Release Change Reference, StarOS Release 21.25

First Published: 2021-09-30

Last Modified: 2022-10-25

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

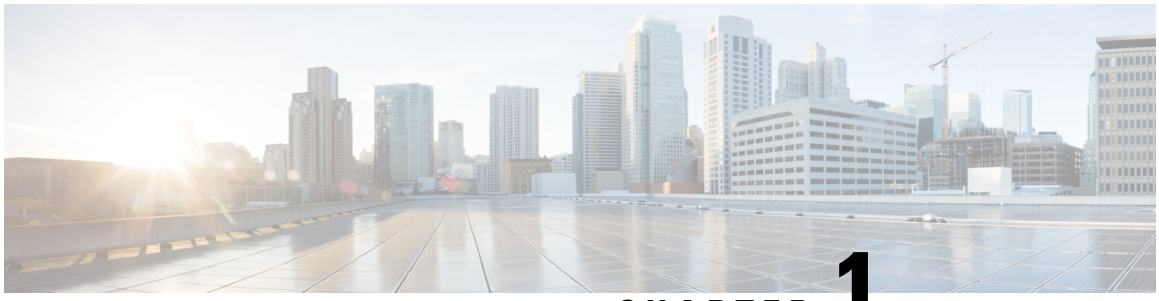
Conventions Used

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**



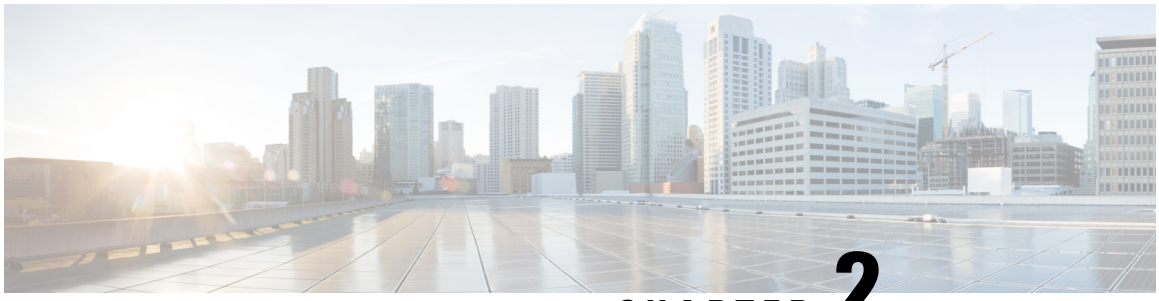
CHAPTER 1

Release 21.25 Features and Changes Quick Reference

Release 21.25 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
5GS Interworking using N26 Interface Support, on page 17	MME	21.25
Adding ECPD Identification and Account Numbers to Pilot Packets, on page 43	• GGSN • P-GW	21.25
Cinder Volume Multi-Attach	• P-GW • SAEGW	21.25
DNS Client KPI Enhancement, on page 51	P-GW	• 21.25 • 21.25.4
EPS to 5GS Mobility Enhancement, on page 55	MME	21.25.12
Handling Uneven Resource Distribution Notifications on Session Managers	• GGSN • P-GW • SAEGW	21.25
LTE To Wi-Fi Success Rate, on page 65	ePDG	21.25

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
No IMSI or MSISDN Included in LRR for VoLTE EM Call from User of Foreign Network, on page 63	MME	21.25.6
Password Expiration Notification, on page 71	P-GW	21.25.3
Reject Paging Request for Active Emergency VoLTE Call	MME	21.25
Sending EMM Information during Periodic TAU	MME	21.25
Suppressing Handover Request for VoWiFi IR Subscribers	ePDG	21.25
TCP Reset with Invalid Sequence Number should not Trigger Connection Close, on page 87	P-GW	21.25
Support for Tariff-Time-Change in Fast Path, on page 89	P-GW	21.25.4
Video Shaping Tethered Data, on page 91	ECS	21.25
VPP Metric Enhancement, on page 95	P-GW	21.25



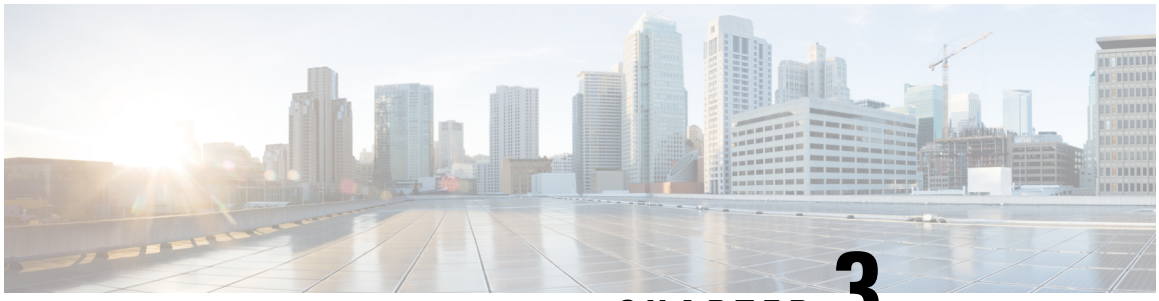
CHAPTER 2

Feature Defaults Quick Reference

Feature Defaults

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

Feature	Default
5GS Interworking using N26 Interface Support	Disabled - Configuration Required
Adding ECPD Identification and Account Numbers to Pilot Packets	Disabled - Configuration Required
Cinder Volume Multi-Attach	Enabled - Always-on
DNS Client KPI Enhancement	Disabled - Configuration Required
EPS to 5GS Mobility Enhancement	Disabled - Configuration Required
Handling Uneven Resource Distribution Notifications on Session Managers	Disabled - Configuration Required
LTE to Wi-Fi Success Rate	Disabled - Configuration Required
IMSI not Included in LRR	Disabled - Configuration Required
Reject Paging Request for Active Emergency VoLTE Call	Enabled - Always-on
Sending EMM Information during Periodic TAU	Disabled - Configuration Required
Suppressing Handover Request for VoWiFi IR Subscribers	Disabled - Configuration Required
Support for Tariff-Time-Change in Fast Path	Enabled - Always-on
TCP Reset with Invalid Sequence Number should not Trigger Connection Close	Disabled - Configuration Required
Video Shaping Tethered Data	Disabled - Configuration Required
VPP Metric Enhancement	Disabled - Configuration Required



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.25 software release.

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

Bulk statistics changes for 21.25 include:

- New Bulk Statistics, on page 5
- Modified Bulk Statistics, on page 13
- Deprecated Bulk Statistics, on page 13

New Bulk Statistics

APN Schema

The following bulkstatistics are added in the APN schema as part of the DNS client KPI enhancement feature:

Bulkstats	Description
dns-nf-pcscf-total-queries-sent	Count of the total query for DNS.
dns-nf-pcscf-success-queries	Count of total successful queries from the DNS server.
dns-nf-pcscf-success-positive-cache-queries	Count of total queries from the DNS cache.
dns-nf-pcscf-domain-not-found	Query count when FQDN queried is not available in the DNS server config file.
dns-nf-pcscf-query-timeouts	Query count when the DNS server is not reachable.
dns-nf-pcscf-socket-errors	Query count when the DNS server encountered socket error.
dns-nf-pcscf-unable-to-connect	Unsuccessful query count when not able to connect to the DNS server.

Bulkstats	Description
dns-nf-pcscf-cache-corrupted	Unsuccessful query count due to cache corruption.
dns-nf-pcscf-other_failures	Count for failures other than listed here.

ECS Schema

The following bulkstatistics are added in the ECS schema as part of the VPP metrics feature:

Variables	Description
TCP	
tcp-vpp-flows-cur	Indicates the current number of flows through VPP for TCP analyzer.
tcp-vpp-flows	Indicates the total number of flows through VPP for TCP analyzer.
tcp-vpp-pkts	The total number of IP packets through VPP for TCP analyzer.
tcp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.
UDP	

Variables	Description
udp-vpp-flows-cur	Indicates the current number of flows through VPP for UDP analyzer.
udp-vpp-flows	Indicates the total number of flows through VPP for UDP analyzer.
udp-vpp-pkts	Indicates the total number of IP packets through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for UDP analyzer.
HTTP	
http-vpp-flows-cur	Indicates the current number of flows through VPP for HTTP analyzer.
http-vpp-flows	Indicates the total number of flows through VPP for HTTP analyzer.
http-vpp-pkts	Indicates the total number of IP packets through VPP for HTTP analyzer.
http-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTP analyzer.
http-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTP analyzer.
http-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTP analyzer.

Variables	Description
http-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTP analyzer.
http-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTP analyzer.
Secure-HTTP	
https-vpp-flows-cur	Indicates the current number of flows through VPP for HTTPS analyzer.
https-vpp-flows	Indicates the total number of flows through VPP for HTTPS analyzer.
https-vpp-pkts	Indicates the total number of IP packets through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTPS analyzer.
P2P	
p2p-vpp-flows-cur	Indicates the current number of flows through VPP for P2P analyzer.
p2p-vpp-flows	Indicates the total number of flows through VPP for P2P analyzer.

Variables	Description
p2p-vpp-pkts	Indicates the total number of IP packets through VPP for p2p analyzer.
p2p-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for P2P analyzer.

ePDG Schema

The following bulkstatistics are added in the ePDG schema as part of the LTE to Wi-Fi Success Rate feature:

Table 1: Bulk Statistics Variables in the ePDG Schema

Variables	Description
vpnname	The name of the VPN associated with the interface.
vpnid	The identification number of the context configured on the system that is currently facilitating the ePDG service. VPN ID is an internal reference number.
servname	The name of the ePDG service for which these statistics are being displayed.
servid	The identification number of the ePDG service for which these statistics are displayed. Service ID is an internal reference number.
ho-disc-remote	The total number of disconnected sessions remotely before connect during LTE to Wi-Fi handoff.
ho-disc-admin	The total number of sessions disconnected by Administrator during LTE to Wi-Fi handoff.
ho-disc-idle-timeout	The total number of sessions disconnected due to idle timeout during LTE to Wi-Fi handoff.

Variables	Description
ho-disc-abs-timeout	The total number of sessions disconnected due to absolute timeout during LTE to Wi-Fi handoff.
ho-disc-longdur-timeout	The total number of sessions disconnected due to long duration timeout during LTE to Wi-Fi handoff.
ho-disc-sesssetup-timeout	The total number of sessions disconnected due to session setup timeout during LTE to Wi-Fi handoff.
ho-disc-noresource	The total number of sessions disconnected due to non availability of resources during LTE to Wi-Fi handoff
ho-disc-authfail	The total number of sessions disconnected due to authorization failure during LTE to Wi-Fi handoff.
ho-disc-flowadd-failure	The total number of sessions disconnected due to flow add failure during LTE to Wi-Fi handoff.
ho-disc-invalid-dest	The total number of sessions disconnected due to invalid destination during LTE to Wi-Fi handoff.
ho-disc-srcaddr-violation	The total number of sessions disconnected due to source address violation during LTE to Wi-Fi handoff.
ho-disc-dupreq	The total number of sessions disconnected due to duplicate request during LTE to Wi-Fi handoff.
ho-disc-addrassign-failure	The total number of sessions disconnected due to address assignment failure during LTE to Wi-Fi handoff.
ho-disc-misc	The total number of sessions disconnected due to miscellaneous reasons during LTE to Wi-Fi handoff.
ho-disc-mip-reg-timeout	The total MIP registration timeout during LTE to Wi-Fi handoff.
ho-disc-invalid-apn	The number of sessions disconnected because an ePDG rejected the incoming new call due to an APN syntax error (invalid length).
ho-disc-icsr-delete	The number of times that a session got deleted on the standby ICSR chassis when a call clear trigger is received from the active chassis or the call is removed for re-establishment when a full checkpoint was received.
ho-disc-invalid-qci	The total number of sessions disconnected due to invalid QCI received from the AAA server during LTE to Wi-Fi handoff.
ho-disc-ue-redirected	The total number of sessions disconnected due to UE redirection during LTE to Wi-Fi handoff.
ho-disc-roaming-mandatory	The total number of sessions disconnected due to DNS failure when roaming is mandatory during LTE to Wi-Fi handoff.
ho-disc-ho-disc-invalid-imei	The total number of sessions disconnected due to invalid IMEI received from UE during LTE to Wi-Fi handoff.
ho-disc-gtpc-abort-sess-cmd	The total number of disconnected sessions due to GTP control plane path failure during LTE to Wi-Fi handoff.

Variables	Description
ho-disc-gtpu-abort-sess-cmd	The total number of disconnected sessions due to GTP user plane path failure during LTE to Wi-Fi handoff.
ho-disc-gtpu-error-indication	The total number of disconnected sessions due to error indication message on GTP user plane during LTE to Wi-Fi handoff.
ho-disc-pgw-not-reachable	The total number of disconnected sessions due to P-GW during LTE to Wi-Fi handoff.
ho-disc-reject-from-pgw	The total number of disconnected sessions due to P-GW rejecting the Create Session Request during LTE to Wi-Fi handoff.
ho-disc-s2b-access-denied	The total number of sessions disconnected due to S2B cause codes mapped to private IKEv2 notify payload type access denied during LTE to Wi-Fi handoff.
ho-disc-s2b-network-failure	The total the number of sessions disconnected due to S2B cause codes mapped to private IKEv2 notify payload type network failure during LTE to Wi-Fi handoff.
ho-disc-s2b-msg-failure	The total number of sessions disconnected due to S2B cause codes mapped to private IKEv2 notify payload type message failure during LTE to Wi-Fi handoff.
ho-disc-s2b-rat-disallowed	The total number of sessions disconnected due to S2B cause code rat disallowed during LTE to Wi-Fi handoff.
ho-disc-s2b-context-not-found	The total number of sessions disconnected due GTPv2 cause code "Context Not Found" during LTE to Wi-Fi handoff.
ho-disc-epdg-pcscf-restoration	The total number of sessions disconnected due to P-GW triggered reactivation request for P-CSCF restoration during LTE to Wi-Fi handoff.
ho-disc-dns-server-not-reachable	The total number of disconnected sessions due to DNS server not reachable during LTE to Wi-Fi handoff.
ho-disc-dns-no-resource-records	The total number of disconnected sessions when no valid record is fetched from the DNS server during LTE to Wi-Fi handoff.
ho-disc-dns-no-matching-server	The total number of disconnected sessions when the fetched service parameters from DNS record doesn't match the configured protocol (GTP or PMIPv6) during LTE to Wi-Fi handoff.
ho-disc-aaa-server-not-reachable	The total number of disconnected sessions due to the AAA server being unreachable from ePDG during LTE to Wi-Fi handoff.
ho-disc-aaa-invalid-aaa-attribute	The total number of disconnected sessions due to authentication failure at AAA server and invalid attributes received in Diameter messages from the AAA server during LTE to Wi-Fi handoff.
ho-disc-aaa-apn-validation-failed	The total number of disconnected sessions due to APN mismatch at SWu and SWm interfaces during LTE to Wi-Fi handoff.
ho-disc-aaa-admin	Indicates the AAA Admin disconnect during LTE to Wi-Fi handoff.

Variables	Description
ho-disc-aaa-invalid-pdn-type	The total number of disconnected sessions due to mismatch over PDN type between UE and AAA server during LTE to Wi-Fi handoff.
ho-disc-aaa-non-uicc-auth-failed	The total number of non-UICC disconnected sessions due to AAA server during LTE to Wi-Fi handoff.
ho-disc-aaa-network-too-busy	The total number of sessions disconnected due to network busy during LTE to Wi-Fi handoff.
ho-disc-aaa-network-failure	The total number of sessions disconnected due to network failure during LTE to Wi-Fi handoff .
ho-disc-aaa-roaming-not-allowed	The total number of sessions disconnected due to roaming not allowed during LTE to Wi-Fi handoff.
ho-disc-aaa-rat-disallowed	The total number of sessions disconnected due to result code or experimental result code returned by Diameter during LTE to Wi-Fi handoff.
ho-disc-aaa-no-subscription	The total number of sessions disconnected due to non subscription of AAA during LTE to Wi-Fi handoff.
ho-disc-aaa-operator-policy	The total number of disconnected sessions due to lack of suitable operator policy configuration during LTE to Wi-Fi handoff.
ho-disc-aaa-no-non-3gpp-subscript	The total number of sessions disconnected due to AAA cause codes mapped to 3GPP IKEv2 private notify payload error type "#9000 No Non 3gpp Subscription" during LTE to Wi-Fi handoff.
ho-disc-aaa-user-unknown	The total number of sessions disconnected due to AAA cause codes mapped to 3GPP IKEv2 private notify payload error type "#9001 User Unknown" during LTE to Wi-Fi handoff.
ho-disc-aaa-illegal-equipment	The total number of sessions disconnected due to AAA cause codes mapped to 3GPP IKEv2 private notify error payload type "#9006 Illegal ME" during LTE to Wi-Fi handoff.
ho-disc-pgwselectfail-handoff	The total number of disconnected sessions due to P-GW selection failure during LTE to Wi-Fi handoff.
suppress-intr-roaming-ho-active	Indicates the current number of active ePDG sessions for which international roaming handoff attempts succeeded.

MME Schema

The following bulkstatistics are added in the MME schema as part of the N26 Interface Support feature:

Counters	Description
mme-decor-ue-usage-type-src-peer-amf	Displays the the number of MME subscriber sessions, where UE usage type was obtained from peer AMF as part of handover.
n1-mode-atttach-req	Displays the total number of Attach Requests received with N1 mode supported.

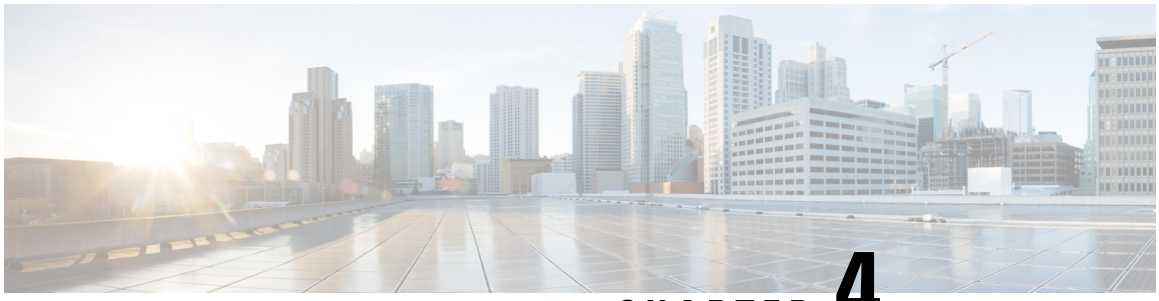
Counters	Description
n1-mode-tau-req	Displays the total number of TAU Requests received with N1 mode supported.
n1-mode-dns-pgw-selection-smf	Displays the total number of times P-GW selection procedures were performed with locally configured P-GW address, without considering the N1 Mode network capability.
n1-mode-dns-pgw-selection-nr	Displays the number of times P-GW DNS selection procedures are performed with DNS RR including the NR network capability.
n1-mode-dns-pgw-selection-common	Displays the number of times P-GW DNS selection procedures are performed with DNS RR excluding the N1 Mode network capability.
n1-mode-dns-pgw-selection-local	Displays the total number of times P-GW selection procedures were performed with locally configured P-GW address, without considering the N1 Mode network capability.

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.25

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.25 software release.

SNMP MIB Alarm Changes for 21.25

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

SNMP MIB Conformance Changes for 21.25

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

SNMP MIB Object Changes for 21.25

This section provides information on SNMP MIB alarm changes in release 21.25.

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

New SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.25.

- starSessMgrInstanceNumber
- starSessMgrCallCount
- starSessUnevenCallDistThrldStr
- starSgiReachabilityContextName

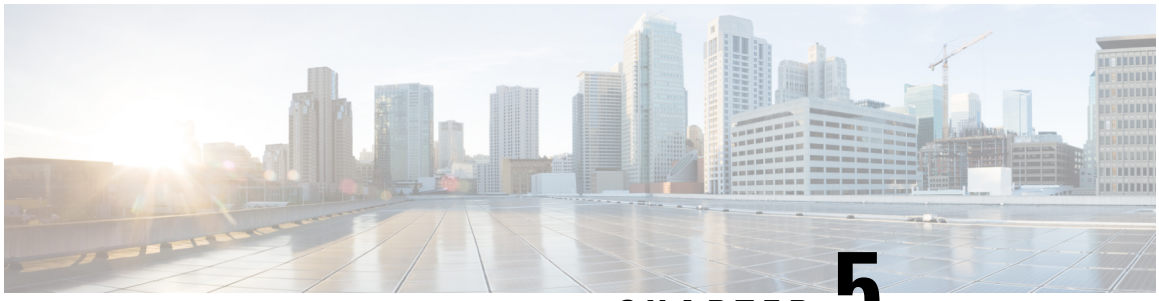
- starSgiReachabilityPgwIPAddr
- starSgiReachabilityApnName
- sessionUnevenDistribution
- sessionUnevenDistributionClear
- starSgiReachabilityAPNDown
- starSgiReachabilityAPNUp

Modified SNMP MIB Object

There are no modified SNMP MIB objects in this release.

Deprecated SNMP MIB Object

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



CHAPTER 5

5GS Interworking using N26 Interface Support

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
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 5GS interworking with N26 interface in compliance with 3GPP 5GS standards. Interworking procedures using the N26 interface, enables the exchange of Mobilty Management (MM) and Session Management (SM) states between the source and target network.

5GS interworking with N26 interface, the User Equipment (UE) operates in the single registration mode. MME supports N26 interface between Access and Mobility Management Function (AMF) in 5GC and MME in EPC to provide seamless session continuity (for example, for voice services) for single registration mode UE. For the 3GPP access, the network keeps only one valid MM state for the UE either in the AMF or MME.

MME uses either the static or dynamic mechanism to select PGW-C+SMF and peer-AMF.

MME supports the following interworking procedures with N26 interface:

- Attach
- EPS to 5GS Mobility Registration
- 5GS to EPS Idle Mode Mobility
- 5GS to EPS Handover
- EPS to 5GS Handover
- 5GS to EPS Handover Cancel
- EPS to 5GS Handover Cancel

Supported IEs and AVPs

MME supports the following IEs for the 5GS interworking feature:

S1AP (eNodeB) Interface:

- **GUMMEI Type**— The S1-AP interface supports **mappedFrom5G** in the Globally Unique Mobility Management Entity Identifier (GUMMEI) type IE. If the UE was previously registered in 5GS, the UE provides a GUMMEI in Access Stratum signalling mapped from the 5G-GUTI and is indicated as **Mapped from 5G-GUTI**.
- **Handover Type**— This indicates the type of handover that was triggered in the source side. The Handover type IE currently supports **EPSto5GS** and **5GStoEPS** type.
- **Handover Restriction List**— This supports **Core Network Type Restrictions**, **NR Restriction in 5GS** and **Last NG-RAN PLMN Identity**.

Note MME currently includes only one serving PLMN in Core Network Restrictions Type IE.

- **Target ID**—This supports **Global RAN Node ID** and **Selected TAI(5GS TAI)**.

Note Global ng-eNB under Global RAN Node ID is currently not supported.

NAS (UE) Interface

- **UE Network Capability (N1-mode)** — MME supports N1-mode handling in theUE Network Capability IE. For UE that supports N1 mode, the UE sets the N1 mode bit to **N1 mode supported** in the UE network capability IE of the ATTACH REQUEST/TRACKING AREA UPDATE REQUEST message.
- **UE Status IE** — MME supports UE Status IE in the ATTACH REQUEST/TRACKING AREA UPDATE REQUEST message and provides the network with information related to the current UE registration status that is used for interworking with 5GS.
- **EPS Network Feature Support (IWK N26)** — MME supports IWK N26 indicator to specify whether interworking without N26 interface is supported or not in ATTACH ACCEPT/TAU ACCEPT message.

S6a (HSS) Interface

- **Interworking-5GS-Indicator AVP** — MME supports Interworking-5GS-Indicator to indicate whether the interworking between 5GS and EPS is subscribed or not subscribed for the APN.
- **Core-Network-Restrictions AVP** — MME supports Core-Network-Restrictions to indicate the types of Core Network that are disallowed for a user.
- **Access-Restriction-Data AVP** — MME supports bit 10 NR in 5GS Not Allowed to check whether NR is 5GS is Allowed or Not Allowed. The Access-Restriction-Data AVP is of type Unsigned32 type and contains a bit mask where each bit when set to 1 indicates a restriction.

S11 (SGW) Interface:

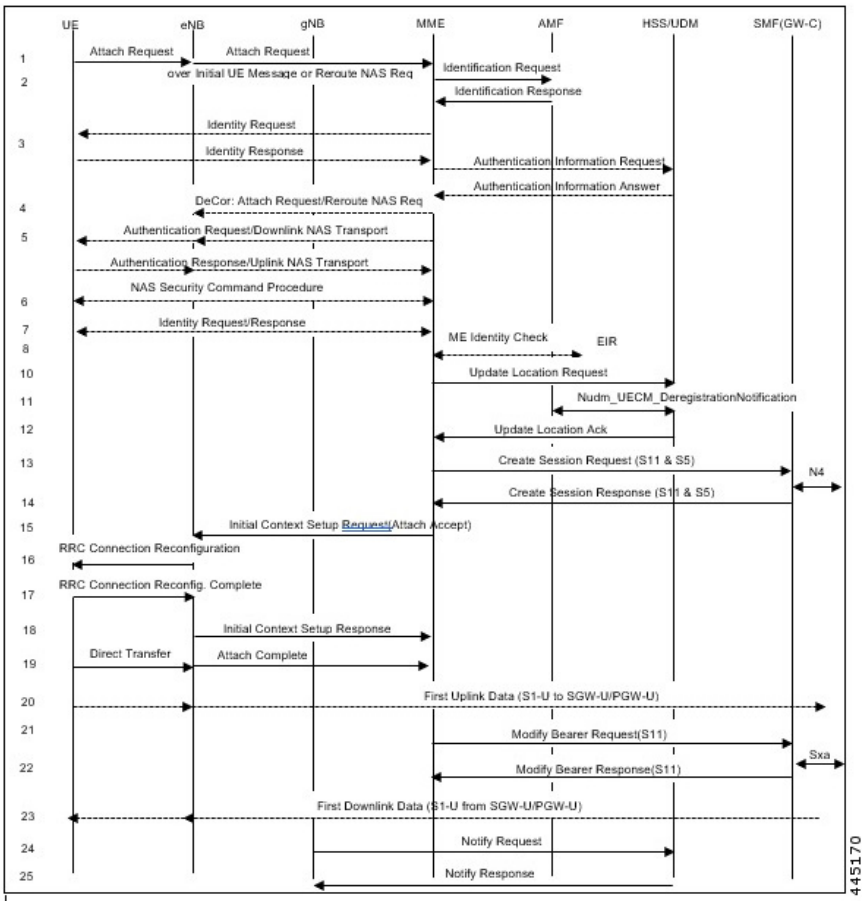
- **Indication Flag** — MME supports 5GSIWKI (5GS Interworking Indication) and REPREFI (Return Preferred Indication) flags.

How it Works

This section describes the call flow procedures related to 5GS interworking with N26 interface.

The following call flow describes the working of 5Gs to EPS attach procedure.

Figure 1: E-UTRAN Initial Attach Call Flow



E-UTRAN Initial Attach Procedure

The following table describes 5GS to EPS attach procedure.

Table 2: E-UTRAN Initial Attach Procedure

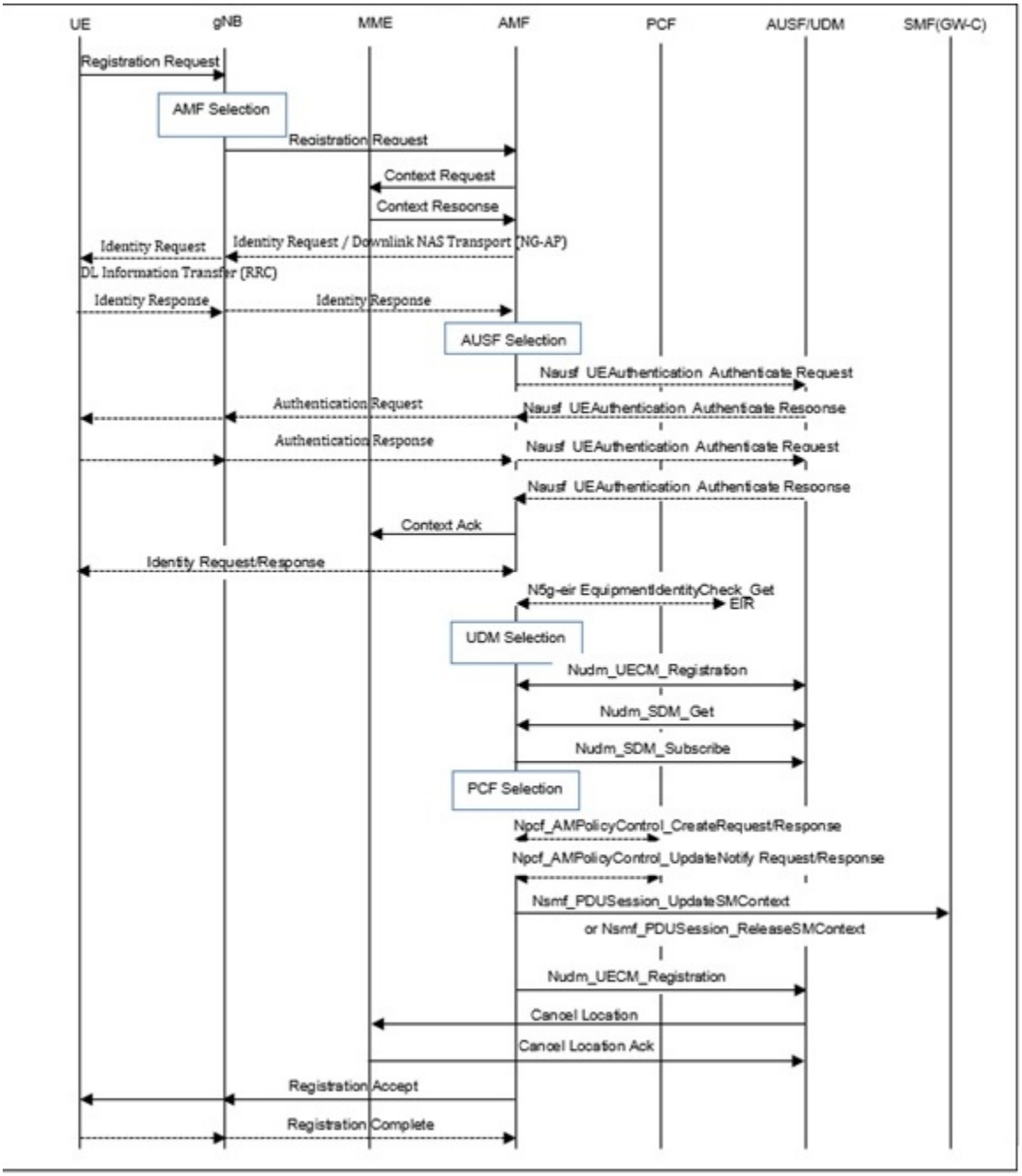
Step	Description
1	Attach Request is carried over Initial UE Message with following conditions: • UE includes N1-mode capability in the **UE Network Capability IE**. • UE includes GUMMEI in the S1-AP message and. indicates that GUMMEI is Mapped from 5G-GUTI. • UE includes a GUTI, mapped from 5G-GUTI into the EPS mobile identity IE, includes old GUTI type IE with GUTI type set to **native GUTI** and includes the UE status IE with a 5GMM registration status set to **UE is in 5GMM-DEREGISTERED state**.
2	MME construct the 5G-GUTI from the received GUTI IE according to the mapping relationship between GUTI and 5G-GUTI defined in 3GPP TS 23.003. MME uses the constructed 5G GUTI to determine the peer AMF address based on DNS or local Static AMF GUAMI configuration. If MME is unable to find the peer AMF address, the new MME sends an Identity Request to the UE to request the IMSI. The UE responds with Identity Response (IMSI).
3	MME sends Identification Request message to the selected peer AMF. .
4	AMF responds with Identification Response message **Note** MME sends Identification Request to the peer AMF irrespective of the "n1-mode" configuration in CC profile (or) MME Service and the feature support check is performed after receiving "Identification Response" message from peer AMF. If the feature support is disabled (or) the UE is unknown in the old AMF, MME initiates Identity procedure with UE.
5	MME sends Update Location Request to HSS and will not set the Dual-registration 5G-indication in ULR-Flag.
6	MME processes and handles the below AVP in the ULA from HSS. MME uses the received information for Mobility restrictions and PGW-C+SMF gateway selection: • Interworking-5GS-Indicator • Core-Network-Restriction • Access-Restriction-Data (NR in 5GS Not Allowed) AVP
7	MME selects PGW-C+SMF based on UE Network capability and mobility restrictions based on the following mechanisms: • Static configuration • Dynamic DNS configuration
8	MME sets the **5GS Interworking Indication** in Indication flags in the Create Session Request and sends to the selected P-GW-C+SMF gateway. MME does not set the Indication bit if Standalone P-GW-C is selected.

Step	Description
9	If the MME receives ePCO from the UE during the Initial Attach or UE requested PDN Connectivity procedures, the MME forwards the ePCO IE to the SGW, if the MME supports ePCO. The SGW shall also forward it to the PGW if the SGW supports ePCO.
10	If UE supports N1 mode in UE network capability, and the Interworking-5GS-Indicator is set to subscribed, MME sets IWKN26 bit to **Interworking without N26 interface not supported** in the Attach Accept message.

EPS to 5GS Mobility Registration Call Flow

The following call flow describes the registration procedure from EPS to 5GS Mobility when, N26 interface is supported for idle and connected states.

Figure 2: EPS to 5GS Mobility Registration Call Flow



The following table describes the procedure to register from EPS to 5GS.

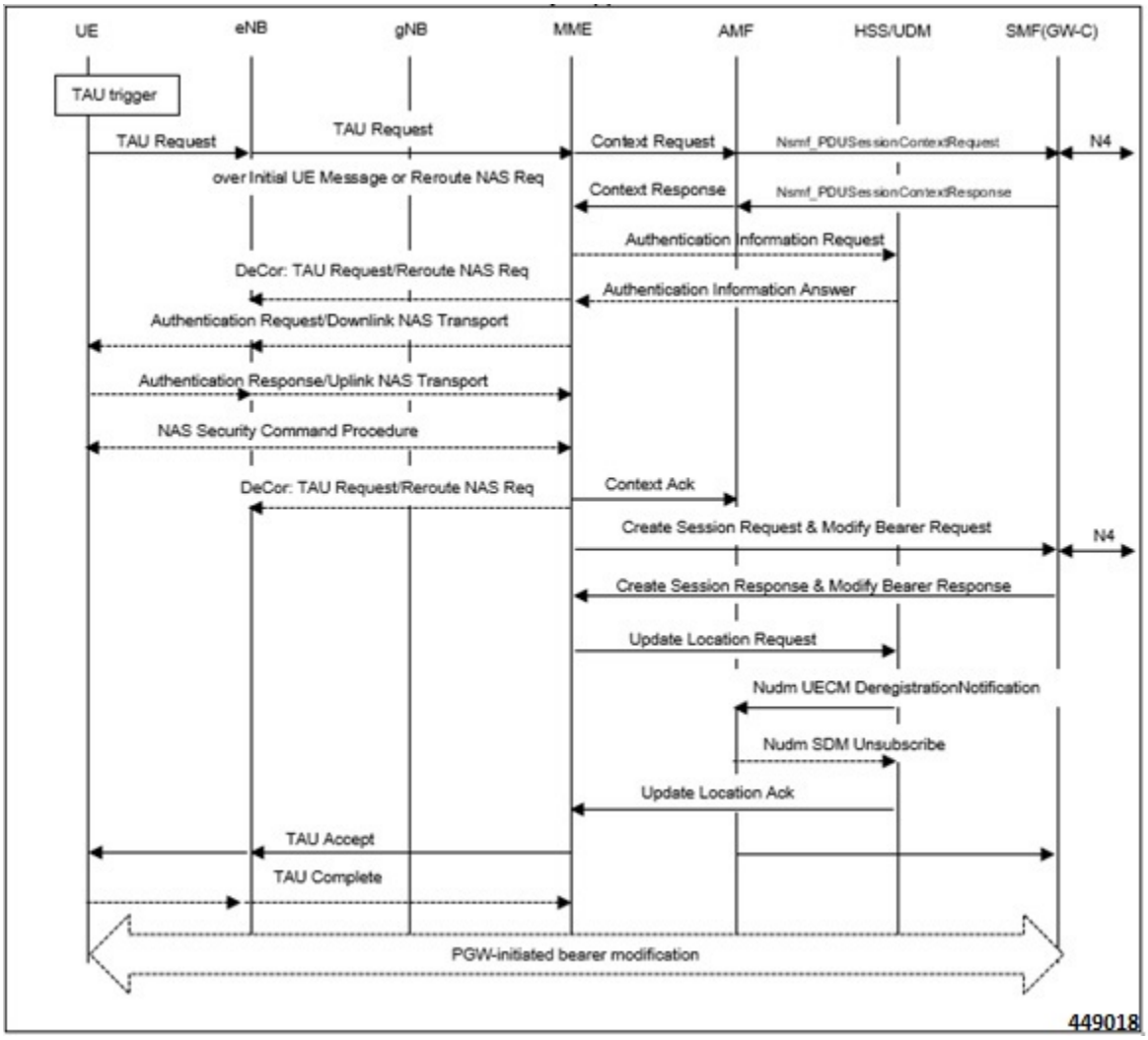
Table 3: EPS to 5GS Mobility Registration Procedure

Step	Description
1	For IDLE mode mobility, the target AMF derives the MME address and 4G GUTI from the old 5G-GUTI and sends Context Request to MME including EPS GUTI mapped from 5G-GUTI and the TAU request message according to TS 23.401. The MME validates the TAU message. **Note** • MME supports FTEID Interface types **S10/N26 MME GTP-C interface (12)** and **N26 AMF GTP-C interface (40)** received in the **Context Request** message from peer AMF. • MME would use the RAT type NR in the **Context Request** message to determine if the peer is AMF.
2	MME includes EPS MM Context, IMSI, ME Identity, UE EPS security context, UE Network Capability, and EPS Bearer context(s) in the Context Response message and sends to the peer AMF. The MME EPS Bearer context includes for each EPS PDN connection the IP address and FQDN for the S5/S8 interface of the PGW-C+SMF and APN. MME also includes in the Context Response new information Return Preferred. Return Preferred is an indication by the MME of a preferred return of the UE to the last used EPS PLMN at a later access change to an EPS shared network. Based on the Return Preferred indication, the AMF stores the last used EPS PLMN ID in UE Context. MME sends Context Response failure if feature support is disabled, Unknown RAT type other than NR is received (or) mobility is restricted.
3	The target AMF sends Context Acknowledge (Serving GW change indication) to MME.
4	HSS+UDM cancels the location of the UE in the MME.

5GS to EPS Idle Mode Mobility Call Flow

The following call flow describes the idle and connected states.

Figure 3: 5GS to EPS Idle Mode Mobility Call Flow



UE performs Tracking Area Update (TAU) procedure in E-UTRA/EPS when it moves from NG-RAN/5GS to E-UTRAN/EPS coverage area. The procedure involves a Tracking Area Update to EPC and setup of default EPS bearer and dedicated bearers in EPC and re-activation, if required.

Table 4: 5GS to EPS Idle Mode Mobility Procedure

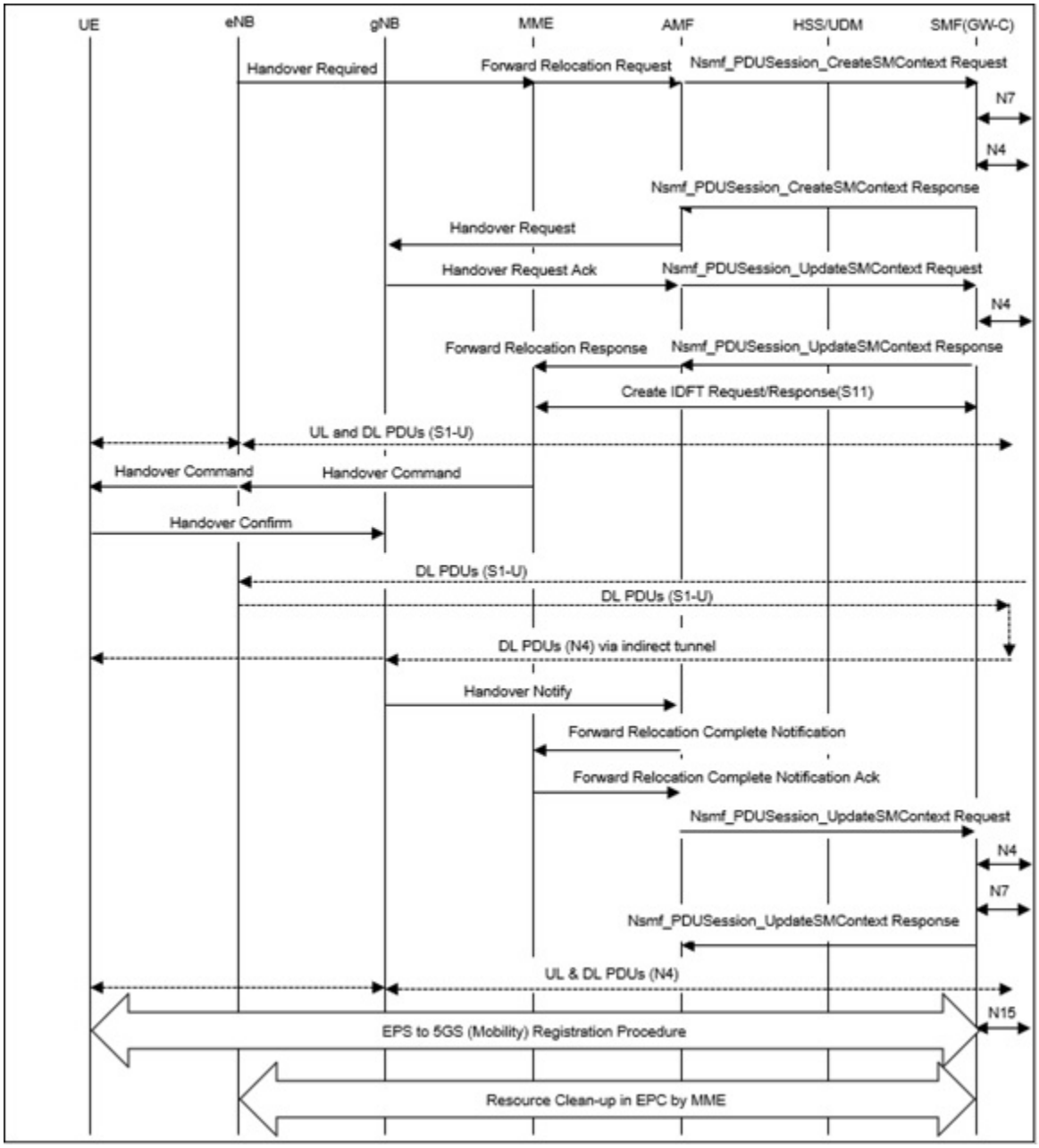
Step	Description
1	Tracking Area Update Request is carried over Initial UE Message with following conditions: • UE includes N1-mode capability in the **UE Network Capability** IE. • UE includes GUMMEI in the S1-AP message and indicates that GUMMEI is Mapped from 5G-GUTI. • UE includes a GUTI, mapped from 5G-GUTI into the EPS mobile identity IE, includes old GUTI type IE with GUTI type set to **native GUTI** and includes the UE status IE with 5GMM registration status set to **UE is in 5GMM-REGISTERED** state.

Step	Description
2	MME constructs the 5G-GUTI from the received GUTI IE according to the mapping relationship between GUTI and 5G-GUTI defined in 3GPP TS 23.003. MME uses the constructed 5G GUTI to determine the peer AMF address based on DNS or local Static AMF GUAMI configuration. If MME is unable to find the peer AMF address, the new MME rejects the TAU Request.
3	MME sends Context Request message to the selected peer AMF.
4	The AMF responds with a Context Response message carrying mapped MM context (including mapped security context), UUT, Return preferred and SM EPS UE Context (default and dedicated GBR bearers) to the MME. If the verification of the integrity protection fails, the AMF returns an appropriate error cause. Return preferred is an optional indication by the AMF of a preferred return of the UE to the 5GS PLMN at a later access change to a 5GS shared network. The PDN GW Address and TEID(s) is part of the EPS Bearer Context for PDN connection in Context Response. However, SGW S11 IP address and TEID for Control Plane is not provided by AMF. **Note** . • MME supports **S10/N26 MME GTP-C** and **N26 AMF GTP-C** FTEID Interface types from peer AMF. • MME sends Context Request to the peer AMF irrespective of the **n1 mode** configuration in CC profile (or) MME Service and the feature support check is performed after receiving **Contect Response** message from peer AMF. If the feature support is disabled, MME rejects the TAU Request and sends the Context Acknowledgement failure.
5	MME selects new SGW-C and send Create Session Request towards the SGW. MME will set the **5GS Interworking Indication** in Indication Flags in the Create Session Request message.
6	MME sends Update Location Request to HSS and will not set the Dual-registration 5G-indication in ULR-Flag.
7	MME processes and handles the following AVPs in the ULA from HSS. • Interworking-5GS-Indicator • Core-Network-Restriction • Access-Restriction-Data (NR in 5GS Not Allowed) AVP. MME uses the received information for Mobility restrictions and PGW-C+SMF gateway selection.
8	If UE supports N1 mode in UE network capability, and the Interworking-5GS-Indicator is set to subscribed, MME shall set IWKN26 bit to “Interworking without N26 interface not supported” in TAU Accept.

EPS to 5GS Handover Call Flow

The following call flow describes the EPS to 5GS handover using N26 interface.

Figure 4: EPS to 5GS Handover Call Flow



The following table describes the handover procedure from EPS to 5GS using N26 interface. 5GS Mobility Registration Procedure is performed, and steps from Context Request to Context Acknowledgement are skipped during the handover to 5GS.

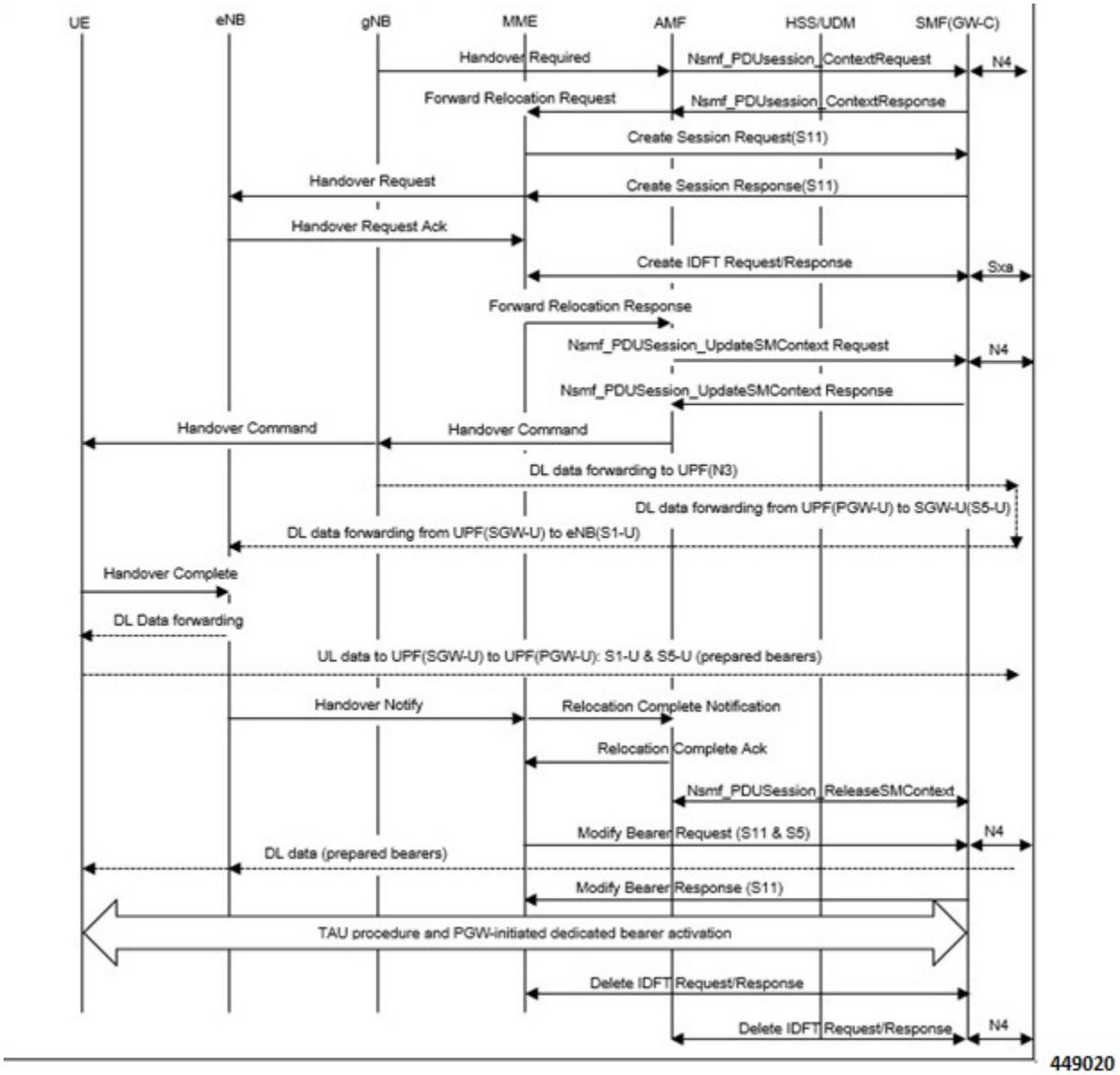
Table 5: EPS to 5GS Handover Procedure

Step	Description
1	MME receives Handover Required from eNB with the Handover type set **EPSto5GS**, Target ID with Global gNB ID and selected 5GS TAI information. **Note** Global ng-eNB is currently not supported.
2	MME uses the 5GS TAI information to determine the peer AMF address based on DNS or local Static AMF TAI configuration. If MME is unable to find the peer AMF address or the feature is disabled, MME sends Handover preparation failure to eNB.
3	MME sends Forward Relocation Request message to the selected peer AMF with the following information: • MME includes EPS MM Context, IMSI, ME Identity, UE security context, UE Network Capability, and EPS Bearer context(s) in the Forward Relocation Request message. The MME EPS Bearer context(s) includes for each EPS PDN connection the IP address and FQDN for the S5/S8 interface of the PGW-C+SMF and APN, and for each EPS bearer the IP address and CN Tunnel Info at the UPF+PGW-U for uplink traffic. • MME includes an additional optional parameter Return preferred; Return preferred is an optional indication provided by the MME to indicate a preferred return of the UE to the last used EPS PLMN at a later access change to an EPS shared network. Based on the Return Preferred indication, the AMF stores the last used EPS PLMN ID in the UE Context.
4	MME receives Forward Relocation Response (Cause, Target to Source Transparent Container, S-GW change indication, CN Tunnel Info for data forwarding, EPS Bearer Setup List, AMF Tunnel Endpoint Identifier for Control Plane, Addresses and TEIDs) from AMF. The EPS Bearer Setup list is the combination of EPS Bearer Setup list from different P-GW-C+SMF(s). **Note** MME supports **S10/N26 MME GTP-C** and **N26 AMF GTP-C** FTEID Interface types from peer AMF.
5	The source MME sends Create Indirect Data Forwarding Tunnel Request (addresses and TEIDs for forwarding) to the S-GW. If the S-GW is relocated it includes the tunnel identifier to the target S-GW. The S-GW responds with a Create Indirect Data Forwarding Tunnel Response (S-GW addresses and TEIDs for forwarding) message to the source MME.
6	The source MME sends a Handover Command (Target to Source transparent container, Bearers subject to forwarding, Bearers to Release) message to the source eNodeB. The Bearers subject to forwarding includes list of addresses and TEIDs allocated for forwarding. The Bearers to Release includes the list of bearers to be released.
7	The NG-RAN notifies the AMF that UE is handover over to NG-RAN and AMF sends Forward Relocation Complete Notification message to the source MME. The source MME in response sends a Forward Relocation Complete Acknowledge message to the target AMF.

5GS to EPS Handover Call Flow

The following call flow describes the 5GS to EPS handover using N26 interface.

Figure 5: 5GS to EPS Handover Call Flow



The following table describes the handover procedure from 5GS to EPS using N26 interface.

Table 6: 5GS to EPS Handover Procedure

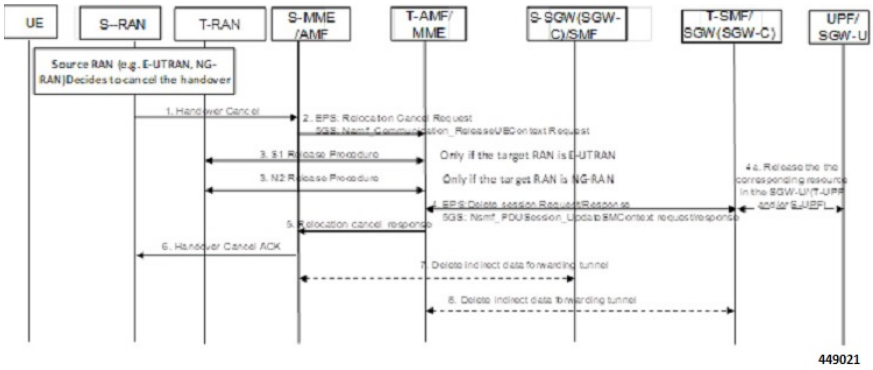
Step	Description
1	MME receives Forward Relocation Request message from AMF. AMF shall include **Return preferred Indication** to indicate preferred return of the UE to the 5GS PLMN at a later access change to a 5GS shared network. AMF includes reserved S-GW address and TEID for both the control plane or EPS bearers in the message. **Note** • MME supports FTEID Interface types **S10/N26 MME GTP-C interface (12)** and **N26 AMF GTP-C interface (40)** received in the **Context Request** message from peer AMF. • MME would use the SGW-C FTEID reserved **TEID** values in the Forward Relocation Request message to determine if the peer is AMF. • If the feature support is disabled, the MME sends Forward Relocation Response failure to peer AMF with cause **Service not supported** .
2	MME selects a new S-GW-C and would send Create Session Request to S-GW and receives Create Session Response from S-GW.
3	MME sends Handover Request message towards eNB with Handover type “5GStoEPS” and includes the Handover Restriction list for eNodeB functions.
4	The target eNodeB sends a Handover Request Acknowledge (EPS Bearer Setup list, EPS Bearers failed to setup list Target to Source transparent container) message to the target MME. The EPS Bearer Setup list includes a list of addresses and TEIDs allocated at the target eNodeB for downlink traffic on S1-U reference point (one TEID per bearer) and addresses and TEIDs for receiving forwarded data if necessary.
5	IDFT enabled MME initiates create IDFT Request message to SMF/GW-C and receives create IDFT response messages from SMF/GW-C.
6	The target MME sends a Forward Relocation Response (Cause, Target to Source transparent container, Serving GW change indication, EPS Bearer Setup List, Addresses and TEIDs) message to the source MME. **Note** For indirect forwarding, this message includes S-GW Address and TEIDs for indirect forwarding (source or target). S-GW change indication indicates that a new S-GW has been selected.
7	The target eNodeB sends a Handover Notify (TAI+ECGI, Local Home Network ID) message to the target MME.
8	The target MME sends a Relocation Complete Notification message to the source AMF. The AMF acknowledges MME with Relocation Complete Acknowledgement message.
9	MME sends Modify bearer request to S-GW and receives Modify bearer response from S-GW.
10	UE initiates Connected mode Tracking Area Update procedure towards MME.

Step	Description
11	If PCC is deployed, the PCF provides the previously removed PCC rules to the P-GW-C+SMF, which triggers the P-GW-C+SMF to initiate dedicated bearer activation procedure and the dedicated Bearer gets activated at MME.

Handover Cancellation Procedure

This section describes Handover cancelation call flow and procedures from EPS to 5GS and from 5GS to EPS.

Figure 6: EPS to 5GS Handover Cancel Call Flow



EPS to 5GS Handover Cancel Procedure

1. The source eNB decides to cancel the previously requested relocation of Handover resources. This may be due to not enough accepted bearers, UE returned to source cell or any other reason.
2. MME terminates the relocation towards the AMF by sending a Relocation Cancel Request message to AMF. MME also resumes operation on the resources in the source side.
3. The AMF acknowledges the release of all resources on the target side by returning a Relocation Cancel Response (Cause) message to the source MME.
4. If indirect forwarding tunnel is setup during handover preparation, then cancellation of handover triggers the MME to send a Delete Indirect Data Forwarding Tunnel Request message to the S-GW to release the temporary resources used for indirect forwarding.

5GS to EPS Handover Cancel Procedure

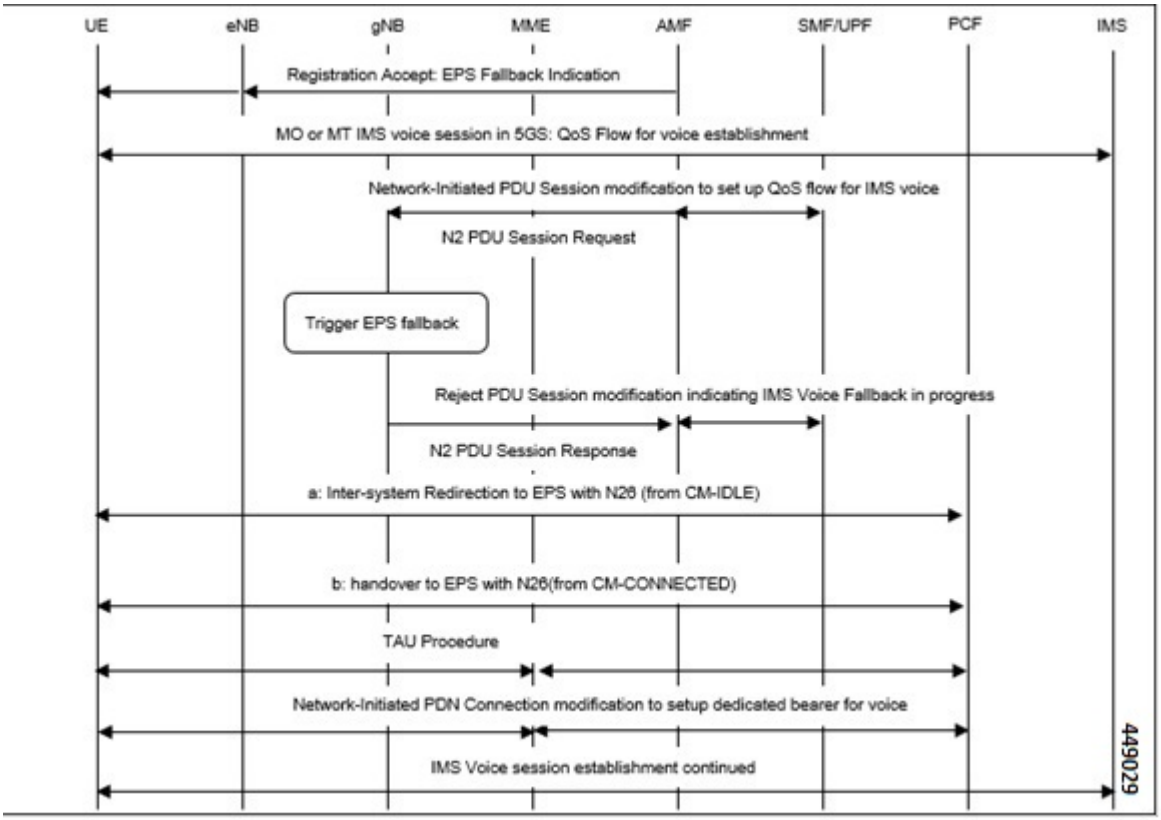
1. MME receives **Relocation Cancel Request** from AMF.
2. MME triggers release of resources towards target RAN node. The target RAN node releases the RAN resource allocated for the handover.
3. MME sends the **Delete session request** (IMSI, Relocation Cancel Indication) to the S-GW/S-GW-C. Based on the Relocation Cancel Indication, MME deletes the session resources established during handover preparation phase in S-GW (S-GW-C and S-GW-U).
4. MME sends **Relocation Cancel Response** towards the AMF.

5. AMF responds with handover cancel ACK towards the source RAN.
6. If indirect forwarding tunnel is setup during handover preparation phase, then cancellation of handover triggers MME to release the temporary resources used for indirect forwarding.

EPS Fallback for IMS Voice Support

MME supports EPS fallback for IMS voice according to 3GPP 23.502.

Figure 7: EPS Fallback for IMS Voice



Combined PGW-C and SMF Selection Procedure

MME supports DNS and Static PGW-C/SMF combined Gateway selection. You can configure PGW-C+SMF in MME Service and in APN profile configuration commands for static gateway selection. 5GSIWKI is set when combined PGW-C/SMF node is selected.

The following steps explain the static based combined P-GW-C/SMF selection procedure and how the fallback to the next available option happens if the selection fails:

1. MME chooses Combined PGW-C/SMF node that supports UE usage type and collocation with S-GW.
2. If step 1 fails, MME selects the Combined PGW-C+SMF node that supports UE usage type.
3. If step 2 fails, MME selects the Combined PGW-C+SMF node that supports collocation with S-GW.

4. If step 3 fails, MME selects the Combined PGW-C+SMF node.
5. If step 4 fails, MME selects the gateway based on UE usage type and standalone PGW collocation.
6. If step 5 fails, MME selects the standalone PGW that supports UE usage type.
7. If step 6 fails, MME selects the gateway that supports standalone PGW collocation.
8. If step 7 fails, MME selects any gateway from all configured entries.

The following steps explain the DNS-based combined PGW-C+SMF selection procedure and how fallback occurs to the next available option if the selection fails:

1. MME selects a gateway matching the UE Usage type, DCNR, and SMF network capability.
2. If step 1 fails, MME selects the gateway matching the DCNR and SMF network capability.
3. If step 2 fails, MME selects the gateway matching the UE usage type and SMF network capability.
4. If step 3 fails, MME selects the gateway matching the SMF network capability.
5. If step 4 fails, MME selects the gateway matching the UE usage type and DCNR network capability.
6. If step 5 fails, MME selects the gateway matching the DCNR network capability.
7. If step 6 fails, MME selects the gateway matching the UE usage type.
8. If step 7 fails, MME selects the gateway matching the default service parameter.
9. If step 8 fails, MME selects the gateway based on local static configuration.

Note The above steps are only for reference purpose based on probable combination where UE/MME supports UUT, DCNR and SMF capability. The selection order varies/depends based on the DNS response, UE capability and MME configuration.

Limitations

This section describes the known limitations for the N26 interface functionality:

- Configuration Transfer Tunnel message is not supported.
- Feature-specific optional IEs are not supported. For example, Extended Trace Information IE.
- Default EGTP service is used for GTPv2 messages on N26 interface.
- A maximum of 32 peer-AMF entries can be configured for GUAMI or TAI configuration.
- NBIoT and CIOT optimization is not supported.
- PGW-C+SMF selection for Emergency Attach or Emergency PDN is not supported.

Supported Standards

The N26 feature support is compliant with the following standards:

- 3GPP 23.401 version 15.10.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 23.501 version 15.8.0 - System architecture for the 5G System (5GS
- 3GPP 23.502 version 15.8.0 - Procedures for the 5G System (5GS)
- 3GPP 33.501 version 15.7.0 - Security architecture and procedures for 5G System
- 3GPP 24.301 version 15.8.0 - Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)
- 3GPP 36.413 version 15.8.0 - S1 Application Protocol (S1AP)
- 3GPP 29.272 version 15.10.0 - Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP 29.274 version 15.9.0 - Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP 23.003 version 15.8.0 - Numbering, addressing and identification
- 3GPP 29.303 version 15.5.0 - Domain Name System Procedures

Configuring N26 Interface for MME

This section describes the configuration of 5GS Interworking support using N26 interface on MME.

Configuring 5GS Interworking using N26 Interface in Call Control Profile

Use the following configuration to enable 5GS Interworking support using N26 interface.

```
configure
  call-control-profile profile_name
    [ no | remove] n1-mode 5gs-interworking-with-n26
    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 5GS-EPS interworking with N26 interface.
- **remove**: Removes the configuration from the Call Control profile and the MME Service configuration applies.

Peer AMF Configuration

Configure Peer AMF GUAMI

Use the following configuration to statically configure the peer AMF address in MME service.

```
configure
  context context_name
    mme service service_name
      peer-amf guami { mcc mcc_value mnc mnc_value region-id region_id set-id
 set_id pointer pointer_value address { ipv4_address | ipv6_address }
      [ no ] peer-amf guami { mcc mcc_value mnc mnc_value region-id region_id
 set-id set_id pointer pointer_value }
      end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* must be an alphanumeric string of 1-63 characters.
- **peer-amf**: Configures a Peer AMF for 5Gs interworking.
- **guami**: Configures Globally Unique AMF Identifier for this Peer.
- **mcc**: Configures the Mobile Country Code for this Peer AMF.
- **mnc**: Configures the Mobile Network Code for this Peer AMF.
- **region-id**: Configures the Region Identifier for this Peer AMF.
- **set-id** : Configures the Set Identifier for this Peer AMF.
- **pointer**: Configures the Pointer value for this Peer AMF.
- **address**: Configures address of Peer AMF. Must be followed by address using dotted-decimal notation. This can also be specified as an IPv6 address.

Configure Peer AMF TAI

```
configure
  context context_name
    mme service service_name
     peer-amf tai-match priority { val mccmcc_value mnc mnc_value tac area_code
 address { ipv4_address | ipv6_address }
      [ no ] peer-amf tai-match priority  val
      end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* must be an alphanumeric string of 1-63 characters.
- **peer-amf**: Configures a Peer AMF for 5Gs interworking.
- **tai-match**: Configures 5GS Tracking Area Information match for this Peer AMF.
- **mcc**: Configures the Mobile Country Code for this Peer AMF.
- **mnc**: Configures the Mobile Network Code for this Peer AMF.
- **address**: Configures address of Peer AMF. Must be followed by address using dotted-decimal notation. This can also be specified as an IPv6 address.

Configure PGW-C with SMF Combined

Use the following command to configure the PGW-C with smf combined configuration in mme-service.

```
configure
   context context_name
      mme service service_name
         [ no ] pgw-address ipv4_address | ipv6_address ue-usage-type  UUT_Value
collocated-node collocated_name smf-combined   weightweight_value
        end
```

Use the following command to configure the P-GW-C with smf combined configuration in apn-call-control-profile.

```
configure
   context context_name
      apn profile profile_name
         [ no ] pgw-address ipv4_address | ipv6_address ue-usage-type  UUT_Value
collocated-node collocated_name smf-combined
        end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* must be an alphanumeric string of 1-63 characters.
- **pgw-address**: Configures p-gw address. Must be followed by address using dotted-decimal notation. This can also be specified as an IPv6 address.
- **ue-usage-type** : Configures UE usage type for disconnecting PDN for up service area.
- **collocated-node**: Configures the Collocation name to select the collocated S/PGW node IP addresses and/or P-GW Node name for 5GS Interworking.

Note Make sure to configure P-GW Node name under **Collocated-node** for 5GS interworking with N26 interface. This configuration allows P-GW Node Name IE to include the configured name in **Context Response** and **Forward relocation Request** messages from MME to AMF over N26 interface.

- **smf-combined** : Configures a combined P-GW and SMF.
- **no**: Removes the configured PGW address.

Configuring DNS Peer AMF

Use the following sample configuration to configure peer-AMF selection using the DNS interface:

```
configure
   mme-service mme_svc_name
      dns peer-amf
      end
```

NOTES:

- **dns peer-amf**: MME sends a DNS query to the DNS server for selecting AMF.

Note The **dns pgw** command under MME Service and Call Control Profile can be reused to configure DNS to select the PGW-C+SMF address.

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 mme-service statistics output

The output of this command includes the following fields:

Field	Description
Outbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS mobility procedure.
Outbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS handover procedure.
Inbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of Inbound relocation using EPS-5GS mobility procedure.
Inbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of Inbound relocation using EPS-5GS handover procedure.

show mme-service statistics recovered-values output

The output of this command includes the following fields:

Field	Description
Outbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS mobility procedure.
Outbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS handover procedure.
Inbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS mobility procedure.
Inbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of Inbound relocation using EPS-5GS handover procedure.

show mme-service statistics 5gs-interworking

Table 7: show mme-service statistics 5gs-interworking Command Output Descriptions

Field	Description
Attach Request Rcvd	Displays the number of Attach Request messages received with UE advertising N1 Mode support.
TAU Request Rcvd	Displays the number of TAU Request messages received with UE advertising N1 Mode support.
SMF-Combined	Displays the number of times P-GW DNS selection procedures performed with DNS RR including the N1 Mode network capability.
NR Capable	Displays the number of times P-GW DNS selection procedures performed with DNS RR including the NR network capability.
Common	Displays the number of times P-GW DNS selection procedures performed with DNS RR excluding the N1 Mode network capability.
PGW Local Config	Displays the number of times P-GW selection procedures performed with locally configured P-GW address, without considering the N1 Mode network capability.

show session disconnect-reasons

The output of this command includes the following fields:

Field	Description
mme-reselection-to-amf	This disconnect reason is incremented, if the subscriber reselects AMF as part of the EPS to 5GS Idle Mobility Registration procedure.

Field	Description
mme-relocation-to-amf	This disconnect reason is incremented, if the subscriber relocates to AMF as part of the EPS to 5GS Handover procedure.

Bulk Statistics

MME Schema

MME Service Bulk Statistics

The following MME Service bulk statistics are included in the MME Schema.

Counters	Description
out-mob-4gto5g-n26-attempted	Displays the total number of attempted outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
out-mob-4gto5g-n26-success	Displays the total number of successful outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface
out-mob-4gto5g-n26-failures	Displays the total number of failed outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
out-ho-4gto5g-n26-attempted	Displays the total number of attempted outbound relocation using EPS to 5GS Handover procedure in N26 interface.
out-ho-4gto5g-n26-success,	Displays the total number of successful outbound relocation using EPS to 5GS Handover procedure in N26 interface.
out-ho-4gto5g-n26-failures	Displays the total number of failed outbound relocation using EPS to 5GS Handover procedure in N26 interface.
in-mob-5gto4g-n26-attempted	Displays the total number of attempted inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-mob-5gto4g-n26-success	Displays the total number of successful inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-mob-5gto4g-n26-failure	Displays the total number of failed inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-ho-5gto4g-n26-attempted	Displays the total number of attempted inbound relocation using 5GS to EPS Handover procedure in N26 interface.
in-ho-5gto4g-n26-success	Displays the total number of successful inbound relocation using 5GS to EPS Handover procedure in N26 interface.
in-ho-5gto4g-n26-failures	Displays the total number of failed inbound relocation using 5GS to EPS Handover procedure in N26 interface.

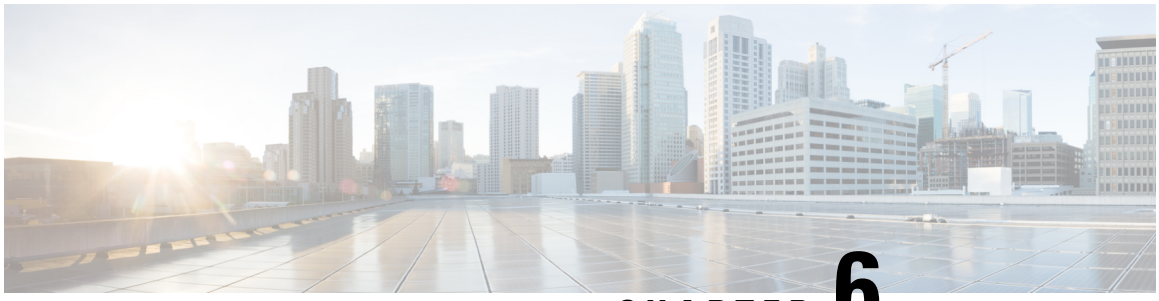
Counters	Description
mme-decor-ue-usage-type-src-peer-amf	Displays the the number of MME subscriber sessions, where UE usage type was obtained from peer AMF as part of handover.
n1-mode-atttach-req	Displays the total number of Attach Requests received with N1 mode supported.
n1-mode-tau-req	Displays the total number of TAU Requests received with N1 mode supported.
n1-mode-dns-pgw-selection-smf	Displays the total number of times P-GW selection procedures were performed with locally configured P-GW address, without considering the N1 Mode network capability.
n1-mode-dns-pgw-selection-nr	Displays the number of times P-GW DNS selection procedures are performed with DNS RR including the NR network capability.
n1-mode-dns-pgw-selection-common	Displays the number of times P-GW DNS selection procedures are performed with DNS RR excluding the N1 Mode network capability.
n1-mode-dns-pgw-selection-local	Displays the total number of times P-GW selection procedures were performed with locally configured P-GW address, without considering the N1 Mode network capability.

MME Service Backup Bulk Statistics

The following MME Service backup bulk statistics are included in the MME-BK Schema.

Counters	Description
recovered-out-mob-4gto5g-n26-attempted	Shows recovered values for total number of attempted outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
recovered-out-mob-4gto5g-n26-success	Shows recovered values for total number of successful outbound relocation using EPS to 5GS idle mode mobility procedure in N26 interface.
recovered-out-ho-4gto5g-n26-attempted	Shows recovered values for total number of attempted outbound relocation using EPS to 5GS Handover procedure in N26 interface.
recovered-out-ho-4gto5g-n26-success	Shows recovered values for total number of successful outbound relocation using 5GS to EPS handover procedure in N26 interface.
recovered-in-mob-5gto4g-n26-attempted	Shows recovered values for total number of attempted inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
recovered-in-mob-5gto4g-n26-success	Shows recovered values for total number of successful inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.

Counters	Description
recovered-in-ho-5gto4g-n26-attempted	Shows recovered values for total number of attempted inbound relocation using 5GS to EPS Handover procedure in N26 interface.
recovered-in-ho-5gto4g-n26-success	Shows recovered values for total number of successful inbound relocation using 5GS to EPS Handover procedure in N26 interface.



CHAPTER 6

Adding ECPD Identification and Account Numbers to Pilot Packets

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The Pilot Packet feature provides key information about a subscriber session, such as subscriber identity and subscriber IP address, to an external element. When the subscriber allocates or deallocates IP address during an event trigger, a “pilot” packet is generated. Using this information new service such as Subscriber Analytics are enabled and sent in UDP transport.

Pilot Packet consists of the following information in the form of Type Length Values (TLVs):

- Allocation/De-allocation Flag
- MSISDN (MDN)
- IMSI
- Allocated Address-IPv4
- Allocated Address-IPv6-Address
- Allocated NAT IPv4 Address
- NAT Address Port Chunk Start
- NAT Address Port Chunk Size
- Serving Network Identifier
- Foreign Agent IP Address
- NAI
- RAT Type

The operator enables the network element with Pilot packet to gain and report enterprise-level information through the Flexible-Services-Container TLV on SGi interface.

Flexible-Services-Container consists of the following enterprise-level information:

- Enterprise Customer Profile Database Identification (ECPD ID)
- Account Number

For example: ECPD ID = 3458312; Account Number = 0442058164-00001

Notes

Following are the important notes:

- P-GW adds new TLV to the Pilot packet for subscribers, only if configured through CLI and received on S6b in AAA message.
- P-GW ignores Flexible-Services-Container received in the Re-Auth procedure.
- The contents and interpretation of the enterprise information (ECPD ID and Account Number) is not required for P-GW or GGSN services. The data is not parsed by P-GW or GGSN and passed transparently in Pilot packet.

Configuring Pilot Packet

To configure Pilot Packets containing key information about a subscriber session to third-party network elements, use the following configuration:

```
configure
   context context_name
     pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type
 | serving-nw-id | flexible-services-container } | name server_name
source-ip-address source_ip_address destination-ip-address destination-ip_address
 destination-udp-port udp_port_value [ dscp-marking dscp-value ] | trigger
rat-change generate { nat-info-only | user-info-and-nat-info |
user-info-only } }
     default pilot-packet { attribute { foreign-agent-ip-address | nai |
 rat-type | serving-nw-id | flexible-services-container } | trigger
rat-change }
     no pilot-packet { attribute { foreign-agent-ip-address | nai |
rat-type | serving-nw-id | flexible-services-container } | name server_name
 | trigger rat-change }
     end
```

NOTES:

- **pilot-packet { attribute flexible-services-container}**: Sends the optional flexible-services-container in Pilot packets.
- **default pilot-packet { attribute flexible-services-container }**: Does not send the optional flexible-services -container in Pilot packets.
- **no pilot-packet { attribute flexible-services-container }**: Disables flexible services container information in Pilot packets.

Verifying the Configuration

Use the following commands to verify the Pilot packets configuration.

- **show configuration**
- **show configuration verbose**

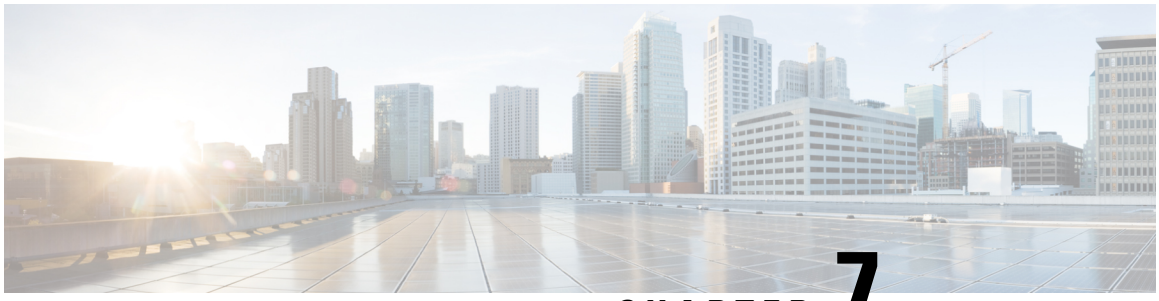
show configuration

The output of this command includes the following field.

Table 8: show config Command Output Description

Field	Description
flexible-services-container	Indicates that an optional TLV Flexible Services Container is sent in Pilot packets.

The **show config verbose** command also includes similar field output.



CHAPTER 7

Cinder Volume Multi-Attach

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• VPC-DI
Feature Default	Enabled - Always-on
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
First introduced.	21.25

Feature Description

In the existing infrastructure, 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 RAID1 is formed, the active CF instance performs disk synchronization over the 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. CF1 (Active) and CF2 (Standby) of QvPC-DI connect 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 is formed using the HD-local disk alone (disk connected to active CF). Therefore, it avoids the HD-RAID mirroring to solve the operational issues.

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.

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 regarding show commands and their outputs for this feature.

show hd raid verbose

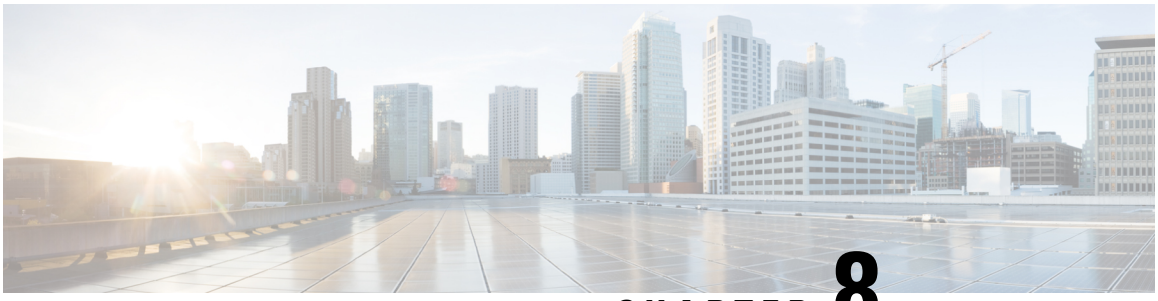
The following new field is added to the output of this command:

- HD Raid
  - Degraded—No (Multiattach)

The following is a sample output:

```
HD RAID:
  State                     : Available (clean)
  Degraded                  : No(Multiattach)
  UUID                      : 3b545d34:e59553c8:a5d0ac8b:78736ca3
  Size                      : 230GB (230000000000 bytes)
  Action                    : Idle
  Disk                      : hd-local1
    State                   : In-sync component
    Created                 : Wed Aug 18 14:44:04 2021
    Updated                 : Thu Aug 19 02:23:36 2021
    Events                  : 32678
    Model                   : QEMU QEMU HARDDISK 2.5+
    Serial Number           : 2b4ea4e4-948e-4641-a342-c82941f9fc98
    Location                : CFC1 A875D844-0E1E-4CA9-A4DB-FB52CB871359
    Size                    : 230.8GB (230854492160 bytes)
  Disk                      : hd-remote1
    State                   : Valid image of 3b545d34:e59553c8:a5d0ac8b:78736ca3
    Created                 : Wed Aug 18 14:44:04 2021
    Updated                 : Thu Aug 19 02:23:36 2021
    Events                  : 32678
    Model                   : QEMU QEMU HARDDISK 2.5+
    Serial Number           : 2b4ea4e4-948e-4641-a342-c82941f9fc98
```

```
Location                : CFC2 7CEB1976-97FE-4E75-A711-9FDC51EF7617
Size                    : 230.8GB (230854492160 bytes)
```



CHAPTER 8

DNS Client KPI Enhancement

Feature Summary and Revision History

Feature Summary

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

Revision History

Revision Details	Release
P-GW supports P-CSCF FQDN received over S6B interface.	21.25.4
First introduced.	21.25

Feature Description

The DNS client supports KPIs for PDN connections. The KPI tracks the number of attempts and failures for DNS queries. This enhancement considers P-CSCF as the network function. P-CSCF maintains the counters and statistics for all successful and failed DNS queries that occur during FQDN resolution. The supported show commands are used to check the details of the DNS KPIs and statistics of the P-CSCF network function. As part of this StarOS 21.25.4 release, support for P-CSCF FQDN received over S6b interface is added.

The rate limit is related to the Time to Live (TTL) value from the DNS server. All responses from the DNS server contain the server TTL value. If the server TTL value is 60 seconds lesser than the honor-low-ttl value configuration, the server TTL value is set to the configured honor-low-ttl value. However, if the server TTL value is less than the configured honor-low-ttl value, there is no change in the configured honor-low-ttl.

When the DNS server reaches the rate limit, all pending FQDN responses contain the default TTL value (60 seconds) as defined in the boxer configuration.

Monitoring and Troubleshooting

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

Show Commands and Outputs

This section provides information about the show commands and outputs for the various DNS statistics for the P-CSCF network function configured under emergency APN.

show dns-client statistics dns-query NF P-CSCF apn name *apn-name*

Table 9: show dns-client statistics dns-query NF P-CSCF apn name <apn-name> Command Output Descriptions

Field	Description
Total Queries Sent	The total number of queries.
Success Queries	The total number of attempted and successful DNS queries of a specific type.
Success Positive Cache Queries	The total number of successful queries from the DNS cache.
Domain Not Found	The total number of queries where the domain name is not found.
Query Timeouts	The total number of queries that timed out.
Socket Related Error	The total number of queries when the DNS Client encounters a socket.
Unable to Connect	The total number of unsuccessful queries when unable to connect to the DNS server.
Cache Corrupted	The total number of unsuccessful queries due to cache corruption.

Field	Description
Other Failures	The total number of queries failed due to other failure reasons.

Use the following command to clear the DNS statistics for P-CSCF network function, which is configured under emergency APN:

clear dns-query NF P-CSCF apn name *apn-name*

show dns-client statistics dns-query NF P-CSCF apn all

Table 10: show dns-client statistics dns-query NF P-CSCF apn all Command Output Descriptions

Field	Description
Total Queries Sent	The total number of queries.
Success Queries	The total number of attempted and successful DNS queries of a specific type.
Success Positive Cache Queries	The total number of successful queries from the DNS cache.
Domain Not Found	The total number of queries where the domain name is not found.
Query Timeouts	The total number of queries that timed out.
Socket Related Error	The total number of queries when the DNS Client encounters a socket.
Unable to Connect	The total number of unsuccessful queries when unable to connect to the DNS server.
Cache Corrupted	The total number of unsuccessful queries due to cache corruption.
Other Failures	The total number of queries failed due to other failure reasons..

Use the following command to clear the DNS statistics for P-CSCF network function, which is configured under emergency APN:

clear dns-query NF P-CSCF apn all

show dns-client log fqdn-limit-logs client *client-name*

The rate limit is related to the number of FQDNs configured through the following CLI:

cache honor-low-ttl *value* **fqdns-per-sec** *value*

Use the following command to check the details of the DNS client rate limit logging. This command shows the timestamp when the FQDN limit is reached.

show dns-client log fqdn-limit-logs client *client-name*

The following is a sample output of the command:

```
[ISP1]laas-setup# show dns-client logs fqdn-limit-logs client PGW_DNS
TimeStamp                  FQDN Limit Details

Wed 2021-09-08 01:57:01 FQDN limit reached for DNS Server low ttl value
Wed 2021-09-08 02:01:17 FQDN limit cleared for DNS Server low ttl value
Wed 2021-09-08 02:01:17 FQDN limit reached for DNS Server low ttl value
Wed 2021-09-08 02:04:12 FQDN limit cleared for DNS Server low ttl value
Wed 2021-09-08 02:04:12 FQDN limit reached for DNS Server low ttl value
Wed 2021-09-08 02:06:44 FQDN limit cleared for DNS Server low ttl value
Wed 2021-09-08 02:14:15 FQDN limit reached for DNS Server low ttl value
[ISP1]laas-setup#
```

Use the following command to clear the details of the DNS client rate limit logging:

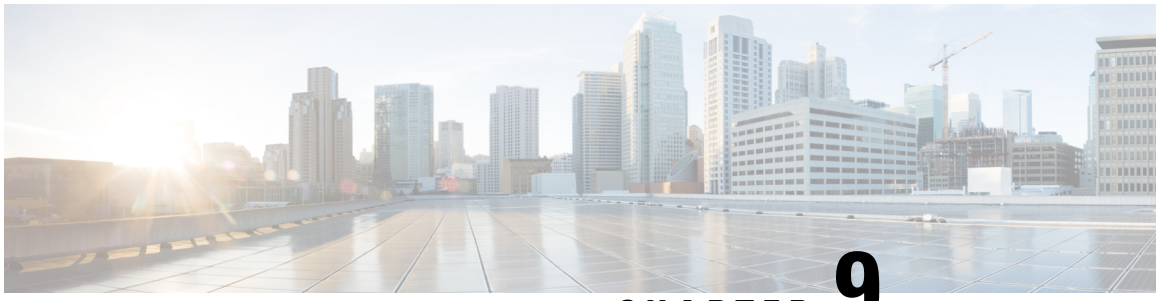
clear dns-client *client_name* log fqdn-limit logs

Bulk Statistics

The APN schema supports the following bulk statistics.

Table 11: Bulk Statistics Variables in the APN Schema

Bulk Statistics	Description
dns-nf-pcscf-total-queries-sent	The total number of queries sent.
dns-nf-pcscf-success-queries	The total number of successful queries from the DNS server.
dns-nf-pcscf-success-positive-cache-queries	The total number of queries from the DNS cache.
dns-nf-pcscf-domain-not-found	The total number of P-CSCF domain not found in the DNS server.
dns-nf-pcscf-query-timeouts	The total number of queries when the DNS server is not reachable.
dns-nf-pcscf-socket-errors	The total number of queries when the DNS server encounters socket error.
dns-nf-pcscf-unable-to-connect	The total number unsuccessful queries when unable to connect to the DNS server.
dns-nf-pcscf-cache-corrupted	The total number of unsuccessful queries on the DNS server due to cache corruption.
dns-nf-pcscf-other_failures	The total number of queries on the DNS server due to other failures.



CHAPTER 9

EPS to 5GS Mobility Enhancement

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The **release-s1-s11-on-timer-expiry-upon-clr** CLI configuration allows MME to wait for the resource release timeout to expire.	21.25.12

Feature Changes

Previous Behavior: During Evolved Packet System (EPS) to 5GS Mobility registration (TAU), when the MME receives the Cancel Location Request (CLR), S1 and S11 resources are released instantly.

New Behavior: During EPS to 5GS Mobility registration (TAU), when you configure the **release-s1-s11-on-timer-expiry-upon-clr** CLI, and when MME receives CLR with MME UPDATE

PROCEDURE, then MME waits for the **ho-resource-release-timeout** to expire and releases S1 and S11 resources. If it is not configured, and when MME receives CLR with MME UPDATE PROCEDURE, then MME instantly releases S1 and S11 resources.

Note The changes are applicable only to N26 and have no impact on S10.

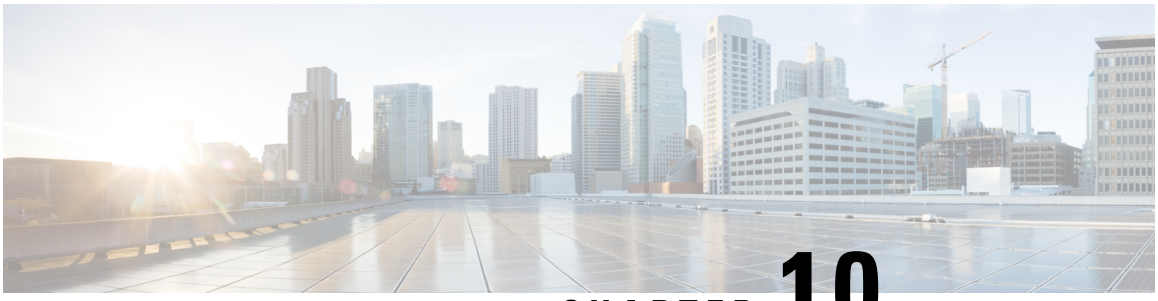
Command Changes

Use the following configuration to allow MME resource timeout to expire.

```
configure
  context context_name
    mme-service service_name
       [ no ] release-s1-s11-on-timer-expiry-upon-clr
  end
```

NOTES:

- **release-s1-s11-on-timer-expiry-upon-clr**: MME to wait for timer expiry after receiving a Cancel Location Request (CLR) from the HSS for EPS to 5GS Mobility registration procedure before releasing S1 and S11.
- **no**: MME releases resources instantly when CLR is received.



CHAPTER 10

Handling Uneven Resource Distribution Notifications on Session Managers

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The SNMP traps and alarms support uneven distribution of resources on session managers across the system. The active session manager task calculates the threshold of resource usage. The supported SNMP trap and alarm configures the monitoring threshold difference between the number of calls among the session managers.

This feature supports the following functions:

1. Raise alarms and traps

   The alarm will be raised when the load difference between the most loaded and least loaded session manager is greater than the configured threshold. The session manger load is calculated by the number of sessions.

2. Clear alarms and traps

   The alarm will be cleared when the load difference between the most loaded and least loaded session manager is lesser than the configured threshold. The session manger load is calculated by the number of sessions.

Note The threshold calculations does not consider the standby session manager instances.

Configuring Threshold Levels and SNMP Traps

Configuring Threshold Levels

Use the following configuration to configure threshold levels for session manager:

```
configure
   [ no ] threshold sess-uneven-dist threshold_percentage [ clear
clear_threshold_percentage [ sess-min-sessmgr-cnt number_of_sessmgr_with_least_calls
 [ sess-active number_of_min_active_session_system_wide ]]]
   [ no ] threshold monitoring sess-uneven-dist
   threshold poll sess-uneven-dist interval interval_range
   default threshold sess-uneven-dist
   end
```

NOTES:

- **threshold**: Configures a specific threshold-based alarm.
- **sess-uneven-dist** *threshold_percentage*: The number of threshold indicates the percentage difference of established session between the most loaded session manager and the least loaded session manager. The default value for threshold is 50%.
- **clear** *clear_threshold_percentage*: Clears the configured alarm threshold. The default value for threshold is 50%.

- **sess-min-sessmgr-cnt** *number_of_sessmgr_with_least_calls*: Configures the number of count of session managers with minimum number of calls to be monitored for calculating uneven session distribution.
- **sess-active** *number_of_min_active_session_system_wide*: Configures the active sessions after which uneven call distribution threshold will be monitored. The default value is 10000.
- **monitoring sess-uneven-dist**: Enables or disables thresholds alerting for a group of thresholds. The number of threshold indicates the percentage difference of established session between the most loaded session manager and the least loaded session manager.
- **poll sess-uneven-dist interval** *interval range*: Configures the threshold polling interval. The value is rounded up to the closest multiple of 30 seconds. The default value is 900.
- **default**: Sets or restores the default value assigned for the specified parameter.

Configuring SNMP Traps

Use the following configuration to configure SNMP traps for session managers and uneven resource distribution:

```
configure
   snmp trap [ enable | suppress ] { sessionUnevenDistribution |
sessionUnevenDistributionclear }
   end
```

NOTES:

- **sessionUnevenDistribution**: Configures the threshold for detection of uneven call distribution on session manager.
- **sessionUnevenDistributionclear**: Clears the threshold detection of uneven call distribution on session manager.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show threshold

The output of this command displays the following fields:

```
show threshold

Threshold operation model: ALARM

Configured thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
```

```
        Clear Threshold:  10%


Active thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%
        Poll Interval:    120Seconds
        Next Poll Time:   2021-Aug-10+17:32:00


Enabled threshold groups: (name, scope)
        sess-uneven-dist              SYSTEM

Non-default poll intervals:
        place-holder                             0Sec
        sess-uneven-dist                       120Sec

No outstanding alarm
```

show threshold all

The output of this command displays the following fields:

```
show threshold all

Threshold operation model: ALARM

Configured thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%


Active thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%
        Poll Interval:    120Seconds
        Next Poll Time:   2021-Aug-10+17:34:00


Enabled threshold groups: (name, scope)
        sess-uneven-dist              SYSTEM

Non-default poll intervals:
        place-holder                             0Sec
        sess-uneven-dist                       120Sec

No outstanding alarm
```

show threshold default

The output of this command displays the following fields:

```
show threshold default
Default Thresholds:
```

```
sess-uneven-dist                      15Min     Notify Above     50%
```

show snmp trap statistics

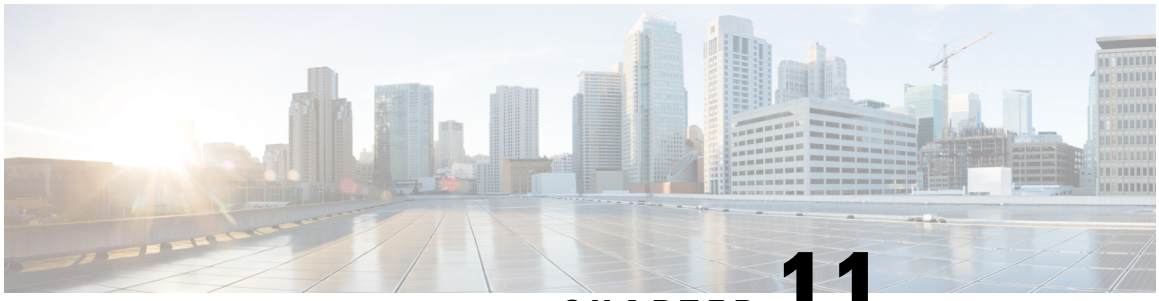
The output of this command displays the following fields:

```
show snmp trap statistics
SNMP Notification Statistics:
  Total number of notifications   : 118
  Last notification sent          : Tuesday August 10 17:31:56 IST 2021
  Notification sending is         : enabled
  Notifications have never been disabled
  Notifications have never been cleared
  Notifications in current period : 2
  Notifications in previous period: 0
  Notification monitor period     : 300 seconds

Trap Name                          #Gen #Disc  Disable Last Generated
---------------------------------- ----- -----  ------- --------------------

SessionUnevenDistribution             1     0       0  2021:08:10:13:36:00
SessionUnevenDistributionClear        1     0       0  2021:08:10:15:12:00

Total number of notifications Disabled  : 92
```



CHAPTER 11

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

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Changes

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

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

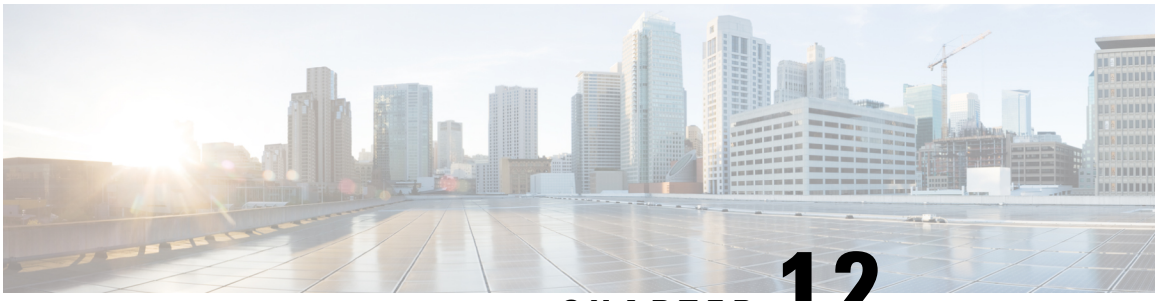
Command Changes

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

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

NOTES:

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



CHAPTER 12

LTE To Wi-Fi Success Rate

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	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference - Bulkstatistic Descriptions*

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The ePDG supports disconnect reasons collectively for call types such as fresh attach, handoff (HO), and LTE to Wi-Fi HO calls.

The disconnect reasons for LTE to Wi-Fi HO help operators to categorize failures during LTE to Wi-Fi HO scenarios. The disconnect reason statistics and bulk statistics are configurable through the CLI.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show epdg-service statistics

The following commands display disconnect reasons for LTE to Wi-Fi HO:

show epdg-service statistics-All ePDG services

- show epdg-service statistics handoff-disc-reasons - Displays the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for all services.
- clear epdg-service statistics handoff-disc-reasons - Removes the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for all services.

show epdg-service statistics-for Specific ePDG Services

- show epdg-service statistics name <epdg1> handoff-disc-reasons - Displays the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for specific services.
- clear epdg-service statistics name <epdg1> handoff-disc-reasons - Removes the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for specific services.
- show bulkstats variables epdg-handoff-disc - Displays the bulk statistics corresponding to LTE to Wi-Fi HO disconnect reasons.

Bulk Statistics

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

Configuring Bulkstats Schema

Use the following sample configuration to configure bulkstats schema for LTE to Wi-Fi HO disconnect reasons statistics.

```
configure
  bulkstats mode
    epdg-handoff-disc schema SchemaHODisc_name format format_string active-only

    epdg-handoff-disc schema SchemaHODisc_name active-only format format_string

     end
```

NOTES:

- **epdg-handoff-disc schema**: Configures bulkstats schema for transferring LTE to Wi-Fi HO disconnect reason statistics.
- **active-only**: Configures statistics on the active chasis only.
- **format** *format_string*: Assigns the naming convention format. *format_string*must be a string of 1 through 3599 characters, including spaces within double quotation marks (" ").

The following is an example of the format string:

```
"vpnid:%vpnid%,servid:%servid%,RemDisc:%ho-disc-remote%,
AdminDisc:%ho-disc-admin%,IdleTimeout:%ho-disc-idle-timeout%,
AbsTimeout:%ho-disc-abs-timeout%,LongDurTimeout:%ho-disc-longdur-timeout%,
SessSetuptimeout:%ho-disc-sesssetup-timeout%,NoRes:%ho-disc-noresource%,"
```

Clearing Bulkstats Schema

Use the following sample configuration to clear the bulkstats for LTE to Wi-Fi Ho disconnect reasons statistics.

```
configure
  bulkstats mode
     no epdg-handoff-disc schema SchemaHODisc_name
     end
```

NOTES:

- **no epdg-handoff-disc-schema**: Removes bulkstats schema.

ePDG Schema

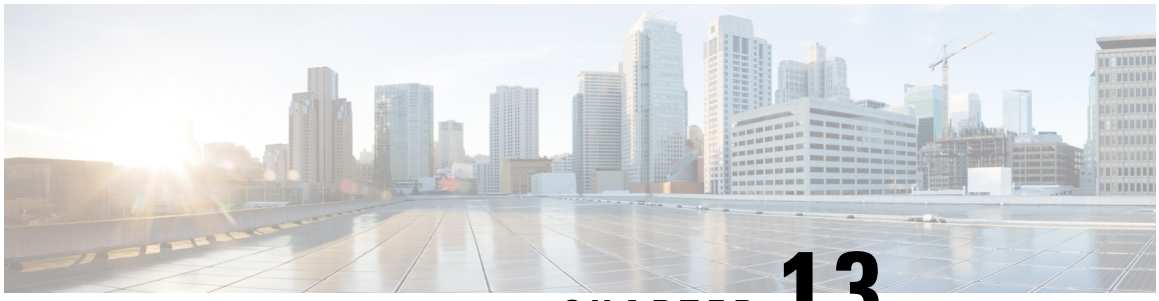
Table 12: Bulk Statistics Variables in the ePDG Schema

Variables	Description
vpnname	The name of the VPN associated with the interface.
vpnid	The identification number of the context configured on the system is facilitating the ePDG service. VPN ID is an internal reference number.
servname	The name of the ePDG service for which these statistics are being displayed.
servid	The identification number of the ePDG service for which these statistics are displayed. Service ID is an internal reference number.

Variables	Description
ho-disc-remote	The total number of disconnected sessions remotely before connect during LTE to Wi-Fi handoff.
ho-disc-admin	The total number of sessions disconnected by Administrator during LTE to Wi-Fi handoff.
ho-disc-idle-timeout	The total number of sessions disconnected due to idle timeout during LTE to Wi-Fi handoff.
ho-disc-abs-timeout	The total number of sessions disconnected due to absolute timeout during LTE to Wi-Fi handoff.
ho-disc-longdur-timeout	The total number of sessions disconnected due to long duration timeout during LTE to Wi-Fi handoff.
ho-disc-sesssetup-timeout	The total number of sessions disconnected due to session setup timeout during LTE to Wi-Fi handoff.
ho-disc-noresource	The total number of sessions disconnected due to non availability of resources during LTE to Wi-Fi handoff
ho-disc-authfail	The total number of sessions disconnected due to authorization failure during LTE to Wi-Fi handoff.
ho-disc-flowadd-failure	The total number of sessions disconnected due to flow add failure during LTE to Wi-Fi handoff.
ho-disc-invalid-dest	The total number of sessions disconnected due to invalid destination during LTE to Wi-Fi handoff.
ho-disc-srcaddr-violation	The total number of sessions disconnected due to source address violation during LTE to Wi-Fi handoff.
ho-disc-dupreq	The total number of sessions disconnected due to duplicate request during LTE to Wi-Fi handoff.
ho-disc-addrassign-failure	The total number of sessions disconnected due to address assignment failure during LTE to Wi-Fi handoff.
ho-disc-misc	The total number of sessions disconnected due to miscellaneous reasons during LTE to Wi-Fi handoff.
ho-disc-mip-reg-timeout	The total MIP registration timeout during LTE to Wi-Fi handoff.
ho-disc-invalid-apn	The number of sessions disconnected because an ePDG rejected the incoming new call due to an APN syntax error (invalid length).
ho-disc-icsr-delete	The number of times that a session got deleted on the standby ICSR chassis when a call clear trigger is received from the active chassis or the call is removed for re-establishment when a full checkpoint was received.
ho-disc-invalid-qci	The total number of sessions disconnected due to invalid QCI received from the AAA server during LTE to Wi-Fi handoff.
ho-disc-ue-redirected	The total number of sessions disconnected due to UE redirection during LTE to Wi-Fi handoff.

Variables	Description
ho-disc-roaming-mandatory	The total number of sessions disconnected due to DNS failure when roaming is mandatory during LTE to Wi-Fi handoff.
ho-disc-ho-disc-invalid-imei	The total number of sessions disconnected due to invalid IMEI received from UE during LTE to Wi-Fi handoff.
ho-disc-gtpc-abort-sess-cmd	The total number of disconnected sessions due to GTP control plane path failure during LTE to Wi-Fi handoff.
ho-disc-gtpu-abort-sess-cmd	The total number of disconnected sessions due to GTP user plane path failure during LTE to Wi-Fi handoff.
ho-disc-gtpu-error-indication	The total number of disconnected sessions due to error indication message on GTP user plane during LTE to Wi-Fi handoff.
ho-disc-pgw-not-reachable	The total number of disconnected sessions due to P-GW during LTE to Wi-Fi handoff.
ho-disc-reject-from-pgw	The total number of disconnected sessions due to P-GW rejecting the Create Session Request during LTE to Wi-Fi handoff.
ho-disc-s2b-access-denied	The total number of sessions disconnected due to S2B cause codes mapped to private IKEv2 notify payload type access denied during LTE to Wi-Fi handoff.
ho-disc-s2b-network-failure	The total the number of sessions disconnected due to S2B cause codes mapped to private IKEv2 notify payload type network failure during LTE to Wi-Fi handoff.
ho-disc-s2b-msg-failure	The total number of sessions disconnected due to S2B cause codes mapped to private IKEv2 notify payload type message failure during LTE to Wi-Fi handoff.
ho-disc-s2b-rat-disallowed	The total number of sessions disconnected due to S2B cause code rat disallowed during LTE to Wi-Fi handoff.
ho-disc-s2b-context-not-found	The total number of sessions disconnected due GTPv2 cause code "Context Not Found" during LTE to Wi-Fi handoff.
ho-disc-epdg-pcscf-restoration	The total number of sessions disconnected due to P-GW triggered reactivation request for P-CSCF restoration during LTE to Wi-Fi handoff.
ho-disc-dns-server-not-reachable	The total number of disconnected sessions due to DNS server not reachable during LTE to Wi-Fi handoff.
ho-disc-dns-no-resource-records	The total number of disconnected sessions when no valid record is fetched from the DNS server during LTE to Wi-Fi handoff.
ho-disc-dns-no-matching-server	The total number of disconnected sessions when the fetched service parameters from DNS record doesn't match the configured protocol (GTP or PMIPv6) during LTE to Wi-Fi handoff.
ho-disc-aaa-server-not-reachable	The total number of disconnected sessions due to the AAA server being unreachable from ePDG during LTE to Wi-Fi handoff.

Variables	Description
ho-disc-aaa-invalid-aaa-attribute	The total number of disconnected sessions due to authentication failure at AAA server and invalid attributes received in Diameter messages from the AAA server during LTE to Wi-Fi handoff.
ho-disc-aaa-apn-validation-failed	The total number of disconnected sessions due to APN mismatch at SWu and SWm interfaces during LTE to Wi-Fi handoff.
ho-disc-aaa-admin	Indicates the AAA Admin disconnect during LTE to Wi-Fi handoff.
ho-disc-aaa-invalid-pdn-type	The total number of disconnected sessions due to mismatch over PDN type between UE and AAA server during LTE to Wi-Fi handoff.
ho-disc-aaa-non-uicc-auth-failed	The total number of non-UICC disconnected sessions due to AAA server during LTE to Wi-Fi handoff.
ho-disc-aaa-network-too-busy	The total number of sessions disconnected due to network busy during LTE to Wi-Fi handoff.
ho-disc-aaa-network-failure	The total number of sessions disconnected due to network failure during LTE to Wi-Fi handoff .
ho-disc-aaa-roaming-not-allowed	The total number of sessions disconnected due to roaming not allowed during LTE to Wi-Fi handoff.
ho-disc-aaa-rat-disallowed	The total number of sessions disconnected due to result code or experimental result code returned by Diameter during LTE to Wi-Fi handoff.
ho-disc-aaa-no-subscription	The total number of sessions disconnected due to non subscription of AAA during LTE to Wi-Fi handoff.
ho-disc-aaa-operator-policy	The total number of disconnected sessions due to lack of suitable operator policy configuration during LTE to Wi-Fi handoff.
ho-disc-aaa-no-non-3gpp-subscript	The total number of sessions disconnected due to AAA cause codes mapped to 3GPP IKEv2 private notify payload error type "#9000 No Non 3gpp Subscription" during LTE to Wi-Fi handoff.
ho-disc-aaa-user-unknown	The total number of sessions disconnected due to AAA cause codes mapped to 3GPP IKEv2 private notify payload error type "#9001 User Unknown" during LTE to Wi-Fi handoff.
ho-disc-aaa-illegal-equipment	The total number of sessions disconnected due to AAA cause codes mapped to 3GPP IKEv2 private notify error payload type "#9006 Illegal ME" during LTE to Wi-Fi handoff.
ho-disc-pgwselectfail-handoff	The total number of disconnected sessions due to P-GW selection failure during LTE to Wi-Fi handoff.



CHAPTER 13

Password Expiration Notification

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
This feature is enhanced with a new option to the **save config** command. The enhancement supports downgrade and ensures that the user profiles do not get lost after downgrade.	• 21.25.3
In this release, P-GW supports password expiration notification to Context, AAA, and RADIUS users.	21.23

Feature Description

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

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

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

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

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

For example:

```
login: xxx
password: xxx

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

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

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

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

Upgrade and Downgrade Process for Password Expiration Notification

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

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

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

Upgrading and Downgrading Procedures Using Save Configuration Command

Use the following upgrade process:

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

Use the following downgrade process:

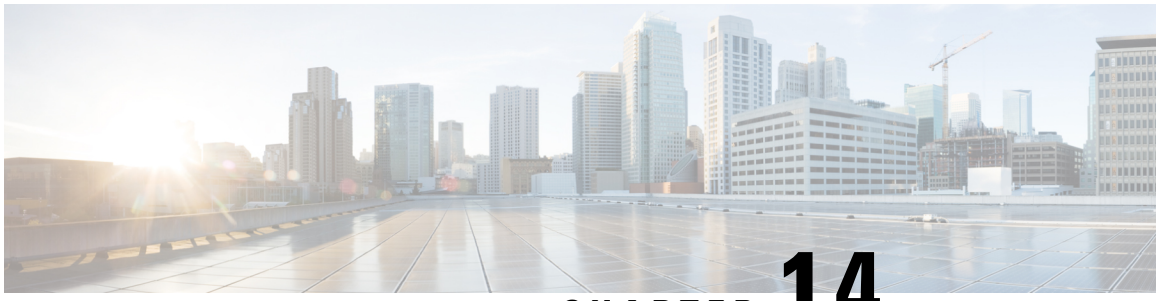
Use the **legacy-password-expiry** CLI command in the **save config** command, based on which new keywords are not saved. Configuration is stored in a format which previous release recognizes.

Use the following configuration under context configuration:

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

NOTES:

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



CHAPTER 14

Reject Paging Request for Active Emergency VoLTE Call

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* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Support is added to reject Paging Requests for active emergency VoLTE calls.	21.25

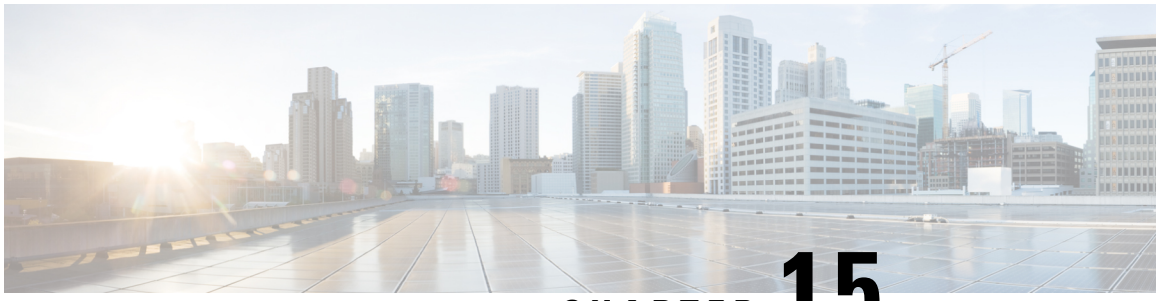
Reject Paging Request for Active Emergency VoLTE Call

Reject Paging Request for Active Emergency VoLTE Call

When a UE does not respond to the SIP INVITE message sent from the IMS PDN, the call is redirected to MSS or CS. The MSS sends a Paging Request message to MME with the CS call type.

When a VoLTE emergency call is active, MME considers the ARP priority (1 to 8) for emergency call and rejects the Paging Request from MSS triggered by an incoming MT CSFB call. MME does not initiate any activity towards the UE. When MME finds the "CS call" in Paging Request and "emergency PDN" in the UE context, it sends a Paging Reject back to the MSC to stop the CS paging procedure.

For more information, refer to the *SMS over SGs Interface* chapter in the *MME Administration Guide*.



CHAPTER 15

Sending EMM Information during Periodic TAU

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The MME sends EMM information to the UE during normal and handover TAU procedures. The MME can be configured to send EMM information in periodic TAU even in scenarios when the active flag is not set.

In releases prior to 21.25, MME sent the EMM information to UE during periodic TAU when an active flag was set. When the active flag was not set during periodic TAU, the NBIoT UE did not receive the EMM information from MME.

Configuring EMM Information

This section describes the configuration to enable or disable EMM information for periodic TAU in the Call Control Profile Configuration and MME Service Configuration modes.

Configuring EMM Information in Call Control Profile

Use the following sample configuration to enable or disable EMM information in the Call Control profile for periodic TAU when active flag is not set:

```
configure
   call-control-profile profile_name
      [ remove ] tau { send-emm-info } [ access-type { all | nb-iot |
wb-eutran } ]
     end
```

Configuring EMM Information in MME Service

Use the following sample configuration to enable or disable EMM information in the MME service for periodic TAU when active flag is not set:

```
configure
   context context_name
     mme-service service_name
        [ default ] { policy } tau { send-emm-info } [ access-type { all
| nb-iot | wb-eutran } ]
       end
```

Note The **set-ue-time** option under **tau** in the mme-service configuration must be enabled for this feature.

NOTES:

- **tau**: Enables the tracking area update procedure.
- **send-emm-info**: Sends EMM information to UE in case of Periodic TAU with Active Flag not set.
- **access-type { all | nb-iot | wb-eutran }**: Enables access type extension.
  - **nb-iot**: Enables the configuration for NB-IoT access type.
  - **wb-eutran**: Enables the configuration for WB-EUTRAN access type.

- **all**: Enables the configuration for NB-IoT and WB-EUTRAN access types.
- **remove**: Removes the configured values.
- **default**: Restores the configuration to default (disabled) state.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show mme-service statistics

The output of this command displays the following fields:

- Send EMM in Periodic TAU without Bearer Activation:
  - NB-IOT—Displays the count for NB-IoT access type.
  - WB-EUTRAN—Displays the count for WB-EUTRAN access type.

show mme-service all

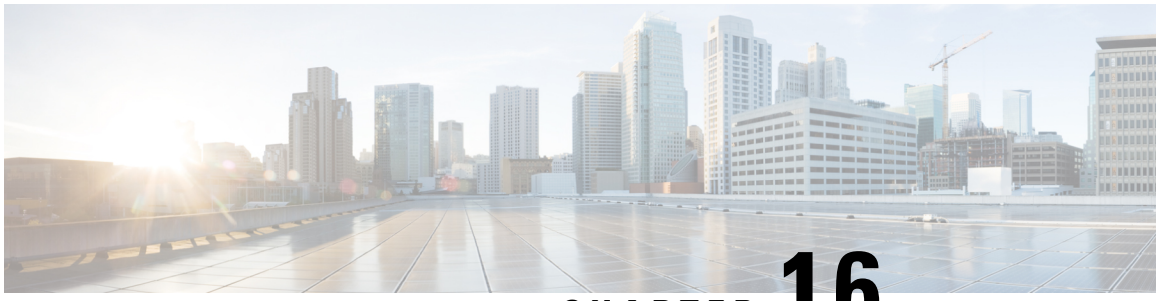
The output of this command displays the following fields:

- Send EMM Info for Periodic TAU—Indicates whether the EMM information for periodic TAU is enabled or disabled.
  - Access Type—Indicates the access type—WB-EUTRAN, NB-IOT, or WB-EUTRAN and NB-IOT.

show call-control profile full all

The output of this command displays the following fields:

- Send EMM Info for Periodic TAU—Indicates whether the EMM information for periodic TAU is enabled or disabled.
  - Access Type—Indicates the access type—WB-EUTRAN, NB-IOT, or WB-EUTRAN and NB-IOT.



CHAPTER 16

Suppressing Handover Request for VoWiFi IR Subscribers

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The ePDG supports VoWiFi fresh attach request for IR subscribers. This enhancement also includes a related counter and bulk statistic.	21.25

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

Feature Description

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

If the IR fresh attach request is on dedicated ePDG, there is no change in functionality and it is processed as in normal attach case.

How it Works

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

handover international-roamer suppress

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

no handover international-roamer suppress

Note This CLI is disabled by default.

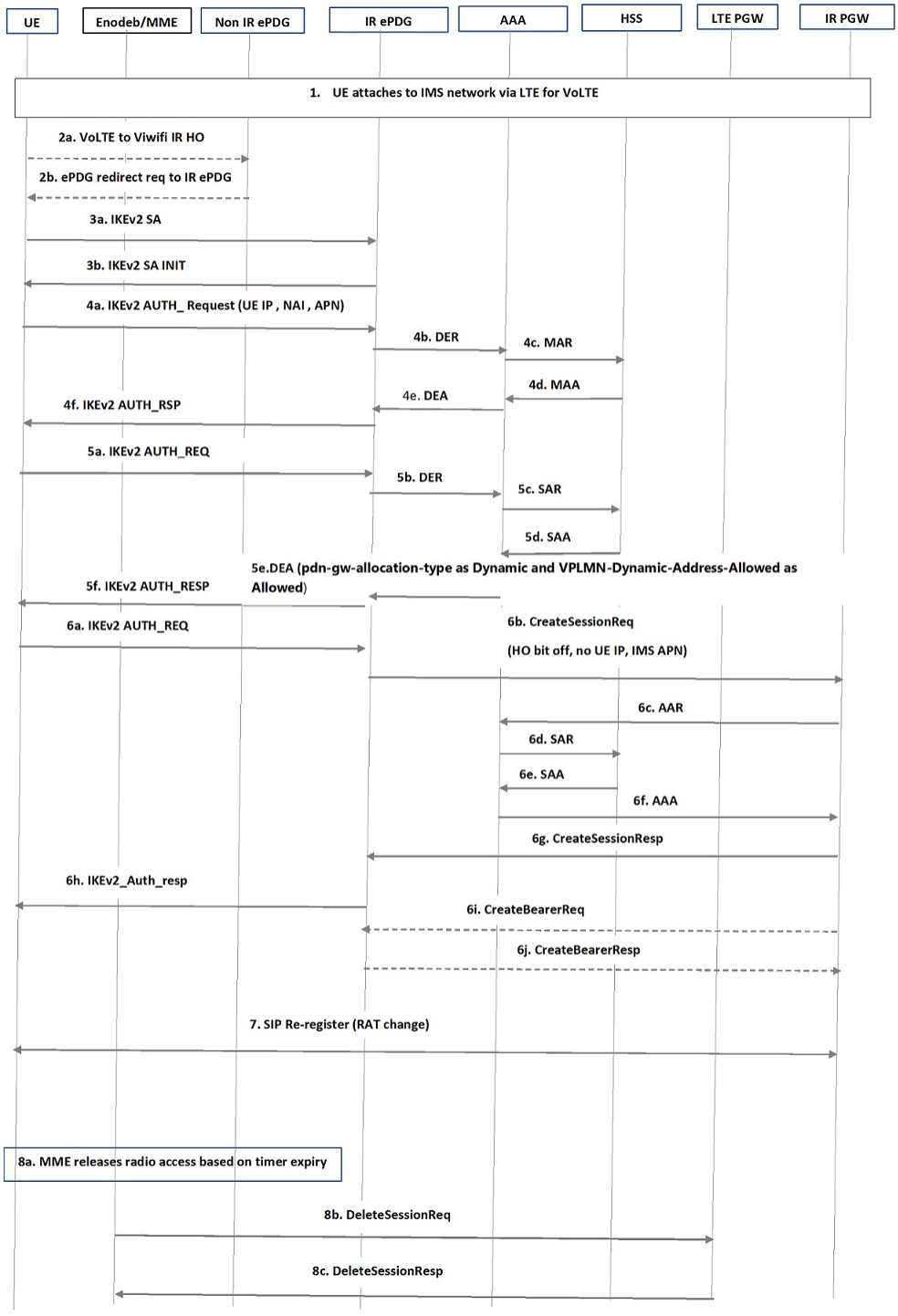
Enabling the CLI in normal ePDG impacts the normal ePDG HO call flows. The following warning message is displayed on enabling the feature:

Warning This feature is customer-specific. Enabling this feature might impact the calls.

VoLTE to VoWi-Fi IR HO Call Flows

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

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



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

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show epdg-service statistics suppress-ir-handover

The output of this command includes the following fields:

Fields/Counters	Description
Attempts: 1	Total number of ePDG sessions for which international roaming handoff attempted on international roaming HO suppression supported ePDG.
Success: 1	Total number of ePDG sessions for which international roaming handoff attempts succeeded on international roaming HO suppression supported ePDG.
Failures: 0	Total number of ePDG sessions for which international roaming handoff attempts failed on international roaming HO suppression supported ePDG.
Active: 1	Total number of current active ePDG sessions for which international roaming handoff attempts succeeded on international roaming HO suppression supported ePDG.

show epdg-service name *name*

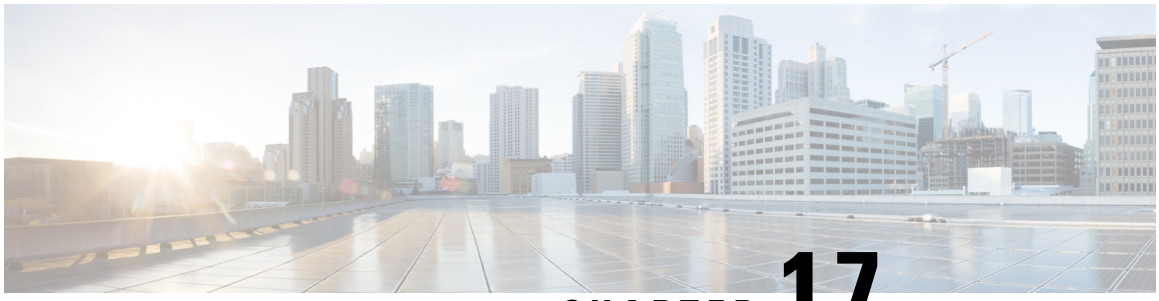
The output of this command includes the following fields to check whether IR suppress handover is enabled or disabled.

Fields/Counters	Description
Suppress International Roamer Handover	Specifies if the suppress international roamer HO is enabled or disabled.

Bulk Statistics

The ePDG schema supports the following bulk statistics for suppressing handover request for VoWiFi IR subscribers:

Bulk Statistics	Description
suppress-intr-roaming-ho-attempts	Indicates the total number of ePDG sessions for which international roaming handoff attempted. This increments when international roaming handoff is attempted on international roaming HO suppression supported ePDG.
suppress-intr-roaming-ho-success	Indicates the total number of ePDG sessions for which international roaming handoff attempts succeeded. This increments when international roaming handoff attempt succeeds on international roaming HO suppression supported ePDG.
suppress-intr-roaming-ho-failures	Indicates the total number of ePDG sessions for which international roaming handoff attempts failed. This increments when international roaming handoff attempt fails on international roaming HO suppression supported ePDG.
suppress-intr-roaming-ho-active	Indicates the current number of active ePDG sessions for which international roaming handoff attempts succeeded.



CHAPTER 17

TCP Reset with Invalid Sequence Number should not Trigger Connection Close

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release, the TCP RST segment will be sequence number validated.	• 21.25 • 21.20.25 • 21.15.60

Feature Changes

Previous Behavior: P-GW always accepted TCP RST Segments as valid and closed the TCP Data Connection Session on receiving a RST Segment.

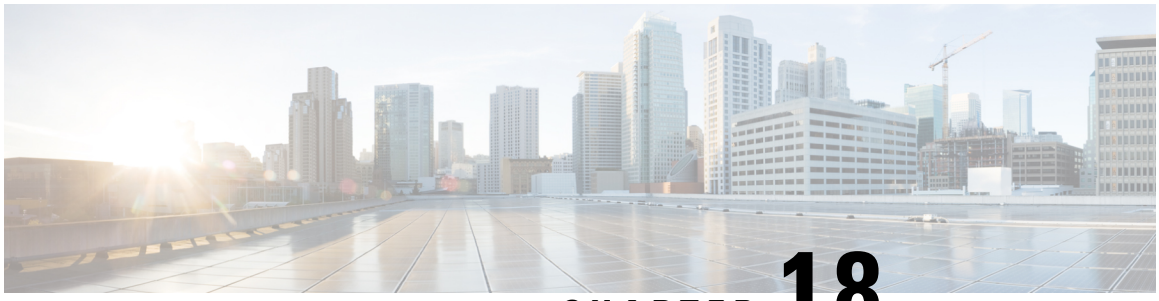
New Behavior: If a TCP RST Segment is received and the TCP FSM is in SYN-RCVD state, the TCP RST Segment is sequence number validated. Refer to RFC793 for more information.

If the validation fails (an invalid TCP RST segment), the TCP RST segment is not processed at P-GW and the TCP Data Connection is not closed. The TCP RST segment is passed on seamlessly to the destination.

If the TCP RST Segment is valid, then the normal TCP Data Connection teardown continues.

The new TCP RST Segment validation is only done in TCP FSM SYN-RCVD state. For other TCP FSM states, the behaviour has not changed.

Impact on Customer: TCP Data connection is not closed for invalid TCP RST Segment in SYN-RCVD state and flow at PDN-GW continues to be active.



CHAPTER 18

Support for Tariff-Time-Change in Fast Path

Feature Summary and Revision History

Summary Data

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

Revision History

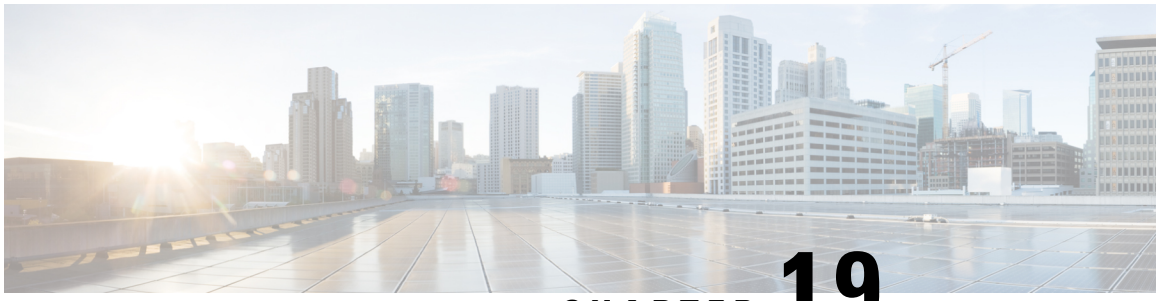
Revision Details	Release
Tariff-Time-Change AVP is supported in fast path.	• 21.25.4 • 21.20.22

Feature Changes

Previous Behavior: When the Tariff-Time-Change AVP was received from Gy for a Rating Group, traffic was switched to the slowpath and thus slowed down user's traffic.

New Behavior: When the Tariff-Time-Change AVP is received from Gy for a Rating Group, traffic continues to flow in the fast path and maintains the user's traffic rate.

Customer Impact: End-user will receive seamless traffic.



CHAPTER 19

Video Shaping Tethered Data

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ECS
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* • *ECS Administration Guide*

Revision History

Revision Details	Release
In this release, if the ruledef matches the video and if the data flow is identified as tethered, then the configured flow limits are applied.	21.25

Feature Description

The video shaping tethered data feature streams video data packets through Wi-Fi tethered data. This feature applies the configured flow limits under the matched video rule, and the configured rating-group and content ID for the tethered charging-action in the following scenarios:

- If the ruledef matches the video
- If the data flow is tethered
- If the tethered limit is lower than the configured limit

Note After configuring the Tethering detection rules, you can configure the video detection rules.

Configuring Video Shaping Tethered Data

Configuring Tethered Flow

Use the following sample configuration to enable tethered flow condition.

```
configure
   active-charging service service_name
      trigger-condition condition_name
         [ no ] tethered-flow
         end
```

NOTES:

- **no**: Disables the tethered traffic flow.
- **tethered-flow**: Identifies the tethered traffic.

Configuring Map Charging

Use the following sample configuration to enable map charging.

```
configure
   active-charging service service_name
      trigger-action action_name
         [ no ] map charging-action charging_action_name attribute charging
         end
```

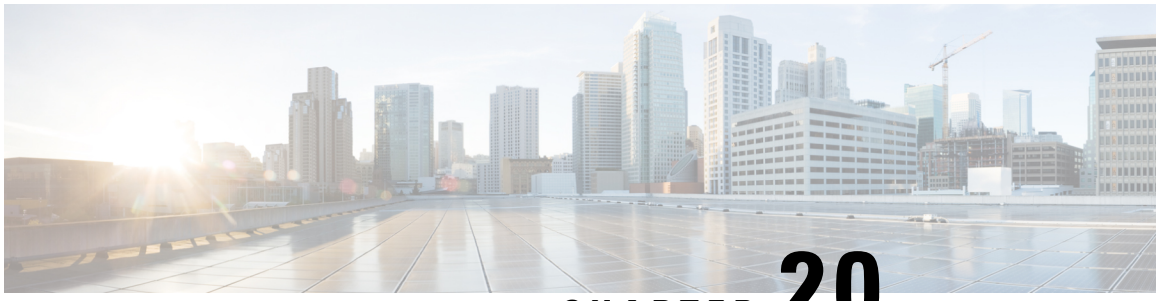
NOTES:

- **no**: Disables the map charging.
- **map charging-action** *charging_action_name* **attribute charging**: Applies the rating group, content ID, online and offline charging based on the rule set for video shaping.

Verifying the Configuration

Use the following command to verify the feature configuration:

show configuration verbose



CHAPTER 20

VPP Metric Enhancement

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The and **show active-charging flows summary**commands are enhanced to get the statistics from VPP.	21.26
The following enhancements were introduced: • Analyzer level statistics (TCP, UDP, P2P, HTTP, HTTPS) • VPP statistics collection using the CLI configuration	21.25
First introduced.	21.24

Feature Description

The Vector Packet Processing (VPP) metrics help to analyze and debug the VPP offloaded traffic. This feature applies only to platforms that support VPP.

Traffic flows are dealt in different ways based on how P-GW recognizes them. For example, some flows are managed with VPP and some are not. To enhance troubleshooting, statistics are added at rulebase, subscriber, and analyzer protocol levels for VPP flows. The supported analyzer protocols include Transmission Control Protocol (TCP), User Datagram Protocol (UDP), peer-to-peer (P2P) analyzer, Hypertext Transfer Protocol (HTTP), and Hypertext Transfer Protocol Secure (HTTPS). System level bulk statistics are supported for troubleshooting.

This feature is partially controlled through the active-charging service configuration. Only the subscriber-specific statistics related to VPP offload are controlled using CLI.

Configuring Metrics Collection

Use the following sample configuration to enable or disable metrics collection from VPP for subscriber and rulebase.

```
configure
  active-charging service service_name
    [ no ] statistics-collection { all | vpp }
    end
```

NOTES:

- **all**: Configures both Ruledef and VPP statistics collection.
- **vpp**: Configures VPP statistics collection.
- **no**: Resets the seed-time value to the default value of 0.
- By default, this CLI is disabled.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show active-charging flows full debug-info all

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

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

show active-charging rulebase statistics name

The output of this command displays the following fields:

Table 14: show active-charging rulebase statistics name Command Output Descriptions

Field	Description
VPP Offload Statistics:	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv4 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv4 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv4 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv4 downlink bytes discarded.

Field	Description
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv6 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv6 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv6 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv6 downlink bytes discarded.

show active-charging subscribers all

The output of this command displays the following fields.

Table 15: show active-charging subscribers all Command Output Descriptions

Field	Description
VPP-PKTS-UP	Total number of packets detected in uplink direction through VPP.
VPP-PKTS-DOWN	Total number of packets detected in downlink direction through VPP.

show-active-charging subscribers full all

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

Table 16: show active-charging subscribers full all Command Output Descriptions

Field	Description
VPP Offload Statistics: Enabled/Disabled	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.

Field	Description
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv4 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv4 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv4 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv4 downlink bytes discarded.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv6 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv6 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv6 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv6 downlink bytes discarded.

show active-charging analyzer statistics name

The output of this command displays the following fields. The fields are common for http, secure-http, p2p, tcp, udp.

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

Field	Description
Total VPP FP Packets	Total number of Fast Path packets through VPP.
VPP Fastpath Statistics:	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.

Field	Description
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.

Bulk Statistics

The ECS schema includes the following bulk statistics.

ECS Schema

Table 18: Bulk Statistics Variables in the ECS Schema

Variables	Description
vpp-tot-flows	Indicates total number of flows through VPP.
vpp-cur-flows	Indicates total number of active current flows through VPP.
IPv4	
vpp-IPv4-uplk-pkts	Indicates total number of IPv4 packets detected in uplink direction through VPP.
vpp-IPv4-dwnlk-pkts	Indicates total number of IPv4 packets detected in downlink direction through VPP.
vpp-IPv4-uplk-bytes	Indicates total number of IPv4 bytes detected in uplink direction through VPP.
vpp-IPv4-dwnlk-bytes	Indicates total number of IPv4 bytes detected in downlink direction through VPP.
vpp-IPv4-uplk-drop-pkts	Indicates the total number of dropped IPv4 packets detected in uplink direction through VPP.
vpp-IPv4-dwnlk-drop-pkts	Indicates the total number of dropped IPv4 packets detected in downlink direction through VPP.
vpp-IPv4-uplk-drop-bytes	Indicates the total number of dropped IPv4 bytes detected in uplink direction through VPP.

Variables	Description
vpp-IPv4-dwnlk-drop-bytes	Indicates the total number of dropped IPv4 bytes detected in downlink direction through VPP.
IPv6	
vpp-IPv6-uplk-pkts	Indicates total number of IPv6 packets detected in uplink direction through VPP.
vpp-IPv6-dwnlk-pkts	Indicates total number of IPv6 packets detected in downlink direction through VPP.
vpp-IPv6-uplk-bytes	Indicates total number of IPv6 bytes detected in uplink direction through VPP.
vpp-IPv6-dwnlk-bytes	Indicates total number of IPv6 bytes detected in downlink direction through VPP.
vpp-IPv6-uplk-drop-pkts	Indicates the total number of dropped IPv6 packets detected in uplink direction through VPP.
vpp-IPv6-dwnlk-drop-pkts	Indicates the total number of dropped IPv6 packets detected in downlink direction through VPP.
vpp-IPv6-uplk-drop-bytes	Indicates the total number of dropped IPv6 bytes detected in uplink direction through VPP.
vpp-IPv6-dwnlk-drop-bytes	Indicates the total number of dropped IPv6 bytes detected in downlink direction through VPP.
TCP	
tcp-vpp-flows-cur	Indicates the current number of flows through VPP for TCP analyzer.
tcp-vpp-flows	Indicates the total number of flows through VPP for TCP analyzer.
tcp-vpp-pkts	The total number of IP packets through VPP for TCP analyzer.
tcp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.

Variables	Description
tcp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.
UDP	
udp-vpp-flows-cur	Indicates the current number of flows through VPP for UDP analyzer.
udp-vpp-flows	Indicates the total number of flows through VPP for UDP analyzer.
udp-vpp-pkts	Indicates the total number of IP packets through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for UDP analyzer.
HTTP	
http-vpp-flows-cur	Indicates the current number of flows through VPP for HTTP analyzer.
http-vpp-flows	Indicates the total number of flows through VPP for HTTP analyzer.
http-vpp-pkts	Indicates the total number of IP packets through VPP for HTTP analyzer.
http-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTP analyzer.

Variables	Description
http-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTP analyzer.
http-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTP analyzer.
http-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTP analyzer.
http-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTP analyzer.
Secure-HTTP	
https-vpp-flows-cur	Indicates the current number of flows through VPP for HTTPS analyzer.
https-vpp-flows	Indicates the total number of flows through VPP for HTTPS analyzer.
https-vpp-pkts	Indicates the total number of IP packets through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTPS analyzer.
P2P	
p2p-vpp-flows-cur	Indicates the current number of flows through VPP for P2P analyzer.

Variables	Description
p2p-vpp-flows	Indicates the total number of flows through VPP for P2P analyzer.
p2p-vpp-pkts	Indicates the total number of IP packets through VPP for P2P analyzer.
p2p-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for P2P analyzer.