) (NOTE 3)	x-s2b-gtp+nc-smf+ue-<uut> (default) x-s2b-gtp+ue-<uut>	0	1	0	SMF (Default) PGW

475875

- **NOTE 1:**

  Default Behavior: SMF+PGW-C supports Rel-16 functionality to support 4G-only UEs, that is, the SMF+PGW-C shall generate PDU Session ID for 4G-only UEs.

  Custom Behavior: To handle the case where SMF+PGW-C is Rel-15 and cannot support 4G only UEs.

- **NOTE 2:**

  Default Behavior: When Interworking-5GS APN-Configuration is set to not allowed, the APN configuration is in UDR, but handover to 5G SA is not allowed.

  Custom Behavior: When Interworking-5GS APN-Configuration is set to not allowed, the APN configuration is in SPR and not in UDR, hence P-GW needs to be selected.

- **NOTE 3:** Whenever SMF+PGW-C IP or FQDN is not preferably upgraded in the DNS server or in the local ePDG config, in such a case if the CLI (**smf-not-configured**) is configured, then ePDG ignores the SMF+PGW-C selection and always choose P-GW in all the scenario.

Note The service parameters from DNS are updated considering that **UE-Usage-Type** is enabled and received from AAA. If **UE-Usage-Type** is either not enabled or not received from AAA, then the service parameters would remain the same as the existing implementation, that is, **x-s2b-gtp** in case of PGW and **x-s2b-gtp+nc-smf** in case of SMF+PGW-C.

In case of dynamic selection mechanism, ePDG would first initiate the S-NAPTR query against AAA provided FQDN or Local FQDN or APN-FQDN to DNS server, to get the PGW/SMF+PGW-C IP address based on **UE-Usage-Type**. DNS server shall return NAPTR RRs (Resource Records) and these RRs shall be fed to a filter where only RRs with the service-parameter **x-3gpp-pgw: x-s2b-gtp+ue-<value>** or **x-3gpp-pgw: x-s2b-gtp+nc-smf+ue-<value>** shall be considered by ePDG. The PGW or SMF+PGW-C IP provided by the DNS server shall be considered only when the ue-usage-type matches with the **UE-Usage-Type** AVP received from AAA/CPAR in the DEA message.

In case of local/static SMF+PGW-C selection mechanism, the **UE-Usage-Type** configured under apn-profile should match with the **UE-Usage-Type** AVP from AAA/CPAR in DEA message.

Below are the sample configurations:

```
pgw-address 1.1.1.1 ue-usage-type 130 smf-combined
pgw-address 1.1.1.1 ue-usage-type 130
```

Fallback Mechanism for SMF+PGW-C Selection with UE-Usage-Type

With both **Interworking-5G** and **UE-Usage-Type** features enabled, based on the decision matrix if the selected gateway is SMF+PGW-C, ePDG uses the existing fallback mechanisms, priority, and preference order of selection and the same is applicable to UUT associated SMF+PGW-Cs as well. The existing fallback selection order is as follows:

1. **error-terminate** configured (pgw-selection agent-info error-terminate)
   a. PDN-GW-Allocation-Type from AAA: Dynamic
      - Enabled **pgw-selection prefer aaa-pgw-id**

        AAA->DNS->Local
      - Enabled **pgw-selection local-configuration-preferred** and **pgw-selection prefer aaa-pgw-id**

        AAA->Local->DNS
      - Enabled **pgw-selection local-configuration-preferred**

        Local->DNS
      - Disabled both **pgw-selection local-configuration-preferred** and **pgw-selection prefer aaa-pgw-id**

        DNS->Local

   b. PDN-GW-Allocation-Type from AAA: Static or Absent
      - Enabled **pgw-selection prefer aaa-pgw-id**

        AAA->DNS->Local
      - Enabled **pgw-selection local-configuration-preferred** and **pgw-selection prefer aaa-pgw-id**

AAA->Local->DNS

- Enabled **pgw-selection local-configuration-preferred**

  Local->AAA

- Disabled both **pgw-selection local-configuration-preferred** and **pgw-selection prefer aaa-pgw-id**

  AAA->Local

2. **error-terminate** unconfigured (**no pgw-selection agent-info error-terminate**): If **error-terminate** is unconfigured, all the aforementioned cases, 1.a. and 1.b., remain the same except the below mentioned cases:
   a. PDN-GW-Allocation-Type from AAA: Static or Absent
      - Enabled **pgw-selection local-configuration-preferred**

        Local->AAA->DNS

      - Disabled both **pgw-selection local-configuration-preferred** and **pgw-selection prefer aaa-pgw-id**

        AAA->Local->DNS

DNS Selection

From the DNS responses, ePDG selects SMF+PGW-C with UUT based on the service parameter received from DNS server, i.e., the records with the service parameter **x-s2b-gtp+nc-smf+ue-<value1>. <value2>. <value3>…..**, where one of the UUT value in the service parameter from the received DNS records should match with the **UE-Usage-Type** value received from AAA for the subscriber. That specific SMF+PGW-C IP with UUT given by DNS shall be selected.

- If DNS response has records for the given UUT with SMF+PGW-C capability, which matches with the UUT received from AAA, the corresponding SMF+PGW-C will be selected. If the selected SMF+PGW-Cs IPs are not reachable, the ePDG shall fallback to the alternate SMF+PGW-C address with matching UUT from the DNS records if available. Else, it shall fallback to the locally configured SMF+PGW-C with matching UUT from AAA based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons.
- If the DNS response has no matching UUT records, but has PGW records with matching UUT or both PGW and SMF+PGW-C records without UUT, in this case, ePDG shall ignore the PGW and SMF+PGW-C records and falls back to locally configured SMF+PGW-C with matching UUT from AAA, based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons and the corresponding DNS-related failure statistics would be updated.
- If the DNS query fails or no records received from DNS or DNS is not reachable, ePDG shall fallback to locally configured SMF+PGW-C with matching UUT from AAA, based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons and the corresponding DNS-related failure statistics would be updated.

Local Static Selection

If SMF+PGW-Cs configured with UUT matches with the UUT received from AAA, then the selection of GW IP shall be considered based on:

- If Weight is Defined: Existing Weight algorithms for PGW selection would be applied for UUT based SMF+PGW-C selection as well.
- If No Weights Configured: UUT based SMF+PGW-C shall be selected in a round-robin method.
- If SMF+PGW-C is not configured with the matching UUT from AAA or configured SMF+PGW-Cs without UUT or different UUTs: ePDG ignores the other locally configured SMF+PGW-C. ePDG shall fallback to other PGW selection mechanism like DNS or AAA provided IP, based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons.
- If the selected SMF+PGW-Cs with UUT is not reachable, then ePDG shall fallback to alternate locally configured SMF+PGW-C IP with matching UUT if available, else ePDG shall fallback to other PGW selection mechanism like DNS or AAA provided IP, based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons.
- If no local entries defined: ePDG shall fallback to other PGW selection mechanism like DNS or AAA provided IP, based on the fallback selection order if applicable, else the call would be dropped with appropriate disconnect reasons.
- In both primary and secondary mode configuration under local apn-profile, if the SMF+PGW-C configured with UUT does not matches with the UUT received from AAA, or there is no SMF+PGW-C or SMF+PGW-C configured without UUT, then ePDG shall fallback to the AAA provided IP if available, when the PDN-GW-Allocation-Type received from AAA is static, else the call would be dropped with appropriate disconnect reasons.

Note

- All the above mentioned behaviour under DNS selection and local static selection are applicable for PGW selection based on UUT as well.
- In a handover scenario, ePDG shall consider AAA provided PGW ID (IP address/FQDN) for PGW/SMF+PGW-C selection as per the existing implementation.

Configuring ePDG to Select SMF Based on UE-Usage-Type

Configuring ePDG to select SMF+PGW-C based on **UE-Usage-Type** involves enabling **Interworking-5G** and **UE-Usage-Type** features.

To enable **Interworking-5G**, see the topic Configuring ePDG to Enable 5G Interworking.

To enable **UE-Usage-Type**, see the topic Configuring ePDG to Select P-GW Based on UE-Usage-Type .

Configuration for Local SMF+PGW-C Serving Specific UE-Usage-Type

Use the following configuration command to configure the SMF+PGW-C selection with a specific **UE-Usage-Type**:

```
configure
    apn-profile apn_name
      pgw-address ip_address ue-usage-type value smf-combined
      end
```

NOTES:

- **smf-combined**—Specifies if the PGW and SMF+PGW-C are combined.

Monitoring and Troubleshooting

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

Show Commands and Output

The following two show commands provide information about the **Interworking-5G** with **UE-Usage-Type** for configured services or specific to a service.

show epdg-service statistics interworking-5g ue-usage-type

The show command **show epdg-service statistics interworking-5g ue-usage-type** displays the EPDG statistics for **Interworking-5G** with **UE-Usage-Type** for all the configured services.

```
[pdif]asr5500# show epdg-service statistics interworking-5g ue-usage-type
```

Following fields are available in the output of the **show epdg-service statistics interworking-5g ue-usage-type** in support of this feature:

Table 33: show epdg-service statistics interworking-5g ue-usage-type Command Output Descriptions

Field	Description
UUT SMF+PGW-C Preferred: Total number of SMF+PGW-C preferred based on **UE-Usage-Type** during 5G ePDG sessions for the case where 5GSIWK flag is not set.	
DNS provided SMF+PGW-C	Total number of DNS provided SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions.
Locally configured SMF+PGW-C	Total number of locally configured SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions.
AAA provided SMF+PGW-C IP	Total number of AAA provided SMF+PGW-C selected during 5G ePDG sessions.
UUT SMF+PGW-C Only: Total number of SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions for the case where 5GSIWK flag is set and PDUSessionID will be forwarded to SMF+PGW-C.	
DNS provided SMF+PGW-C	Total number of DNS provided SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions.
Locally configured SMF+PGW-C	Total number of locally configured SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions.
AAA provided SMF+PGW-C IP	Total number of AAA provided SMF+PGW-C selected for 5G ePDG sessions.
UUT PGW Only: Total number of PGW selected based on **UE-Usage-Type** during 5G ePDG sessions	
DNS provided PGW	Total number of DNS provided PGW selected based on **UE-Usage-Type** during 5G ePDG sessions.

Field	Description
Locally configured PGW	Total number of locally configured PGW selected based on **UE-Usage-Type** during 5G ePDG sessions
AAA provided PGW IP	Total number of AAA provided PGW selected during 5G ePDG sessions.
PGW/SMF+PGW-C Not Available Reasons: Provide counters on how many times **UE-Usage-Type** based PGW/SMF+PGW-C selection is failed due to no matching **UE-Usage-Type** with locally configured PGW/SMF+PGW-C.	
No PGW configured locally with matching UUT	Total number of gateway selection failures due to no matching **UE-Usage-Type** with locally configured PGW during 5G ePDG sessions.
No SMF+PGW-C configured locally with matching UUT	Total number of gateway selection failure due to no matching **UE-Usage-Type** with locally configured SMF+PGW-C during 5G ePDG sessions.
Total Number of SMF+PGW-C Fallback: Fallback related counters (Attempted/Success/Failure) for total number of SMF+PGW-C provided by AAA, DNS, and local configuration for the associated **UE-Usage-Type**. In general, an attempt for next SMF+PGW-C, if the previously selected SMF+PGW-C for the associated **UE-Usage-Type** is failed, then it will be considered as fallback. This implies that when a create session request sent for the selected SMF+PGW-C is failed due to some reason, ePDG shall attempt fallback and sends create session request to the next available SMF+PGW-C for the associated **UE-Usage-Type**.	
SMF+PGW-C Fallback Attempted	Total number of **UE-Usage-Type** based SMF+PGW-C fallbacks attempted during 5G ePDG sessions.
SMF+PGW-C Fallback Success	Total number of **UE-Usage-Type** based SMF+PGW-C fallbacks succeeded during 5G ePDG sessions.
SMF+PGW-C Fallback Failure	Total number of **UE-Usage-Type** based SMF+PGW-C fallbacks failed during epdg 5G sessions.
Alternate SMF+PGW-C not found	Total number of alternate **UE-Usage-Type** based SMF+PGW-Cs not available in either AAA or DNS, when the call is dropped for a 5G ePDG session.
Local SMF+PGW-C Resolution: Fallback related counters for total number of SMF+PGW-C based on **UE-Usage-Type** provided by local configuration.	
SMF+PGW-C Fallback Attempted	Total number of local **UE-Usage-Type** based SMF+PGW-C fallbacks attempted during 5G ePDG sessions.
SMF+PGW-C Fallback Success	Total number of local **UE-Usage-Type** based SMF+PGW-C fallbacks succeeded during 5G ePDG sessions.
SMF+PGW-C Fallback Failure	Total number of local **UE-Usage-Type** based SMF+PGW-C fallbacks failed during 5G ePDG sessions.
Alternate SMF+PGW-C not found	Total number of alternate local **UE-Usage-Type** based SMF+PGW-C not available to further fallback for a 5G session to get connected.

Field	Description
Total Number of PGW Fallbacks: Fallbacks related counters (Attempted/Success/Failure) for total number of PGW provided by AAA, DNS, and local configuration for the associated **UE-Usage-Type**. An attempt for the next PGW since the previously selected PGW for the associated **UE-Usage-Type** is failed, will be considered as fallback.	
PGW Fallback Attempted	Total number of **UE-Usage-Type** based PGW fallbacks attempted during 5G ePDG sessions.
PGW Fallback Success	Total number of **UE-Usage-Type** based PGW fallbacks succeeded during 5G ePDG sessions.
PGW Fallback Failure	Total number of **UE-Usage-Type** based PGW fallbacks failed during epdg 5G sessions.
Alternate PGW not found	Total number of alternate **UE-Usage-Type** based PGWs not available in either AAA or DNS, when the call is dropped for a 5G ePDG session.
Local PGW Resolution: Fallback related counters for total number of PGW based on **UE-Usage-Type** provided by local configuration.	
PGW Fallback Attempted	Total number of local **UE-Usage-Type** based PGW fallbacks attempted during 5G ePDG sessions.
PGW Fallback Success	Total number of local **UE-Usage-Type** based PGW fallbacks succeeded during 5G ePDG sessions.
PGW Fallback Failure	Total number of local **UE-Usage-Type** based PGW fallbacks failed during 5G ePDG sessions.
Alternate PGW not found	Total number of alternate local **UE-Usage-Type** based PGWs not available to further fallback for a 5G session to get connected.
DNS Related Failures	
DNS server not reachable	Total number of failures due to DNS server not reachable during 5G ePDG sessions for the associated **UE-Usage-Type**.
No resource records	Total number of failures due to no DNS resource records during 5G ePDG sessions for the associated **UE-Usage-Type**.
No matching UUT PGW service params	Total number of PGW received without matching the **UE-Usage-Type** during 5G ePDG sessions.
No matching UUT SMF+PGW-C service params	Total number of SMF+PGW-C received without matching the **UE-Usage-Type** during 5G ePDG sessions.
DNS PGW list exhausted	Total number of **UE-Usage-Type** based PGW list provided in DNS response, has failed to connect and exhausted during 5G ePDG sessions.
DNS SMF+PGW-C list exhausted	Total number of **UE-Usage-Type** based SMF+PGW-C list provided in DNS response, has failed to connect and exhausted during 5G ePDG sessions.

show epdg-service statistics name service-name interworking-5g ue-usage-type

The show command **show epdg-service statistics name** *service-name* **interworking-5g ue-usage-type** displays the all the counters from previous section with **UE-Usage-Type** for that specific service.

```
[epdg]asr5500# show epdg-service statistics name epdg1 interworking-5g ue-usage-type
```

The output fields of this command are same as the output fields of the **show epdg-service statistics interworking-5g ue-usage-type**. The difference between the two CLIs is that **show epdg-service statistics name service name** *service-name* **interworking-5g ue-usage-type** displays these statistics for a specific service, while **show epdg-service statistics interworking-5g ue-usage-type** displays the statistics at context level.

Error Scenario: Following are the possible error scenarios in this configuration:

Table 34: show epdg-service statistics name service-name interworking-5g ue-usage-type Error Scenarios and Outputs

Error Scenario	Output
If the service name is not valid	Service-Name: No such service
If no statistics are available at epdg level	No statistics available for **Interworking-5G** with **UE-Usage-Type**
If **UE-Usage-Type** is not enabled under a specific service	**UE-Usage-Type** feature is not enabled for this service
If **Interworking-5G** is not enabled under a specific service	**Interworking-5G** feature is not enabled for this service
If both **UE-Usage-Type** and **Interworking-5G** is not enabled under a specific service	Both **Interworking-5G** and **UE-Usage-Type** feature are not enabled for this service

5G Session Statistics

The total number of 5G session statistics for both **Interworking-5G** and **Interworking-5G** with **UE-Usage-Type** would be updated under the below existing 5G counters. The 5G Attempts/Setup/Failures counter must be referred for interworking of 5G with **UE-Usage-Type** as well.

Example:

```
[pdif]asr5500# show epdg-service statistics interworking-5g
```

The ePDG **Interworking-5G** statistics for all services are as follows:

5G Sessions:

- Attempts
- Setup
- Failures

Clear Statistics

The following clear commands will take care of clearing the statistics at context and service levels:

- **clear epdg-service statistics interworking-5g ue-usage-type:** Clears ePDG statistics related to **Interworking-5G** with **UE-Usage-Type**.
- **clear epdg-service statistics name <service name> interworking-5g ue-usage-type:** Clears ePDG statistics related to **Interworking-5G** with **UE-Usage-Type** for a particular service.

Executing the below command also clears the counters specific to **UE-Usage-Type**:

- **clear epdg-service statistics interworking-5g**
- **clear epdg-service statistics name svc1 interworking-5g**

Error Scenarios: Following are the possible error scenarios for the above configurations:

Error Scenario	Output
If no statistics are available at ePDG level.	No ePDG **Interworking-5G** with UE-Usage-Type statistics is available to clear.
If a service is not valid.	Service-Name: No such service.
If **UE-Usage-Type** is not enabled for a specific service.	**UE-Usage-Type** feature is not enabled for this service.
If **Interworking-5G** is not enabled under a specific service.	**Interworking-5G** feature is not enabled for this service.
If both **UE-Usage-Type** and **Interworking-5G** is not enabled under a specific service.	Both **Interworking-5G** and **UE-Usage-Type** feature are not enabled for this service.

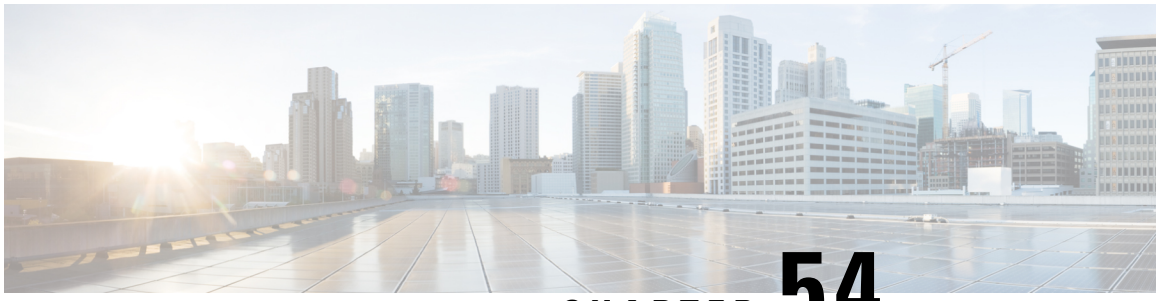
Bulk Statistics

Following new counters are provided under the existing **epdg-interworking-5g** schema:

Bulk Statistics Variables	Description
uut-iwk5g-smf-preferred	Total number of SMF+PGW-C preferred based on **UE-Usage-Type** during 5G ePDG sessions for the case where 5GSIWK flag is not set.
uut-iwk5g-smf-preferred-dns	Total number of DNS provided SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions.
uut-iwk5g-smf-preferred-local	Total number of locally configured SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions.
uut-iwk5g-smf-preferred-aaa	Total number of AAA provided SMF+PGW-C selected during 5G ePDG sessions.
uut-iwk5g-smf-only	Total number of SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions for the case where 5GSIWK flag is set and PDUSessionID will be forwarded to SMF+PGW-C.
uut-iwk5g-smf-only-dns	Total number of DNS provided SMF+PGW-C selected based on **UE-Usage-Type** during 5G ePDG sessions.

Bulk Statistics Variables	Description
uut-iwk5g-smf-only-local	Total number of locally configured SMF+PGW-C selected based on **UE-Usage-Type** duringS 5G ePDG sessions.
uut-iwk5g-smf-only-aaa	Total number of AAA provided SMF+PGW-C selected for 5G ePDG sessions.
uut-iwk5g-pgw-only	Total number of PGW selected based on **UE-Usage-Type** during 5G ePDG sessions
uut-iwk5g-pgw-only-dns	Total number of DNS provided PGW selected based on **UE-Usage-Type** during 5G ePDG sessions.
uut-iwk5g-pgw-only-local	Total number of locally configured PGW selected based on **UE-Usage-Type** during 5G ePDG sessions
uut-iwk5g-pgw-only-aaa	Total number of AAA provided PGW selected during 5G ePDG sessions.
PGW/SMF+PGW-C Not Available Reasons:	
uut-iwk5g-no-local-pgw	Total number of gateway selection failure due to no matching **UE-Usage-Type** with locally configured PGW during 5G ePDG sessions.
uut-iwk5g-no-local-smf	Total number of gateway selection failure due to no matching **UE-Usage-Type** with locally configured SMF+PGW-C during 5G ePDG sessions.
Total Number of SMF+PGW-C Fallback:	
uut-iwk5g-smf-fallback-attempted	Total number of **UE-Usage-Type** based SMF+PGW-C fallback attempted during 5G ePDG sessions.
uut-iwk5g-smf-fallback-success	Total number of **UE-Usage-Type** based SMF+PGW-C fallback succeeded during 5G ePDG sessions.
uut-iwk5g-smf-fallback-failed	Total number of **UE-Usage-Type** based SMF+PGW-C fallback failed during epdg 5G sessions.
uut-iwk5g-smf-fallback-noalt-smf	Total number of alternate **UE-Usage-Type** based SMF+PGW-C not available in either AAA or DNS, when the call is dropped for a 5G ePDG session.
Local SMF+PGW-C Resolution:	
uut-iwk5g-local-smf-fallback-attempted	Total number of local **UE-Usage-Type** based SMF+PGW-C fallback attempted during 5G ePDG sessions.
uut-iwk5g-local-smf-fallback-success	Total number of local **UE-Usage-Type** based SMF+PGW-C fallback succeeded during 5G ePDG sessions.
uut-iwk5g-local-smf-fallback-failed	Total number of local **UE-Usage-Type** based SMF+PGW-C fallback failed during 5G ePDG sessions.
uut-iwk5g-local-smf-fallback-noalt-smf	Total number of alternate local **UE-Usage-Type** based SMF+PGW-C not available to further fallback for a 5G session to get connected.

Bulk Statistics Variables	Description
Total Number of PGW Fallback:	
uut-iwk5g-pgw-fallback-attempted	Total number of **UE-Usage-Type** based PGW fallback attempted during 5G ePDG sessions.
uut-iwk5g-pgw-fallback-success	Total number of **UE-Usage-Type** based PGW fallback succeeded during 5G ePDG sessions.
uut-iwk5g-pgw-fallback-failed	Total number of **UE-Usage-Type** based PGW fallback failed during epdg 5G sessions.
uut-iwk5g-pgw-fallback-noalt-pgw	Total number of alternate **UE-Usage-Type** based PGW not available in either AAA or DNS, when the call is dropped for a 5G ePDG session.
Local PGW Resolution:	
uut-iwk5g-local-pgw-fallback-attempted	Total number of local **UE-Usage-Type** based PGW fallback attempted during 5G ePDG sessions.
uut-iwk5g-local-pgw-fallback-success	Total number of local **UE-Usage-Type** based PGW fallback succeeded during 5G ePDG sessions.
uut-iwk5g-local-pgw-fallback-failed	Total number of local **UE-Usage-Type** based PGW fallback failed during 5G ePDG sessions.
uut-iwk5g-local-pgw-fallback-noalt-pgw	Total number of alternate local **UE-Usage-Type** based PGW not available to further fallback for a 5G session to get connected.
DNS Related Failures:	
uut-iwk5g-dns-server-notreachable	Total number of failures due to DNS server not reachable during 5G ePDG sessions for the associated **UE-Usage-Type**.
uut-iwk5g-dns-no-resourcerecords	Total number of failures due to no DNS resource records during 5G ePDG sessions for the associated **UE-Usage-Type**.
uut-iwk5g-dns-no-matching-pgw-service	Total number of PGW received without matching the **UE-Usage-Type** during 5G ePDG sessions.
uut-iwk5g-dns-no-matching-smf-service	Total number of SMF+PGW-C received without matching the **UE-Usage-Type** during 5G ePDG sessions.
uut-iwk5g-dns-pgw-list-exhausted	Total number of **UE-Usage-Type** based PGW list provided in DNS response, has failed to connect and exhausted during 5G ePDG sessions.
uut-iwk5g-dns-smf-list-exhausted	Total number of **UE-Usage-Type** based SMF+PGW-C list provided in DNS response, has failed to connect and exhausted during 5G ePDG sessions.



CHAPTER 54

UE Radio Capability IE Size

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
MME is enhanced to support 16K UE Radio Capability.	2024.03.0

UE Radio Capability Information Element

The UE Radio Capability Information Element (IE) provides the network with details about the radio capabilities of the User Equipment (UE), including supported RATs, power class, and frequency bands. This information helps the network manage and optimize its interactions with the UE.

MME handles and uses UE capability information to support more band combinations during handovers. The MME has increased the size limit for the UE Radio Capability information and parses the following IEs with UE Radio Capability information of size 16384 bytes.

Note To configure the UE Capability IE size below 9000 bytes, see the Configuring UE Radio Capability IE Size chapter in the *Release Change Reference Guide*.

Table 35: Supported IEs

Messages	Corresponding IEs
INITIAL CONTEXT SETUP REQUEST	UE Radio Capability
UE CAPABILITY INFO INDICATION	UE Radio Capability
HANDOVER-REQUIRED	Source eNB to Target eNB Transparent Container
HANDOVER-REQUEST	Source eNB to Target eNB Transparent Container
FORWARD RELOCATION REQUEST	E-UTRAN Transparent Container

Configure the UE Radio Capability IE

Use this task to set the default value size of UE Radio Capability IE and its size in bytes. With the range increased from 9000 to 16384, it limits the size of the UE Radio Capability IE present in UE Capability Info Indication Message. You can also disable the UE radio capability size limit.

Procedure

Step 1 Create a context name.

context *context_name*

Example:

```
configure
  context context_name
```

Step 2 Specify an MME service name.

mme-service *service_name*

Example:

```
configure
  context context_name
```

```
    mme-service service_name
end
```

Step 3 Use the following steps to enable or disable the UE Radio Capability

a) To specify the default size of UE Radio Capability IE with 9000 bytes.

s1-mme ue-radio-cap

Example:

```
configure
   context context_name
     mme-service service_name
       s1-mme ue-radio-cap
   end
```

b) To specify the size of UE Radio Capability IE in bytes. The size must be an integer in the range of 3072 to 16384.

Note To configure between 9001 and 16384 bytes the IFTASK payload size must be configured with 16K. For more information, see the *Configure IFTASK MEH Payload Size* section.

s1-mme ue-radio-cap size

Example:

```
configure
   context context_name
     mme-service service_name
       s1-mme ue-radio-cap size
   end
```

c) To disable the UE Radio Capability size limit:

no s1-mme ue-radio-cap

Example:

```
configure
   context context_name
     mme-service service_name
       no s1-mme ue-radio-cap
   end
```

Configure IFTASK MEH Payload Size

Use this task to set the maximum payload size from default (9KB) to 16KB.

Procedure

Step 1 Specify the MEH payload in 16kbytes.

iftask meh-payload .

Example:

```
[local]swch82(config)# iftask meh-payload
       #end
```

Step 2 Specify **no** to use the default size of 9KB.

no iftask meh-payload

Example:

```
[local]swch82(config)# no iftask meh-payload
       #end
```

What to do next

Follow the method of procedure to deploy the **iftask meh-payload** CLI:

1. Setup the required iftask configuration.
2. Save the entire configuration into a boot config file.
3. Reload the setup. This is required to configure the huge size mbuf pool with appropriate size and the the maximum supported 16k payload size.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot the UE Radio Capability IE functionality.

Show Commands and Outputs

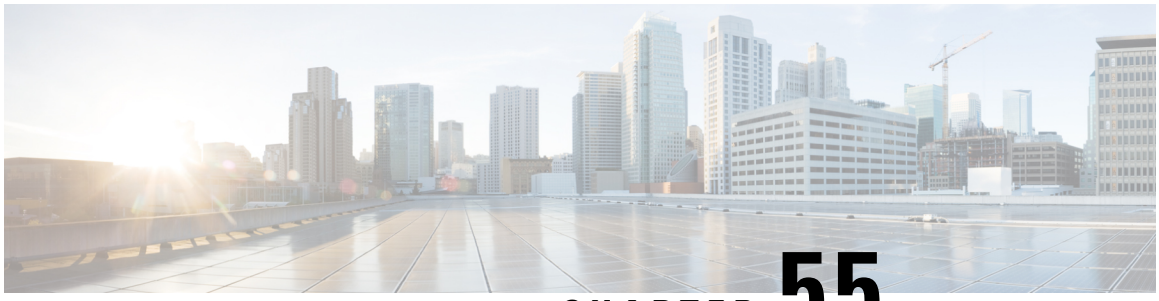
show mme-service statistics

To view the statistics of large packet drops under Protocol error statistics, execute the **show mme-service statistics** command.

…

```
Protocol Error Statistics:
   Transmitted:
    Drops:
    Large Packet               :            0
   Received:
    Drops:
    Large Packet               :            0  Large Container IE             :      0

    Large Packet(9217-16384)   :            0
    Large Packet(16385-24576)  :            0
    Large Packet(24577-32768)  :            0
    Large Packet(32769-40900)  :            0
    Large Packet(40901-49152)  :            0
```



CHAPTER 55

VLAN-aware VMs

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.28.M0

Feature Description

VLAN-aware VMs instances send and receive VLAN-tagged traffic over a single vNIC. VLAN-aware is useful for NFV applications (VNFs) that expect VLAN-tagged traffic, allowing multiple services served by a single vNIC. You can use VLAN-aware VMs with trunk interfaces to facilitate the automated addition and removal of networks with uninterrupted connectivity.

VLAN trunks support VLAN-aware instances by combining VLANs into a single trunked port. To implement trunks for VLAN-tagged traffic:

- Create a parent port and attach the new port to an existing neutron network. When you attach the new port, OpenStack Networking (neutron) adds a trunk connection to the parent port you created.
- Create subports. These subports connect VLANs to instances, which allow connectivity to the trunk.

Deploy a VM instance to use the MAC address that the OpenStack Networking service (neutron) assigned to the subport. The Elastic Services Controller (ESC) 5.8 version supports this VLAN-Aware VM.

Limitations:

Due to the known RFE defects from Red Hat for VLAN-aware VM over SRIOV VF, VLAN-aware has the following two limitations during deployment of VPC DI and while attaching parent ports to the VMs:

- Neutron trunk port created as part of the VLAN-aware VM configuration is in DOWN'status.
- Sub Ports created with multiple VLAN IDs are in Detached state.

For more information, see the VLANs chapter in the *ASR 5500 System Administration Guide*, *VPC-DI System Administration Guide*, and *VPC-SI System Administration Guide*.