ePDG Administration Guide, StarOS Release 21.26

First Published: 2021-12-22

Last Modified: 2023-03-10

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

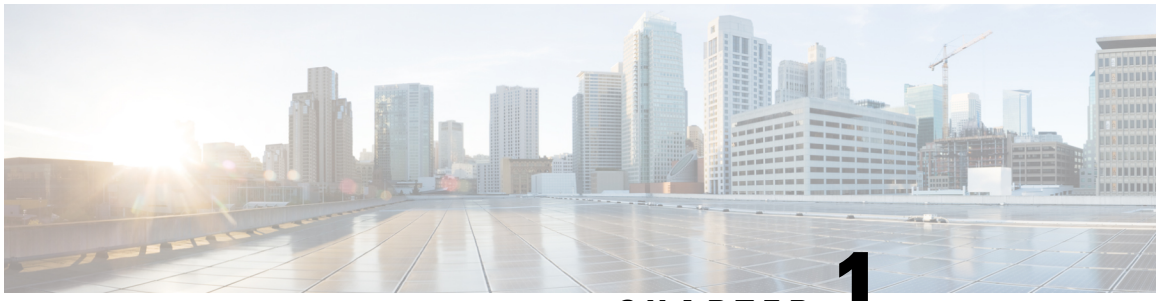
About this Guide

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 preface describes the *ePDG Administration Guide*, how it is organized, and its document conventions.

The guide describes the ePDG (Evolved Packet Data Gateway) and includes network deployments and interfaces, feature descriptions, session flows, configuration instructions, and CLI commands for monitoring and troubleshooting the system. It also contains a sample ePDG configuration file and ePDG engineering rules.

About this Guide



CHAPTER 1

Evolved Packet Data Gateway Overview

This chapter contains an overview of the ePDG (evolved Packet Data Gateway), including:

Product Description

The Cisco® ePDG (evolved Packet Data Gateway) enables mobile operators to provide secure access to the 3GPP E-UTRAN/EPC (Evolved UTRAN/Evolved Packet Core) network from untrusted non-3GPP IP access networks. The ePDG functions as a security gateway to provide network security and internet working control via IPSec tunnel establishment based on information obtained during 3GPP AAA (Authentication, Authorization, and Accounting). The ePDG enables mobile operators to extend wireless service coverage, reduce the load on the macro wireless network, and make use of existing backhaul infrastructure to reduce the cost of carrying wireless calls.

The ePDG has the following key features:

- Support for the IPSec/IKEv2-based SWu interface between the ePDG and the WLAN (Wireless LAN) UEs.
- Routing of packets between the WLAN UEs and the Cisco P-GW (Packet Data Network Gateway) over the S2b interface via GTPv2 or PMIPv6 (Proxy Mobile IP version 6) protocol.
- P-GW selection via DNS client functionality to provide PDN (Packet Data Network) connectivity to the WLAN UEs.
- Support for passing assigned IPv4/IPv6 address configurations from the P-GW to the WLAN UEs.
- Support for the Diameter-based SWm interface between the ePDG and the external 3GPP AAA server.
- Tunnel authentication and authorization for IPSec/PMIPv6/GTPv2 tunnels using the EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) authentication method between the 3GPP AAA server and the WLAN UEs.
- Encapsulation and decapsulation of packets sent over the IPSec/PMIPv6/GTPv2 tunnels.
- Hosts a MAG (Mobile Access Gateway) function, which acts as a proxy mobility agent in the E-UTRAN/EPC network and uses PMIPv6 signaling to provide network-based mobility management on behalf of the WLAN UEs attached to the network.

Platform Requirements

The ePDG service runs on a Cisco ASR 5500 (DPC1/DPC2) chassis running the StarOS operating system , and Virtualized Packet Core (VPC) platforms with optional crypto accelerator card (coleto creek). The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, see the installation guide for the chassis and/or contact your Cisco account representative.

Important The ePDG Hardware Crypto Assist (Coleto Creek) feature on VPC-DI is not fully qualified in this release. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

Important The ePDG Hardware Crypto Assist (Coleto Creek) feature on VPC-DI is fully qualified in release 21.6 and later releases.

MIO Demux Card on ASR 5500

The ePDG service is fully qualified to run on the Management Input/Output (MIO) card for demux functions. ePDG can leverage on the additional card for user plane processing to increase the capacity of the chassis.

Important When IPSec large and demux on MIO are configured together, enable the IPSec large feature (using the **require ipsec-large** command) before enabling the demux on MIO (using the **require demux management-card** command).

For more information on the Demux card, refer the *System Administration Guide*.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the System Administration Guide for your deployment.

Licenses

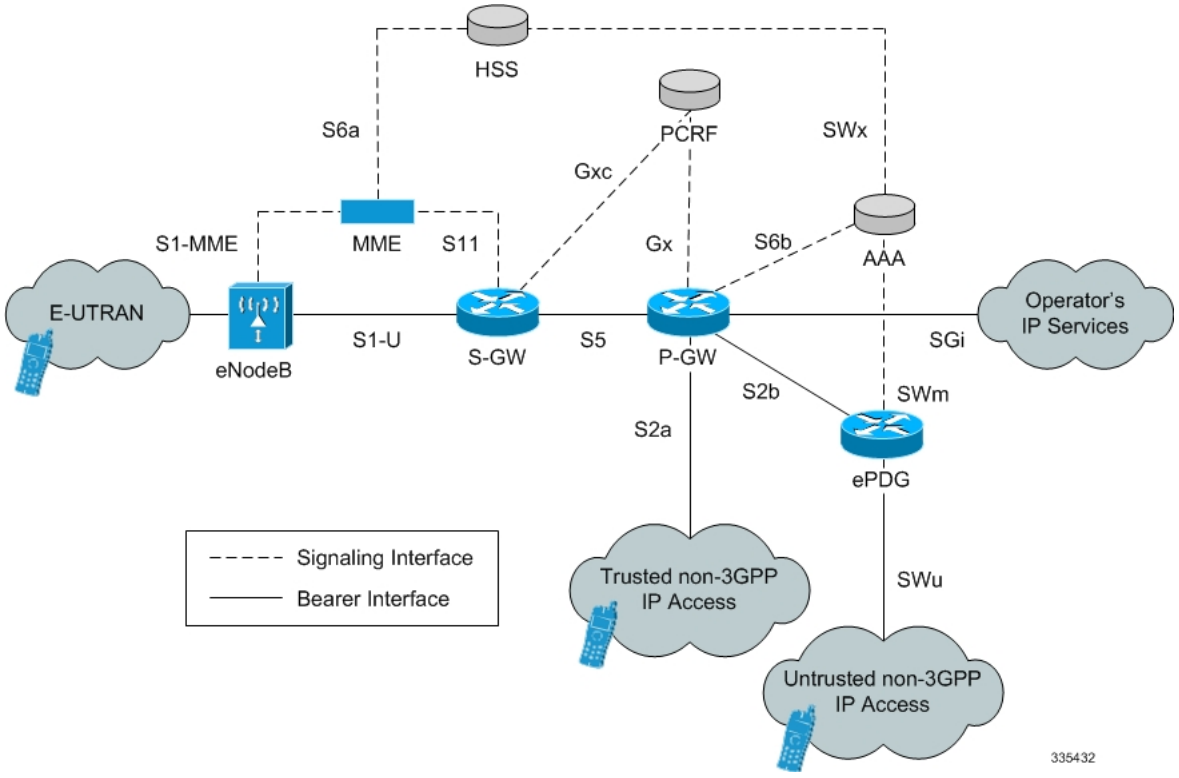
The ePDG is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, see "Managing License Keys" in the *System Administration Guide.*

Network Deployment(s) and Interfaces

This section describes the ePDG as it provides secure access from the WLAN UEs to the Cisco P-GW and a connection to the PDN (Packet Data Network) in the E-UTRAN/EPC (Evolved UTRAN/Evolved Packet Core) network.

The figure below shows the ePDG terminating the SWu interface from the untrusted non-3GPP IP access network and providing secure access to the Cisco P-GW and a connection to the PDN via the PMIPv6/GTPv2 S2b interface. It also shows the network interfaces used by the Cisco MME, S-GW, and P-GW in the E-UTRAN/EPC network.

Figure 1: The ePDG in the E-UTRAN/EPC Network



Network Elements

This section provides a description of the network elements that work with the ePDG in the E-UTRAN/EPC network. For untrusted non-3GPP IP access, note that the network architecture assumes the access network elements do not perform any function other than delivering packets.

ePDG

The ePDG is responsible for interworking between the EPC and untrusted non-3GPP networks that require secure access, such as a WiFi, LTE metro, and femtocell access networks.

eNodeB

The eNodeB (evolved Node B) is the termination point for all radio-related protocols. As a network, E-UTRAN is simply a mesh of eNodeBs connected to neighboring eNodeBs via the X2 interface.

MME

The Cisco MME (Mobility Management Entity) is the key control node for the LTE access network. It works in conjunction with the eNodeB and the Cisco S-GW to control bearer activation and deactivation. The MME

is typically responsible for selecting the Cisco P-GW for the UEs to access the PDN, but for secure access from untrusted non-3GPP IP access networks, the ePDG is responsible for selecting the P-GW.

S-GW

The Cisco S-GW (Serving Gateway) routes and forwards data packets from the 3GPP UEs and acts as the mobility anchor during inter-eNodeB handovers. The S-GW receives signals from the MME that control the data traffic. Every 3GPP UE accessing the EPC is associated with a single S-GW.

P-GW

The Cisco P-GW (Packet Data Network Gateway) is the network node that terminates the SGi interface towards the PDN. The P-GW provides connectivity to external PDNs for the subscriber UEs by being the point of entry and exit for all subscriber UE traffic. A subscriber UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering, charging support, lawful interception, and packet screening. The P-GW is the mobility anchor for both trusted and untrusted non-3GPP IP access networks. For PMIP-based S2a and S2b interfaces, the P-GW hosts the LMA (Local Mobility Anchor) function.

3GPP AAA Server

The 3GPP AAA (Authentication, Authorization, and Accounting) server provides UE authentication via the EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) authentication method.

HSS

The HSS (Home Subscriber Server), is the master user database that supports the IMS (IP Multimedia Subsystem) network entities. It contains subscriber profiles, performs subscriber authentication and authorization, and provides information about the subscriber's location and IP information.

PCRF

The PCRF (Policy and Charging Rules Function) determines policy rules in the IMS network. The PCRF operates in the network core, accesses subscriber databases and charging systems, and makes intelligent policy decisions for subscribers.

Logical Network Interfaces

The following table provides descriptions of the logical network interfaces supported by the ePDG in the E-UTRAN/EPC network.

Table 1: Logical Network Interfaces on the ePDG

Interface	Description
SWu Interface	The secure interface to the WLAN UEs in the untrusted non-3GPP IP access network, the SWu interface carries IPSec tunnels. The ePDG uses IKEv2 signaling to establish IPSec tunnels between the UEs and the ePDG. It also supports the negotiation of configuration attributes such as IP address, DNS, and P-CSCF in the CP (Configuration Parameters) payload of IKE_AUTH Request and Response messages.

Interface	Description
S2b Interface	The interface to the P-GW, the S2b interface runs PMIPv6 (Proxy Mobile IP version 6)/GTPv2 protocol to establish WLAN UE sessions with the P-GW. It also supports the transport of P-CSCF attributes and DNS attributes in PBU (Proxy-MIP Binding Update)/Create Session Request and PBA (Proxy-MIP Binding Acknowledgement)/Create Session Response messages as part of the P-CSCF discovery performed by the WLAN UEs.
SWm Diameter Interface	The interface to the 3GPP Diameter AAA server, the SWm interface is used for WLAN UE authentication. It supports the transport of mobility parameters, tunnel authentication, and authorization data. The EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) method is used for authenticating the WLAN UEs over this interface. SWm interface supports both TCP and SCTP protocols. Below are the default SCTP Parameters: • addip_enable 1 • association_max_retrans 10 • cookie_preserve_enable 1 • hb_interval 30000 • max_burst 4 • max_init_retransmits 8 • path_max_retrans 5 • prsctp_enable 1 • rcvbuf_policy 0 • rto_alpha_exp_divisor 3 • rto_beta_exp_divisor 2 • rto_initial 3000 • rto_max 60000 • rto_min 1000 • sack_timeout 200 • sndbuf_policy 0 • valid_cookie_life 60000

Transport Combinations

Table 2: Transport Combinations for the ePDG

IP Address Allocated by the P-GW for the WLAN UEs	IPSec Tunnels (between the WLAN UEs and the ePDG)	GTPv2	Combination Supported for Deployment?
IPv4	IPv4	IPv4	Yes
IPv4	IPv6	IPv6	Yes
IPv4	IPv6	IPv4	Yes
IPv4	IPv4	IPv6	Yes
IPv6	IPv4	IPv4	Yes
IPv6	IPv6	IPv6	Yes
IPv6	IPv6	IPv4	Yes
IPv6	IPv4	IPv6	Yes
IPv4v6	IPv4	IPv4	Yes
IPv4v6	IPv6	IPv6	Yes
IPv4v6	IPv4	IPv6	Yes
IPv4v6	IPv6	IPv4	Yes

The above table lists the IPv4/IPv6 transport combinations for the ePDG which support for the deployment of transport combination.

PMIPv6 S2b IPv6 transport is qualified.

Features and Functionality

This section describes the ePDG features and functionalities.

Supported Platforms:

All the features below are supported on the following platforms unless mentioned otherwise:

- Cisco ASR 5000 /ASR 5500 (DPC1/DPC2) chassis running the StarOS operating system
- Virtualized Packet Core (VPC)
- Ultra Services Platform-based Ultra Gateway Platform (UGP) virtual network function (VNF)

The following are the ePDG features:

- ePDG Service, on page 37
- IKEv2 and IPSec Encryption, on page 42

- Emergency APN Support on ePDG, on page 27
- Passing on UE Tunnel Endpoint Address over SWm Support, on page 55
- Custom SWm to SWu error code mapping, on page 13
- ePDG Bearer Duration KPIs, on page 27
- Data Buffering Support for DL Packets Before Session Establishment, on page 13
- Downlink DSCP Marking(SWu), on page 16
- ePDG Fast Re-Auth Support, on page 28
- ePDG Offline charging, on page 34
- UE Local IP Address IE in the S2B Interface over GTPv2, on page 67
- AES-NI Support, on page 9
- IPSec Large Support, on page 48

AAA Server Groups

A value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries. This feature provides support for up to 800 AAA server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication, and/or mediation servers are supported per chassis.

Add Health Monitoring for Cavecreek Crypto Chip

System can be recovered by rebooting the card if the chip operations are failing continuously. Health monitoring of Crypto Chip is now supported with enable/disable CLI. By default this feature is disabled.

Configuring Health monitoring of Crypto Chip

The **health-monitoring crypto-chip** CLI command is introduced to configure health monitoring failure threshold:

```
configure
          health-monitoring crypto-chip  failure-threshold failure_threshold

          no health-monitoring crypto-chip
          end
```

Note **no** - This option disables the Health Monitoring of Crypto Chip.

AES-NI Support

Intel® AES New Instructions (Intel® AES NI) is a new encryption instruction set that improves on the Advanced Encryption Standard (AES) algorithm and accelerates the encryption of data in the Intel® Xeon® processor family and the Intel® Core™ processor family.

Important The AES-NI Transform Encryption is supported only on the Ultra Services Platform-based Ultra Gateway Platform (UGP) virtual network function (VNF).

AES-NI capability support

ePDG is enhanced to support the IKEv2 & IPSec encryption utilizing the AES-NI capability. In SW ePDG the IPsec encryption/decryption is done in IFTASK (DPDK based SW component). By default the AES-NI capability is enabled however there is provision to turn it off at init time using the "**[no] require aes-ni capability**" configuration.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the System Administration Guide for your deployment

AES-NI Transform Set Support

ePDG is enhanced to have optional capability of allowing only AES-NI accelerated IKEv2 and IPsec algorithms in configuration. This helps the operator/user to configure the correct set of AES-NI accelerated algorithm set in configuration. For achieving this feature a new configuration is added "**[no] require aes-ni transform-set**". By default the behavior is to allow both AES-NI and non AES-NI algorithms, this keeps backward compatibility. However when this configuration is used then ePDG keeps check of allowing only the AES-NI accelerated IKEv2 & IPsec algorithms and throws error message if other algorithms are tried to be configured.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the System Administration Guide for your deployment

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

The system can be configured to collect bulk statistics and send them to a collection server called a receiver. Bulk statistics are collected in a group. The individual statistics are grouped by schema. The following is a partial list of supported schema:

- **ePDG:** Provides statistics to support the ePDG.

- **ePDG-APN:** Provides statistics to support the ePDG APN level statistics
- **System:** Provides system-level statistics.
- **Card:** Provides card-level statistics.
- **Port:** Provides port-level statistics.

The system supports the configuration of up to four sets of receivers. Each set can have primary and secondary receivers. Each set can be configured to collect specific sets of statistics from the various schema. Bulk statistics can be periodically transferred, based on the transfer interval, using ftp/tftp/sftp mechanisms.

Bulk statistics are stored on the receivers in files. The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for headers and footers only), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics Server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

Important For more information on bulk statistics, see the *System Administration Guide.*

Child SA Rekeying

Rekeying of an IKEv2 Child SA (Security Association) occurs for an already established Child SA whose lifetime is about to exceed a maximum limit. The ePDG initiates rekeying to replace the existing Child SA. The ePDG-initiated rekeying is disabled by default. This is the recommended setting, although rekeying can be enabled using the Crypto Configuration Payload Mode commands.

Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

The congestion control feature monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact on the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the

Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated. A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

- **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
- **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed. The ePDG supports congestion policies to either drop or reject new calls when congestion is detected in the system.

The congestion control overload disconnect feature can also be enabled for disconnecting passive calls during an overload situation. The ePDG selects passive calls based on the overload disconnect configuration options.

The following table lists the **congestion-control threshold** command options supported on the ePDG.

Table 3: Supported Congestion Control Threshold Command Options

Option	Description
license-utilization *percent*	The percent utilization of licensed session capacity as measured in 10 second intervals. *percent* can be configured to any integer value from 0 to 100. Default: 100
max-sessions-per-service-utilization *percent*	The percent utilization of the maximum sessions allowed per service as measured in real time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. *percent* can be an integer from 0 through 100. Default: 80
port-rx-utilization *percent*	The average percent utilization of port resources for all ports by received data as measured in 5 minute intervals. *percent* can be an integer from 0 through 100. Default: 80

Option	Description
port-specific { *slot/port* **| all } [rx-utilization** *percent* **] [tx-utilization** *percent* **]**	Sets port-specific thresholds. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide. *slot/port*: Specifies the port for which port-specific threshold monitoring is being configured. The slot and port must refer to an installed card and port. **all**: Set port specific threshold monitoring for all ports on all cards. **rx-utilization** *percent*: Default 80. The average percent utilization of port resources for the specified port by received data as measured in 5 minute intervals. *percent* must an integer from 0 through 100. **tx-utilization** *percent*: Default 80. The average percent utilization of port resources for the specified port by transmitted data as measured in 5 minute intervals. *percent* must an integer from 0 through 100. Default: Disabled
port-tx-utilization *percent*	The average percent utilization of port resources for all ports by transmitted data as measured in 5 minute intervals. *percent* can be an integer from 0 through 100. Default: 80
service-control-cpu-utilization *percent*	The average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals. *percent* can be an integer from 0 through 100. Default: 80
system-cpu-utilization *percent*	The average percent utilization for all PSC2 CPUs available to the system as measured in 10-second intervals. *percent* can be an integer from 0 through 100. Default: 80
system-memory-utilization *percent*	The average percent utilization of all CPU memory available to the system as measured in 10-second intervals. *percent* can be an integer from 0 through 100. Default: 80

Important For more information on the congestion control command options discussed in the table above, and configuration instructions, see the *System Administration Guide.* For more information on the **congestion-control threshold** command, see the *eHRPD/LTE Command Line Interface Reference* section of *CLI Reference Guide*.

Custom SWm to SWu error code mapping

ePDG does supports mapping of SWm to SWu error codes so that device can identify whether its temporary failure or permanent and can accordingly try connecting to the ePDG.

The communication service providers (CSP) would like the ability to take different actions depending on the severity of the error received from the AAA (SWm interface). If there is a temporary congestion in the network, a retry is appropriate.

In compliance with RFC 5996 2.21.2 ePDG sends AUTHENTICATION_FAILED/24 as Notify Error message type in IKE_AUTH_RESP message on SWu interface for all the SWm interface error codes.

The ePDG needs mapping of SWm to SWu error codes for communicating different error codes to device, enabling device to identify whether its temporary failure or permanent and can accordingly try connecting to the ePDG.

The ePDG continues to release the call while notifying the UE about the SWm error, however the UE based on error code shall take decision when to try connecting again.

For the mapping ePDG uses Notify Error Message type between 31 to 8191 from the range reserved for IANA or from the private range 8192 to 16383.

Data Buffering Support for DL Packets Before Session Establishment

To establish ePDG call once the PGW sends the create session response message to ePDG the call setup is complete at PGW and Downlink traffic may come. However on ePDG processing of create session response and setting up of IPsec tunnel may take small duration, so it is required that before bearer establishment and IPsec tunnel establishment is completed ePDG should have capability to buffer the data. In case of handover especially when the LTE bearer is torn down after sending create session response the downlink traffic shall be sent over the WLAN so this becomes even more important to buffer data on ePDG avoiding any traffic loss.

3GPP standards section 8.6.2 "Handover from 3GPP access to untrusted Non-3GPP IP Access with GTP on S2b" indicates that traffic can come from PGW to ePDG before even the session setup is done at ePDG (during the processing of create session response at ePDG).

Dead Peer Detection

The ePDG supports DPD (Dead Peer Detection) protocol messages originating from the ePDG and the WLAN UEs. DPD is performed when no IKE/IPSec packets reach the ePDG within the configured DPD interval. DPD is configured in the crypto template in the ePDG service. The administrator can also disable DPD. However, the ePDG always responds to DPD availability checks initiated by the UE, regardless of the ePDG idle timer configuration.

Default APN Support

The ePDG supports a default APN when APN information is not available from the WLAN UEs over the SWu interface.

When the APN information is received from the WLAN UEs, the information is sent towards the AAA server via DER (Diameter EAP Request) messages. When the APN information is absent, the AAA server provides the default APN to the ePDG in a DEA (Diameter EAP Answer) message.

The maximum attribute size in Diameter-EAP-Answer (DEA) message is 3400 bytes.

Deprecated IPSec/IKEv2 Algorithms Support

Deprecated algorithms supported removed under IPSec/IKEv2 transform set.

Following algorithms supported is removed under IPSec/IKEv2 transform set as they are deprecated:

- AES-GCM-128 and 64 bit ICV
- AES-GCM-128 and 96 bit ICV

Important Algorithms support changes are applicable only to the trusted builds (DH group5).

The following security supplement certificates signing schema are deprecated for the trusted builds:

- MD2WithRSAEncryption
- MD4WithRSAEncryption
- MD5WithRSAEncryption
- RIPEMD128WithRSAEncryption
- RIPEMD160WithRSAEncryption
- RIPEMD256WithRSAEncryption

Command Changes

crypto template min-key-size

Use the following configuration to set minimum key size.

```
configure
   context context_name
      crypto template crypto_template_name ikev2-dynamic
      authentication min-key-size min_key_size
      [ default | no ] authentication min-key-size
      end
```

NOTES:

- **authentication min-key-size** *min_key_size*: Sets minimum certificate key size, *min_key_size* must be an integer between 255 to 8192.
- **default**: Sets default key size. Default is 255
- **no**: Disables minimum key size validation feature.

crypto map min-key-size

Use the following configuration to set minimum key size.

```
configure
  context context_name
    crypto map crypto_map_name [ikev2-ipv4 | ikev2-ipv6 ]
    authentication min-key-size min_key_size
    [ default | no ] authentication min-key-size
    end
```

NOTES:

- **authentication min-key-size** *min_key_size*: Sets minimum certificate key size, *min_key_size* must be an integer between 255 to 8192.
- **default**: Sets default key size. Default is 255
- **no**: Disables minimum key size validation feature.

DER Format Certificate Size Limit

The supported size of the certificates configured on DER/PEM and the private key in DER/PEM has been increased. Now certificates of larger sizes can be configured.

The new supported size of certificate configured in DER is 6144 bytes and PEM is 8192 bytes. The new supported size of private key in DER is 3072 bytes and PEM is 4096 bytes.

DH Exponential Usage Software

Diffie-Hellman (DH) operation can be optimized by reusing Private Key and KE Payload for multiple sessions for one second. This optimization is based on RFC 7296 (2.12. Reuse of Diffie-Hellman Exponentials) for reuse of DH keys.

The DH group key exponential is reused within one second for multiple sessions. This enhancement is controlled using the **ikev2-ikesa dh-group** CLI command.

For more information on **ikev2-ikesa dh-group** command, refer to the *Command Line Interface Reference*.

DNS Request Support

During IPSec tunnel establishment, the WLAN UEs can request an IP address for the DNS in the CP payload (CFG_REQUEST). The ePDG retrieves the request from the CFG_REQUEST attribute of the first IKE_AUTH message exchange and includes it in the PBU (Proxy-MIP Binding Update) message sent to the P-GW.

The ePDG sends the PBU message by framing the MIPv6 APCO VSE (Additional Protocol Configuration Options Vendor Specific Extension) with an IPv6 and/or IPv4 DNS request to the P-GW. Once the response is received from the P-GW with the list of IPv6 and/or IPv4 DNS addresses in the returned MIPv6 APCO VSE, the ePDG includes the final address(es) in the CP payload (CFG_REPLY) of the final IKE_AUTH Response message sent to the UE.

In case the Protocol used on S2b is GTPv2 then APCO is used in Create Session Request message for requesting the IPv4 or IPv6 DNS server address request and then P-GW communicates the DNS server addresses in the APCO IE in the Create Session Response Message, the ePDG includes the final address(es) in the CP payload (CFG_REPLY) of the final IKE_AUTH Response message sent to the UE.

Note that the ePDG includes a maximum of two IPv4 DNS addresses and/or a maximum of two IPv6 DNS addresses in the CP payload (CFG_REPLY).

Downlink DSCP Marking(SWu)

The ESP IP header of the downlink packet in SWu interface sent out of ePDG has the TOS value copied from the inner IP payload of the ESP packet. But as per the customer requirement the TOS value should be taken from the configuration or GTPU IP header received on S2B side.

Functional description

The ePDG marks the DSCP value in the ESP IP header while sending out in the SWu interface(both IPv4 and IPv6) based on the following order of priority:

1. DSCP Configuration per QCI
   - Use command **qci** *num* **downlink encaps-header dscp-marking** *dscp-marking-value* to configure marking of specific DSCP in downlink direction per QCI.
2. From GTPU header received from PGW.

Download DSCP marking feature is backward compatible, where the Inner-GTP IP packet(S2B) DSCP value should be copied to the outer ESP IP packet(SWu). Use command **qci** *num* **downlink encaps-header copy-inner** *dscp-marking-value* to enable copying of DSCP value from inner-gtp-ip packet header(S2B) to the outer-esp header(SWu)

DSCP marking is supported in different platforms like Cisco ASR 5500 and VPC-Si/VPC-Di.

DSCP and 802.1P Marking

The ePDG can assign DSCP levels to specific traffic patterns in order to ensure that the data packets can be delivered according to the precedence with which they are tagged. The DiffServ markings can be applied to the IP header of the every subscriber data packet transmitted over the SWu and the S2b[GTPv2] interface.

The specific traffic patterns are classified as per their associated QCI/ARP value on the GTP-tunnel. Data packets falling under the category of each of the traffic patterns are tagged with a DSCP marking.

For uplink traffic, i.e. traffic from ePDG to P-GW through GTP tunnel, DSCP markings can be configured using global qci-qos mapping configuration association in ePDG service. In this case, only outer IP header is used for routing the packet over GTP-u' interface. Hence TOS field of only outer IP header is changed, i.e. subscriber packet is not marked with DSCP value at ePDG.

ePDG service does have configuration for association of the global configured qci-qos mapping and further in global qci-qos mapping configuration its expected that encaps-header configuration for dscp marking shall be used for setting the TOS value in the outer IP header.

Following is the global configuration under **qci-qos** mapping:

qci num [uplink { encaps-header { copy-inner | dscp-marking hex } | 802.1p-value num }]

The 802.1p marking shall be done on the uplink traffic per the qci-qos mapping global configuration corresponding to the map configured under ePDG service. This is similar configuration as described above for DSCP marking.

The 802.1p marking shall be done in the "user priority" bits of the "TAG" field in the 802.1q tagged frame.

ePDG also supports:

- DSCP marking of Data Packets in uplink (UE->ePDG->PGW) using qci-qos mapping configuration which can be associated to epdg-service

- ePDG marking the inner IP packet DSCP value received from PGW to the outer ESP header in SWu interface
- DSCP marking of Signaling packets (GTPC, on S2b interface) using CLI in egtp-service configuration
- DSCP marking of diameter packets using CLI in Diameter Endpoint configuration

Dual Stack Support

The ePDG supports PDN type IPv4v6. The ePDG handles traffic originating from both IPv4 and IPv6 UE addresses based on configured traffic selectors. Here Dual stack is mentioned for subscriber traffic (inner IP packets).

The ePDG determines the PDN type based on the requested IP address versions sent from the UE in the CP payload (CFG_REQUEST) within the IKE_AUTH Request message. The ePDG sets the IPv6 Home Network Prefix option and IPv4 Home Address Request option parameters when sending the PBU (Proxy-MIP Binding Update) message to the P-GW, specifying the PDN type as IPv4v6. In case the protocol used on S2b is GTPv2 then the ePDG sets the PDN Type inside PAA (PDN Address Allocation) as IPv4v6 and sends the same in Create Session Request Message to the P-GW. The ePDG sends the addresses allocated by the P-GW in the PBA (Proxy-MIP Binding Acknowledgement) / Create Session Response message to the UE via the CP payload (CFG_REPLY) in the IKE_AUTH Response message.

EAP Authentication

Enables secure user and device level authentication with a 3GPP AAA server or via 3GPP2 AAA proxy and the authenticator in the ePDG.

The ePDG uses the Diameter-based SWm interface to authenticate subscriber traffic with the 3GPP AAA server. Following completion of the security procedures (IKEv2) between the UE and ePDG, the ePDG selects EAP-AKA as the method for authenticating the subscriber session. EAP-AKA uses symmetric cryptography and pre-shared keys to derive the security keys between the UE and EAP server. The ePDG represents the EAP authenticator and triggers the identity challenge-response signaling between the UE and back-end 3GPP AAA server. On successful verification of user credentials, the 3GPP AAA server obtains the Cipher Key and Integrity Key from the HSS. It uses these keys to derive the MSK (Master Session Key) that are returned on EAP-Success to the ePDG. The ePDG uses the MSK to derive the authentication parameters.

After the user credentials are verified by the 3GPP AAA and HSS, the ePDG returns the PDN address obtained from the P-GW (using PMIPv6/GTPv2) to the UE. In the connection establishment procedures, the PDN address is triggered based on subscription information conveyed over the SWm reference interface. Based on the subscription information and requested PDN-Type signaled by the UE, the ePDG informs the P-GW of the type of required address (IPv6 and/or IPv4 Home Address Option for dual IPv4/v6 PDNs).

EAP-MSCHAPv2/EAP-TLS/EAP-TTLS Based Support For NON UICC Devices

The 3GPP standard provides a mechanism for the UICC (SIM based) devices connectivity to the EPC via non-3GPP access enabling them for voice and video services over WiFi. However lot of non UICC devices such as iPads, Tablets, Laptops do not have defined 3GPP standard mechanism for connecting over WLAN to EPC via ePDG. These devices can use the same LTE subscription as for the UICC device do not have potential to utlize CSPs and monetize voice and video offering by extending the same to non UICC devices.

EAP-AKA is the mechanism defined in 3GPP standards for authenticating and authorizing the mobile devices using AAA server. The non UICC devices cannot support EAP-AKA.

For non UICC devices as IMSI is not present the IMSI mentioned in below flows is vIMSI which can be alphanumeric type (limit to 24 chars) or decimal digit IMSI and in such case when alphanumeric vIMSI is used its expected that AAA server shall be providing decimal digit IMSI to ePDG for S2b interface as part of mobile-node-identifier AVP.

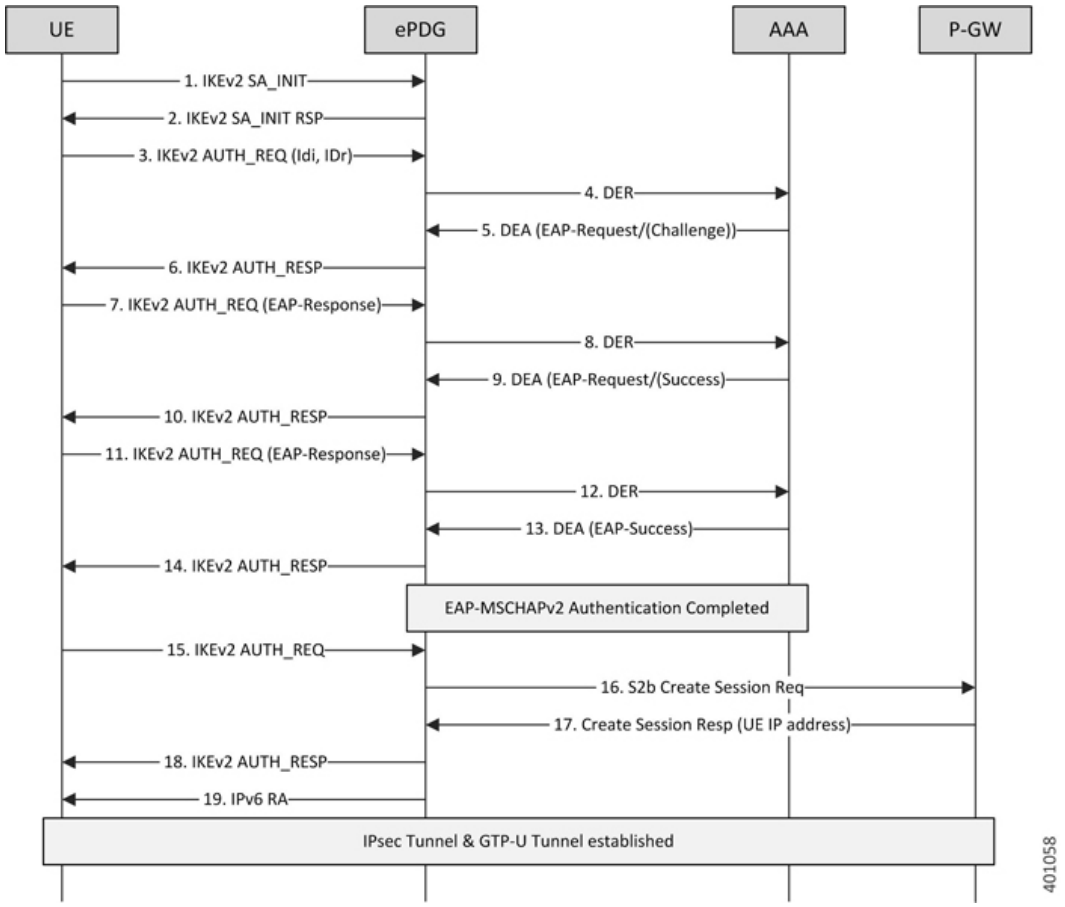
Below is the list of different authentication mechanisms which can be used with ePDG acting as EAP pass-through mode for the non UICC device support:

- EAP-MSCHAPv2
-
  - Single phase
  - Use MSCHAPv2 inside EAP
  - Challenge/Response based mechanism
  - Reference - http://tools.ietf.org/id/draft-kamath-pppext-eap-mschapv2-01.txt and RFC 3079
- EAP-TTLS (using MS-CHAPv2)
  - EAP method encapsulating TLS session
  - Two phases
    - Handshake phase (server authentication and key generation)
    - Data Phase (client authentication)
  - Handshake phase provides secure channel for data phase
  - Use MSCHAPv2 for authenticating client/device
  - Reference - RFC 5281
- EAP-TLS
  - Single phase
  - EAP method encapsulating TLS session
  - Use certificates between UE and AAA server for mutual authentication
  - Reference - RFC 5216

EAP-MSCHAPv2 authentication mechanism call flow

In this authentication mechanism the ePDG shall be acting in EAP pass-through mode and the AAA server shall be authenticating the device using EAP-MSCHAPv2. The authentication mechanism does have advantage of less lengthy call flow and is standard way. Additionally the operator does not require having certificate based infrastructure. The disadvantage is that MSK is 64 bytes but with 32 byte key and remaining 32 bytes as zeros as opposed to EAP-AKA where we have 64 byte non zero MSK. So effectively weaker authentication mechanism key.The Following diagram shows the call flow for the EAP-MSCHAPv2 based authentication:

Figure 2: EAP-MSCHAPv2 flow



1. UE ePDG: IKEv2 SA_INIT UE (UICC based) sends IKE_SA_INIT Request (SA, KE, Ni, NAT-DETECTION Notify).
2. ePDG UE: IKEv2 SA_INIT RSP The ePDG responds with an IKE_SA_INIT Response (SA, KE, Nr payloads, NAT-Detection Notify).
3. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH_REQ (IDi, [CERTREQ], IDr, SA, CP (CFQ_REQUEST (INTERNAL_IP6_ADDRESS, [INTERNAL_IP6_DNS], [INTERNAL_IP6_PCSCF]), TSi, TSr)). The UE does not include AUTH payload to indicate that it will use the EAP-MSCHAPv2 method for authenticating itself to AAA. IDi contains the NAI in the form "A<IMSI> nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org". Per standards the prefix can be 0/1 indicating EAP-AKA/EAP-SIM now as we shall be indicating to AAA server that use different authentication method here EAP-MSCHAPv2 so can indicate using "A". ePDG shall be transparent to received prefix and shall send to AAA server so that operator is free to use any prefix except the defined ones.
4. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host,Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload, User-Name (NAI), RAT-Type (WLAN), MIP6-Feature-Vector, Visited-Network-Identifier) message to the 3GPP AAA Server. The EAP-Payload shall contain the UE identity encoded by ePDG.
5. AAA server ePDG: DEA The 3GPP AAA Server initiates the authentication challenge and responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload). The EAP-Payload shall contain the Challenge packet which is used to begin the EAP MS-CHAP-V2 protocol.

6. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (IDr, [CERT (X509 CERTIFICATE SIGNATURE)], EAP Payload) The IDr is the identity of the ePDG and if the UE requests for certificates then CERT is included. The EAP message received from the 3GPP AAA Server (EAP-Request/Challenge) is included in order to start the EAP procedure over IKEv2.
7. UE ePDG: IKEv2 AUTH_REQ The UE sends EAP message in IKE_AUTH Request (EAP) with user-name, MS-CHAP2- Response AVPs.The EAP message shall be of EAP-Type=EAP-MS-CHAP-V2(Response).
8. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type (AUTHORIZE_AUTHENTICATE), EAP-Payload) message to the 3GPP AAA Server. The EAP-Payload shall contain the message as sent by UE.
9. AAA server ePDG: DEA The 3GPP AAA Server on successful authentication responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload)
10. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the EAP-MSCHAPv2 message as received from the AAA server.
11. UE ePDG: IKEv2 AUTH_REQ The UE sends IKE_AUTH Request (EAP) with EAP-MSCHAPv2 "Success Response packet". UE successfully validates the EAP MS-CHAP-V2 Success Request packet sent by the AAA server, respond.
12. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload) message to the 3GPP AAA Server. The EAP-Payload shall contain the message as sent by UE.
13. AAA server ePDG: DEA The 3GPP AAA Server sends an EAP success (Session-Id, Auth-Application-Id: 16777264, Result-Code, Origin-Host, Origin-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload User-Name(0<IMSI>mnc<mnc val>.mcc<mcc val>.pub.3gppnetwork.org), EAP-Master-Session-Key, APN-Configuration (Context-Identifier, PDN-Type: IPv4v6, Service-Selection (apn name), MIP6-Agent-Info), Auth-Session-State: STATE_MAINTAINED, Origin-State-Id). At this point mutual authentication is done and device is authorized by AAA server. The MSK can be generated by AAA server using following logic however ePDG is transparent to MSK generation logic and till the devices and AAA server are in sync any other logic of MSK generation should also work. MSK = MasterReceiveKey + MasterSendKey + 32 bytes zeroes (padding) Note - Extensible Authentication Protocol Method for Microsoft CHAP derives two 16-byte keys, MasterSendKey and MasterReceiveKey (as specified in [RFC3079], section 3.3).
14. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the EAP-MSCHAPv2 message as received from the AAA server.
15. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH request (AUTH) The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.
16. ePDG PGW: S2b Create Session Req ePDG sends Create Session Request (IMSI, [MSISDN],Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, [APCO], Bearer Contexts(), [Recovery], [Private IE (P-CSCF)]). Selection Mode shall be set to "MS or network provided APN subscribed verified". The PGW performs the necessary interactions with 3GPP-AAA, PCRF and OCS/OFCS. ePDG shall set the HO in Indication flags IE and also the preserved IP address as received from UE in PAA IE.
17. PGW ePDG: Create Session Resp The PGW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, PGW S2b F-TEID, PAA, [APN-AMBR],APCO, Bearer Contexts Created (EPS Bearer ID, Cause, [TFT], S2b-U PGW F-TEID, Bearer Level QoS), [Recovery], [Private IE (P-CSCF)]) message.
18. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (AUTH, CP, SA, CFG_REPLY ([INTERNAL_IP4_ADDRESS], [INTERNAL_IP4_NETMASK], [INTERNAL_IP4_DNS],

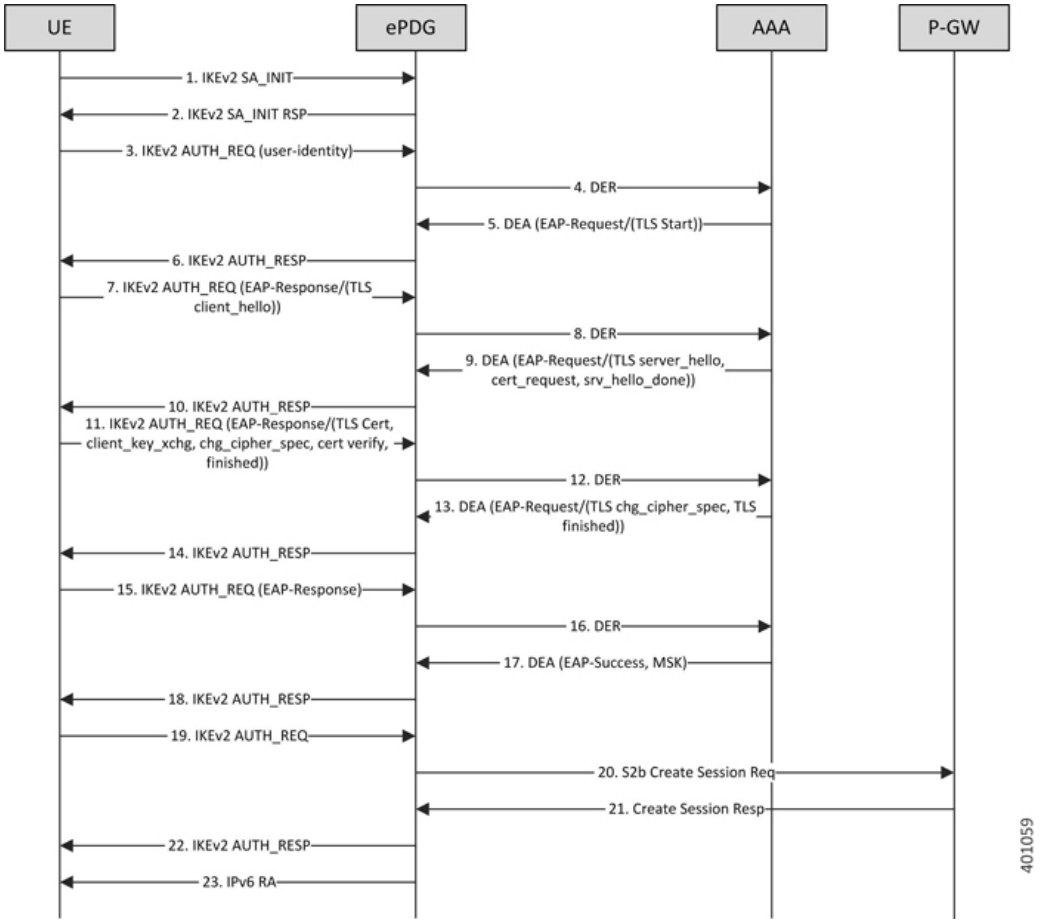
INTERNAL_IP6_ADDRESS, INTERNAL_IP6_SUBNET, INTERNAL_IP6_DNS, [P-CSCF]) TSi, TSr) At this stage the ePDG has completed the ipsec SA and tunnel setup and also GTP-U tunnel setup thus completing the data path. The IP address provided by PGW is communicated to UE.

19. ePDG UE: IPv6 RA The assumption is that the IP stack needs the RA to initialize the address.

EAP-TLS authentication mechanism Call Flow

In this mechanism it's assumed that the authenticator entity shall be AAA server supporting the certificate based authentication. The ePDG shall be acting in EAP pass-through mode thus communicating the EAP-TLS negotiation between device and AAA server. The AAA server once completing the authentication mechanism shall be sharing the MSK to ePDG for generating the AUTH parameters and completing the IKEv2 authentication. Following diagram shows the call flow for the EAP-TLS based authentication:

Figure 3: IPsec Based EAP-TLS Flow



1. UE ePDG: IKEv2 SA_INIT UE (UICC based) sends IKE_SA_INIT Request (SA, KE, Ni, NAT-DETECTION Notify).
2. ePDG UE: IKEv2 SA_INIT RSP The ePDG responds with an IKE_SA_INIT Response (SA, KE, Nr payloads, NAT-Detection Notify).
3. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH_REQ (IDi, [CERTREQ], IDr, SA, CP (CFQ_REQUEST (INTERNAL_IP6_ADDRESS, [INTERNAL_IP6_DNS], [INTERNAL_IP6_PCSCF]), TSi, TSr)). The UE does not include AUTH payload to indicate that it will use the EAP-TLS method for authenticating itself to AAA. IDi contains the NAI in the form "A<IMSI>

nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org". Per standards the prefix can be 0/1 indicating EAP-AKA/EAP-SIM now as we shall be indicating to AAA server that use different authentication method here EAP-TLS so can indicate using "A". ePDG shall be transparent to received prefix and shall send to AAA server so that operator is free to use any prefix except the defined ones.

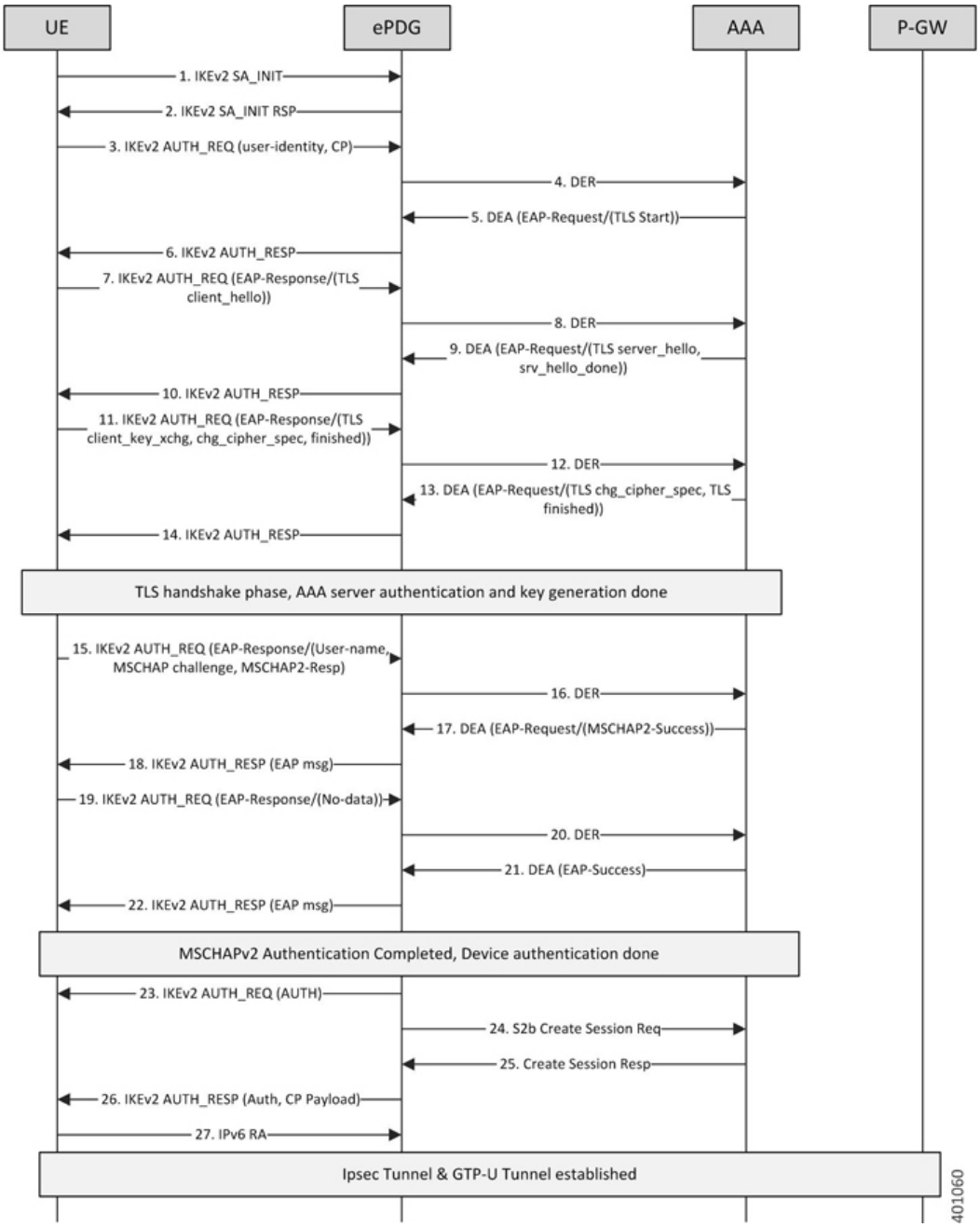
4. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload, User-Name (NAI), RAT-Type(WLAN), MIP6-Feature-Vector, Visited-Network-Identifier) message to the3GPP AAA Server. The EAP-Payload shall contain the UE identity encoded by ePDG.
5. AAA server ePDG: DEA The 3GPP AAA Server initiates the authentication challenge and responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload). The EAP-Payload shall contain the EAP-TLS/Start, the Start 'S' bit is set with no data.
6. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (IDr, [CERT (X509 CERTIFICATE SIGNATURE)], EAP Payload) The IDr is the identity of the ePDG and if the UE requests for certificates then CERT is included. The EAP message received from the 3GPP AAA Server (EAP-Request/Start) is included in order to start the EAP procedure over IKEv2.
7. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH_REQ (EAP payload) containing the TLS client hello handshake message.
8. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload, User-Name (NAI), RAT-Type(WLAN), MIP6-Feature-Vector, Visited-Network-Identifier) message to the 3GPP AAA Server. The EAP-Payload shall contain the TLS client hello handshake message.
9. AAA server ePDG: DEA The 3GPP AAA Server initiates the authentication challenge and responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload). The AAA server will then respond with an EAP-Request packet with EAP-Type=EAP-TLS. The data field of this packet will encapsulate one or more TLS records. These will contain a TLS server_hello handshake message, possibly followed by TLS certificate, server_key_exchange, certificate_request, server_hello_done and/or finished handshake messages, and/or a TLS change_cipher_spec message.
10. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the TLS message as received from the AAA server.
11. UE ePDG: IKEv2 AUTH_REQ The UE sends EAP message in IKE_AUTH Request (EAP). The data field of this packet MUST encapsulate one or more TLS records containing a TLS client_key_exchange, change_cipher_spec, and finished messages.
12. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host,Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload) message to the 3GPP AAA Server. The EAP-Payload shall contain the message as sent by UE.
13. AAA server ePDG: DEA The 3GPP AAA Server on successful authentication responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload) where EAP-Payload does contain the TLS finished message.
14. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the TLS message as received from the AAA server.
15. UE ePDG: IKEv2 AUTH_REQ The UE sends EAP message in IKE_AUTH Request (EAP) with no data.
16. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type (AUTHORIZE_AUTHENTICATE), EAP-Payload) message to the 3GPP AAA Server. The EAP-Payload shall contain the message as sent by UE.

17. AAA server ePDG: DEA The 3GPP AAA Server sends an EAP success (Session-Id, Auth-Application-Id: 16777264, Result-Code, Origin-Host, Origin-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload User-Name(0<IMSI>mnc<mnc val>.mcc<mcc val>.pub.3gppnetwork.org), EAP-Master-Session-Key, APN-Configuration (Context-Identifier, PDN-Type: IPv4v6, Service-Selection (apn name), MIP6-Agent-Info), Auth-Session-State:STATE_MAINTAINED, Origin-State-Id). At this point device is authenticated and authorized by AAA server.
18. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the TLS message as received from the AAA server.
19. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH request (AUTH) The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INITmessage.
20. ePDG PGW: S2b Create Session Req ePDG sends Create Session Request (IMSI, [MSISDN],Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, [APCO], Bearer Contexts(), [Recovery], [Private IE (P-CSCF)]). Selection Mode shall be set to "MS or network provided APN subscribed verified". The PGW performs the necessary interactions with 3GPP-AAA, PCRF and OCS/OFCS. ePDG shall set the HO in Indication flags IE and also the preserved IP address as received from UE in PAA IE.
21. PGW ePDG: Create Session Resp The PGW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, PGW S2b F-TEID, PAA, [APN-AMBR],APCO, Bearer Contexts Created (EPS Bearer ID, Cause, [TFT], S2b-U PGW F-TEID, Bearer Level QoS), [Recovery], [Private IE (P-CSCF)]) message.
22. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (AUTH, CP, SA, CFG_REPLY([INTERNAL_IP4_ADDRESS], [INTERNAL_IP4_NETMASK],[INTERNAL_IP4_DNS], INTERNAL_IP6_ADDRESS, INTERNAL_IP6_SUBNET, INTERNAL_IP6_DNS, [P-CSCF]) TSi, TSr) At this stage the ePDG has completed the ipsec SA and tunnel setup and also GTP-U tunnel setup thus completing the data path. The IP address provided by PGW is communicated to UE.
23. ePDG UE: IPv6 RA The assumption is that the IP stack needs the RA to initialize the address.

EAP-TTLS authentication mechanism Call Flow

The EAP-TTLS based approach is useful when there is no certificate based infrastructure present for the operator to configure certificate for each device. Unlike EAP-TLS it enables the device authentication without certificates using customized AVPs. Here we have defined MSCHAPv2 based authentication mechanism. Here the AAA server needs to provide the key similar to MSK to ePDG for validating/generating the AUTH payload during IKEv2 xchg. Following diagram shows the call flow for the EAP-TTLS based authentication:

Figure 4: IPsec EAP-TTLS MSCHAPv2 Flow



1. UE ePDG: IKEv2 SA_INIT UE (UICC based) sends IKE_SA_INIT Request (SA, KE, Ni, NAT-DETECTION Notify).
2. ePDG UE: IKEv2 SA_INIT RSP The ePDG responds with an IKE_SA_INIT Response (SA, KE, Nr payloads, NAT-Detection Notify).
3. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH_REQ (IDi, [CERTREQ], IDr, SA, CP (CFQ_REQUEST (INTERNAL_IP6_ADDRESS, [INTERNAL_IP6_DNS], [INTERNAL_IP6_PCSCF]), TSi, TSr)). The UE does not include AUTH payload to indicate that it will use the EAP-TTLS method for authenticating itself to AAA. IDi contains the NAI in the form "A<IMSI>

nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org". Per standards the prefix can be 0/1 indicating EAP-AKA/EAP-SIM now as we shall be indicating to AAA server that use different authentication method here EAP-TTLS so can indicate using "A". ePDG shall be transparent to received prefix and shall send to AAA server so that operator is free to use any prefix except the defined ones.

4. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload, User-Name (NAI), RAT-Type(WLAN), MIP6-Feature-Vector, Visited-Network-Identifier) message to the 3GPP AAA Server. The EAP-Payload shall contain the UE identity encoded by ePDG.
5. AAA server ePDG: DEA The 3GPP AAA Server initiates the authentication challenge and responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload). The EAP-Payload shall contain the EAP-TTLS/Start, the Start 'S' bit is set with no data.
6. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (IDr, [CERT (X509 CERTIFICATE SIGNATURE)], EAP Payload) The IDr is the identity of the ePDG and if the UE requests for certificates then CERT is included. The EAP message received from the 3GPP AAA Server (EAP-Request/Start) is included in order to start the EAP procedure over IKEv2.
7. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH_REQ (EAP payload) containing the TLS client hello handshake message.
8. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload, User-Name (NAI), RAT-Type(WLAN), MIP6-Feature-Vector, Visited-Network-Identifier) message to the 3GPP AAA Server. The EAP-Payload shall contain the TLS client hello handshake message.
9. AAA server ePDG: DEA The 3GPP AAA Server initiates the authentication challenge and responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload). The AAA server will then respond with an EAP-Request packet with EAP-Type=EAP-TTLS. The data field of this packet will encapsulate one or more TLS records. These will contain a TLS server_hello handshake message, possibly followed by TLS certificate, server_key_exchange, server_hello_done and/or finished handshake messages, and/or a TLS change_cipher_spec message.
10. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the TLS message as received from the AAA server.
11. UE ePDG: IKEv2 AUTH_REQ The UE sends EAP message in IKE_AUTH Request (EAP). The data field of this packet MUST encapsulate one or more TLS records containing a TLS client_key_exchange, change_cipher_spec, and finished messages.
12. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host,Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload) message to the3GPP AAA Server. The EAP-Payload shall contain the message as sent by UE.
13. AAA server ePDG: DEA The 3GPP AAA Server on successful authentication responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload) where EAP-Payload does contain the TLS finished message.
14. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the TLS message as received from the AAA server. This stage the first phase of TTLS is done completing the TLS handshake and AAA server is authenticated by device and keys are generated to secure subsequent message handling.
15. UE ePDG: IKEv2 AUTH_REQ The UE sends EAP message in IKE_AUTH Request (EAP) with user-name, MS-CHAP2- Response, MS-CHAP Challenge AVPs.
16. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm,

Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload) message to the3GPP AAA Server. The EAP-Payload shall contain the message as sent by UE.

17. AAA server ePDG: DEA The 3GPP AAA Server on successful authentication responds with DEA (Session-Id, Base AVPs, Auth-Request-Type and EAP-Payload), Upon receipt of these AVPs from the UE, the AAA server MUST verify that the value of the MS-CHAP-Challenge AVP and the value of the Ident in the client's MS-CHAP2-Response AVP are equal to the values generated as challenge material. If either item does not match exactly, the AAA server MUST reject the UE. In success case, AAA shall encode the MS-CHAP2-Success attribute.
18. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the EAP-TTLS message as received from the AAA server.
19. UE ePDG: IKEv2 AUTH_REQ The UE sends IKE_AUTH Request (EAP) with no data. Upon receipt of the MS-CHAP2-Success AVP, the UE is able to authenticate the AAA. If the authentication succeeds, the UE sends an EAP-TTLS packet to the TTLS server containing no data (that is, with a zero-length Data field). Upon receipt of the empty EAP-TTLS packet from the client, the TTLS server considers the MS-CHAP-V2 authentication to have succeeded.
20. ePDG AAA server :DER The ePDG sends the DER (Session-Id, Auth-Application-Id, Origin-Host,Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload) message to the 3GPP AAA Server. The EAP-Payload shall contain the message as sent by UE.
21. AAA server ePDG: DEA The 3GPP AAA Server sends an EAP success (Session-Id, Auth-Application-Id: 16777264, Result-Code, Origin-Host, Origin-Realm, Auth-Request-Type(AUTHORIZE_AUTHENTICATE), EAP-Payload User-Name(0<IMSI>mnc<mnc val>.mcc<mcc val>.pub.3gppnetwork.org), EAP-Master-Session-Key, APN-Configuration (Context-Identifier, PDN-Type: IPv4v6, Service-Selection (apn name), MIP6-Agent-Info), Auth-Session-State:STATE_MAINTAINED, Origin-State-Id). At this point mutual authentication is done and device is authorized by AAA server.
22. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (EAP Payload) The EAP payload shall contain the TLS message as received from the AAA server.
23. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH request (AUTH) The UE takes its own copy of the MSK asinput to generate the AUTH parameter to authenticate the first IKE_SA_INITmessage.
24. ePDG PGW: S2b Create Session Req ePDG sends Create Session Request (IMSI, [MSISDN],Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, [APCO], Bearer Contexts(), [Recovery], [Private IE (P-CSCF)]). Selection Mode shall be set to "MS or network provided APN subscribed verified". The PGW performs the necessary interactions with 3GPP-AAA, PCRF and OCS/OFCS. ePDG shall set the HO in Indication flags IE and also the preserved IP address as received from UE in PAA IE.
25. PGW ePDG: Create Session Resp The PGW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, PGW S2b F-TEID, PAA, [APN-AMBR],APCO, Bearer Contexts Created (EPS Bearer ID, Cause, [TFT], S2b-U PGW F-TEID, Bearer Level QoS), [Recovery], [Private IE (P-CSCF)]) message.
26. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (AUTH, CP, SA, CFG_REPLY([INTERNAL_IP4_ADDRESS], [INTERNAL_IP4_NETMASK],[INTERNAL_IP4_DNS], INTERNAL_IP6_ADDRESS,INTERNAL_IP6_SUBNET, INTERNAL_IP6_DNS, [P-CSCF]) TSi, TSr) At this stage the ePDG has completed the ipsec SA and tunnel setup and also GTP-U tunnel setup thus completing the data path. The IP address provided by PGW is communicated to UE.
27. ePDG UE: IPv6 RA The assumption is that the IP stack needs the RA to initialize the address.

Emergency APN Support on ePDG

ePDG supports emergency APN session to support VoWiFi calls . For areas where the LTE coverage is less or absent then the user will utilize the WiFi to perform the emergency session via ePDG.

A new ePDG-APN bulkstats schema is added to capture the APN level ePDG service statistics.

Emergency APN Support Use Cases

S.No	Use Case	Expected Behavior
1.	ePDG receives the emergency session with UE indicating the emergency APN connectivity request for UE whose profile is present at AAA/HSS.	Call should be successfully established.
2.	ePDG receives the emergency session with UE indicating the emergency APN connectivity request for UE whose authentication fails at AAA.	ePDG shall be rejecting the call.
3.	Local PGW configured within the Emergency APN support and dynamic PGW selection fails as DNS server does not respond.	ePDG shall be utilizing the APN profile configuration and establish call with local configured PGW.
4.	Local PGW configured within the Emergency APN support and PGW obtained from dynamic PGW selection fails does not responds.	ePDG shall be utilizing the APN profile configuration and establish call with local configured PGW.
5	Local configuration based PGW selection is configured as preferred way of PGW selection corresponding to emergency APN profile.	ePDG shall be utilizing the APN profile configuration and establish call with local configured PGW.

ePDG and PGW Support on the Same Chassis (with GTPv2)

ePDG and PGW services does work together in combo mode (both enabled on the same chassis) with common component resources like IPsec being utilized in best effort manner. Session recovery including card migration is supported for the combo mode

ePDG Bearer Duration KPIs

ePDG supports QCI based bearer duration information display at more granular leval to enable customers to Monitor VoWiFi dedicated bearers.

For more information on *show subscriber statistics* and for *show session duration* commands refer CLI Reference Guide.

ePDG Fast Re-Auth Support

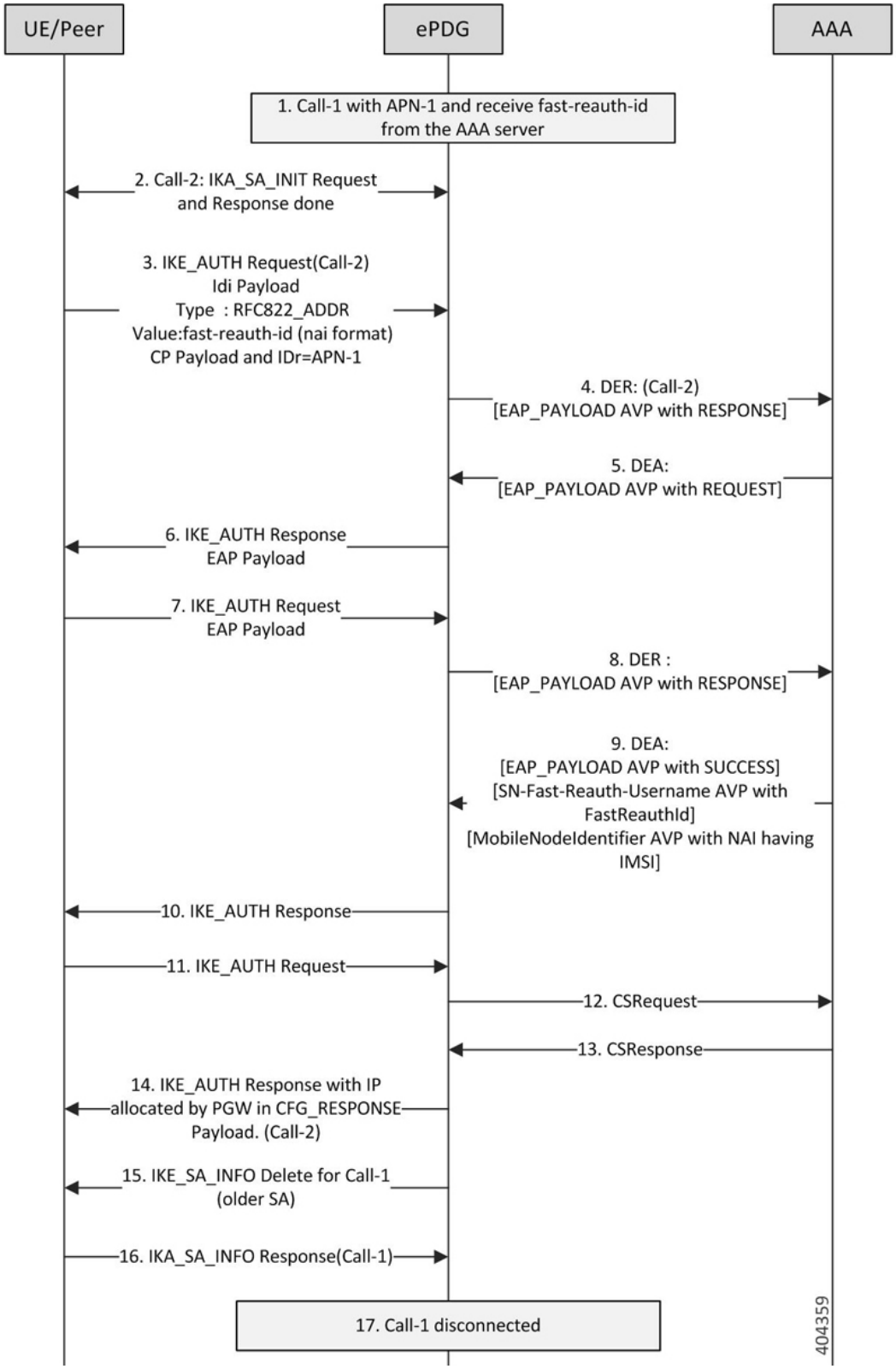
The UEs accessing through ePDG can perform multiple reattach due to movement across/within WLAN Network and can also access multiple PDN at the same time. In these cases, the UE authentication is performed frequently with AAA-server involving HSS node interaction for EAP-AKA algorithm.

The operator providing the untrusted WLAN access solution through ePDG can enable fast-reauthentication in AAA-server and UE in order to perform faster authentication and reduce the load in HSS. This is because the fast-reauthentication uses the keys derived in the previous full-authentication. Also fast-reauthentication helps the operator to enable local-policy in UE node to authenticate itself to AAA server periodically for enhanced security.

Reattach with fast-reauth-id Call flow

Below call flow describes Reattach with fast-reauth-id.

Figure 5: Reattach with fast-reauth-id (with CP Payload)



1. Call-1 established for APN-1 and AAA-Server has provided fast-reauth-id during this authentication process. ePDG will store mapping between IMSI and fast-reauth-id.
2. UE starts Call-2 for fast-reauthentication by sending the IKE-SA-INIT message to ePDG. IKE-SA established between UE and ePDG with IKA_SA_INIT message exchange.
3. The UE sends the fast-reauth-id in NAI format(fast-reauth-idrealm) in the IDi payload and the APN-1 (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The UE includes the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to give indication that it needs to reconfigure the IP address.
4. ePDG Identifies the previous session based on the received fast-reauth-id as it already created mapping. ePDG will handle this request as new session. This is because the presence of CP-Payload indicates that the call should be established till PGW without retaining the IP address(S2B interface). The ePDG sends the Diameter-EAP-Request message to the 3GPP AAA Server, containing the fast-reauth-id and APN.

Important Please note that ePDG uses the new diameter-session-id here as it is creating a new session.

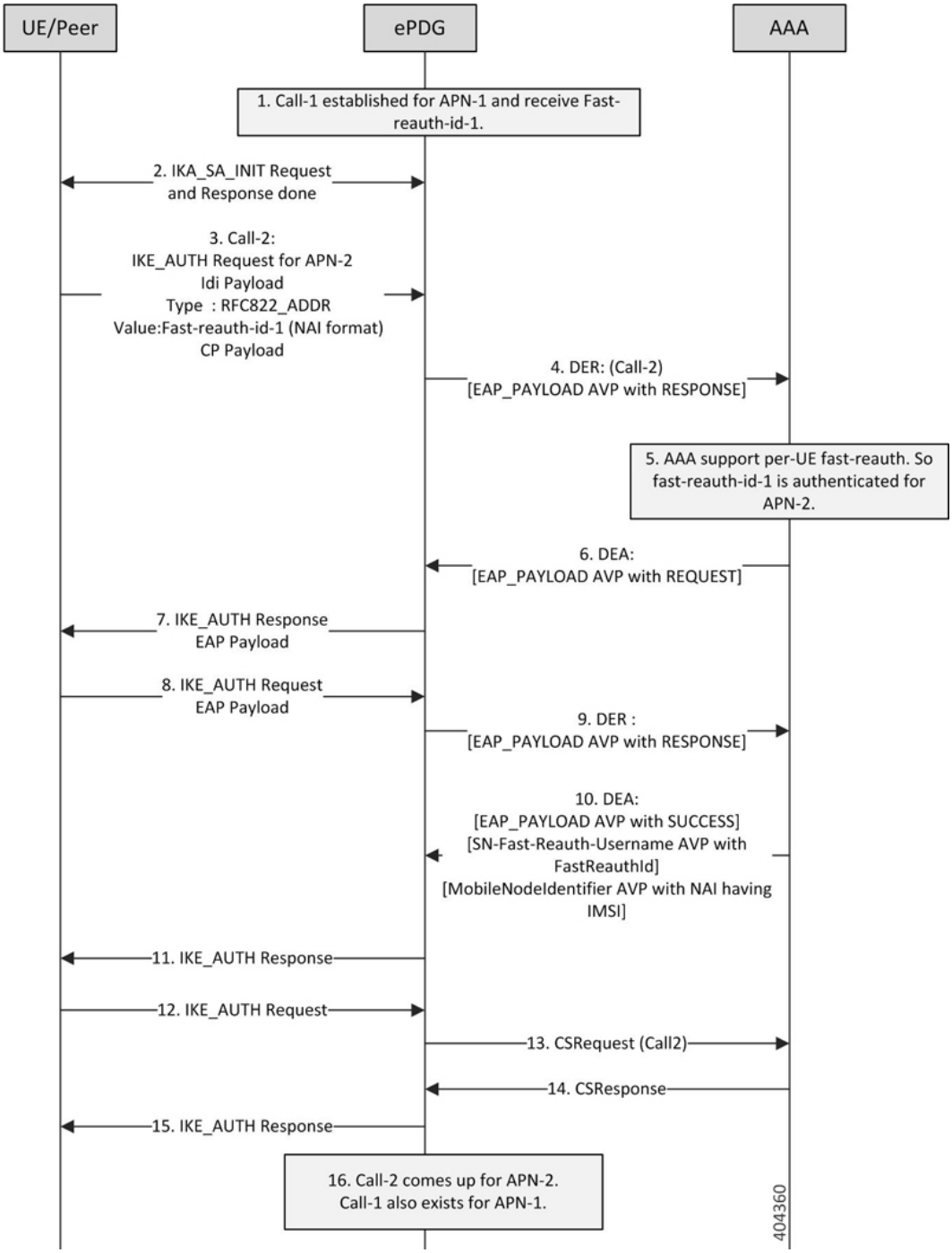
5. The 3GPP AAA Server shall validate the fast-reauthentication-id and initiates the fast re-authentication request.

Important Please note that there is no communication with HSS/HLR at this stage since fast-reauthentication-id is used. This makes the procedure faster and reduce load in HSS.

6. The ePDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). The EAP message received from the 3GPP AAA Server (EAP-Request/Fast-Reauthentication) is included in order to start the EAP procedure over IKEv2.
7. The UE checks the authentication parameters and responds to the fast-reauthentication. The only payload (apart from the header) in the IKEv2 message is the EAP message.
8. The ePDG forwards the EAP-Response/Fast-Reauthentication message to the 3GPP AAA Server.
9. The AAA checks, if the Fast-Reauthentication response is correct. When all checks are successful, the 3GPP AAA Server sends the final Diameter-EAP-Answer(with a result code indicating success) including the users IMSI, relevant service authorization information, an EAP success and the key material to the ePDG. This key material shall consist of the MSK generated during the fast-reauthentication process. AAA-Server shall include the SN-Fast-Reauth-Username AVP with the fast-reauthentication-id value given to UE in step 5. ePDG creates mapping between IMSI and Fast-reauthentication-ID at this point.
10. The EAP Success message is forwarded to the UE over IKEv2.
11. The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG in IKE_AUTH message.
12. The ePDG checks the correctness of the AUTH received from the UE. At this point the UE is authenticated. In S2b interface, ePDG initiates GTPv2 signaling between ePDG and PDN GW for creating the default-bearer for APN by sending Create-Session-Request to PGW with UE/APN details and request for IP-address allocation.
13. PGW responds with the Create-Session-Response message containing the allocation IP address, QoS details for this default-bearer connection.

14. The ePDG calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The ePDG sends the assigned Remote IP address in the configuration payload (CFG_REPLY) in the IKE_AUTH_RESPONSE message to UE. Fast-reauthentication is completed and Call-2 is connected now.
15. ePDG initiates the IKE-SA INFO_DELETE message for Call-1 to UE to delete the IKE-SA as part of call deletion.
16. UE responds with IKE-SA INFO_DELETE to delete the IKE-SA.
17. Call-1 is disconnected at ePDG.

Figure 6: Multi-pdn with fast-reauth-id (fast-reauth-id Per UE case with CP Payload)



1. Call-1 established for APN-1 and AAA-Server has provided fast-reauth-id-1 during this authentication process. ePDG will store mapping between IMSI and fast-reauth-id-1
2. UE starts Call-2 to connect to APN-2 using the fast-reauth-id-1. IKE-SA established between UE and ePDG with IKA_SA_INIT message exchange.

3. The UE sends the fast-auth-id-1 in NAI format(fast-reauth-id-1realm) in the IDi payload and the APN-2 (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The UE includes the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to give indication that it needs to configure the IP address.
4. ePDG Identifies the previous session based on the received Fast-reauth-id as it already created mapping. ePDG will handle this request as new session. This is because the request is for new APN and also the presence of CP-Payload indicates that the call should be established till PGW without retaining the IP address(S2B interface). The ePDG sends the Diameter-EAP-Request message to the 3GPP AAA Server, containing the fast-reauth-id-1 and APN-2. Please note that ePDG uses the new diameter-session-id here as it is creating a new session.
5. AAA server supports Fast-Reauthentication on per-UE basis. Hence it accepts fast-reauth-id-1 for APN-2.
6. The 3GPP AAA Server validates the fast-reauth-id-1 and initiates the fast re-authentication request.

Important Please note that there is no communication with HSS/HLR at this stage since fast-reauth-id-1 is used. This makes the procedure faster and reduce load in HSS.

The ePDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). The EAP message received from the 3GPP AAA Server (EAP-Request/Fast-Reauthentication) is included in order to start the EAP procedure over IKEv2.

7. The UE checks the authentication parameters and responds to the fast-reauthentication. The only payload (apart from the header) in the IKEv2 message is the EAP message.
8. The ePDG forwards the EAP-Response/Fast-Reauthentication message to the 3GPP AAA Server.
9. The AAA checks if the Fast-reauthentication response is correct. When all checks are successful, the 3GPP AAA Server sends the final Diameter-EAP-Answer(with a result code indicating success) including the users IMSI, relevant service authorization information, an EAP success and the key material to the ePDG. This key material consists of the MSK generated during the fast-reauthentication process. AAA-Server includes the SN-Fast-Reauth-Username AVP with the fast-reauthentication-id value given to UE in step 5. ePDG creates mapping between IMSI and Fast-reauthentication-ID at this point.
10. The EAP Success message is forwarded to the UE over IKEv2.
11. The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG in IKE_AUTH message.
12. The ePDG checks the correctness of the AUTH received from the UE. At this point the UE is authenticated. In S2b interface, ePDG initiates GTPv2 signaling between ePDG and PDN GW for creating the default-bearer for APN by sending Create-Session-Request to PGW with UE/APN details and request for IP-address allocation.
13. PGW responds with the Create-Session-Response message containing the allocation IP address, QoS details for this default-bearer connection.
14. The ePDG calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The ePDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY) in the IKE_AUTH_RESPONSE message to UE.
15. Call-2 is connected now for APN-2 and Call-1 already exists for APN-1.

ePDG Offline charging

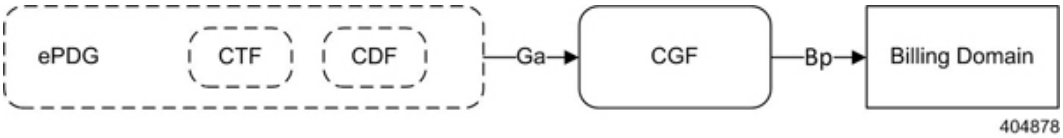
Offline charging is a process where charging information is collected concurrently with that resource usage. The charging information is then passed through a chain of logical charging functions. At the end of this process, CDR files are generated by the network, which are then transferred to the network operator's Billing Domain(BD). Charging information like amount of data transmitted in uplink and downlink direction are collected as part of ePDG-CDR are used to inter-operator settlements.

ePDG Offline charging Architecture

The ePDG Offline charging involves the following functionalists for WLAN 3GPP IP Access:

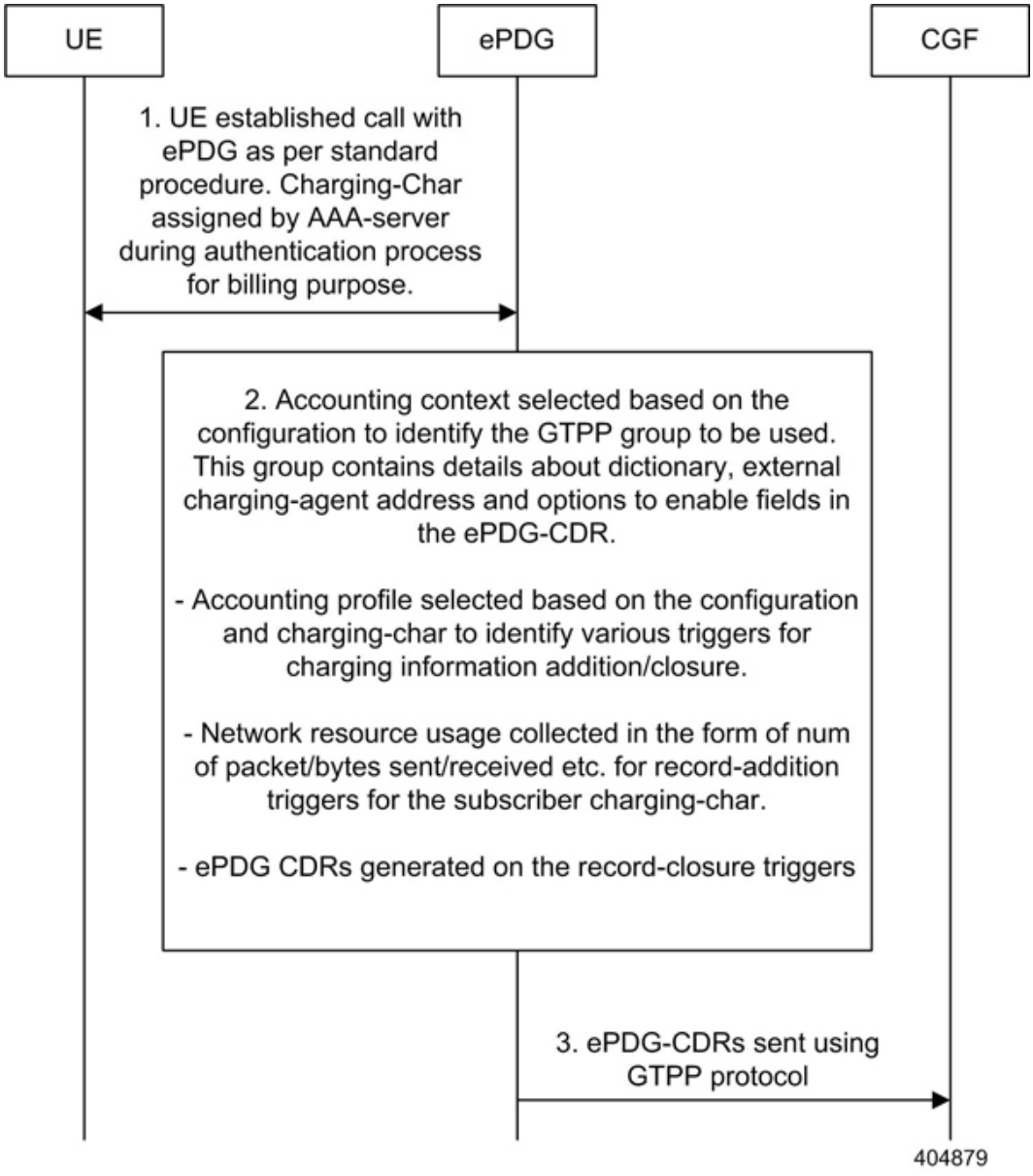
- Charging Trigger Function
- Charging Data Function
- Ga Reference Point

Figure 7: ePDG Offline Charging Architecture



The Charging Trigger Function (CTF) which is an integrated component generates charging events and forwards them to the Charging Data Function (CDF). The CDF, in turn generates ePDG-CDRs which are then transferred to the CGF. Finally, the CGF create ePDG-CDR files and forwards them to the Billing Domain. The CTF and CDF are integrated in ePDG, however, the CGF may exist as a physically separate entity or integrated to ePDG. If the CGF is external to the ePDG, then the CDF forwards the CDRs to the CGF across the Ga interface (using GTPP protocol defined in TS 32.295). ePDG-CDR format is as defined in TS 32.298 v12.6.0.

Figure 8: ePDG Offline Charging Callflow



ePDG Offline Charging

ePDG supports CDRs to bill the UEs for network resource usage as defined in 3GPP specification TS32.298.

Apart from the standard ePDG-CDR fields ePDG Offline Charging feature populates the following additional fields:

- IKEv2 tunnel endpoint IP address(UE Side tunnel endpoint address)
- Source Port number used in IKEv2 tunnel
- ePDG SWu interface IP address(ePDG side tunnel endpoint address)
- Destination Port number used in IKEv2 tunnel

- AP-MAC address used by UE to connect in WLAN network

Custom24 is the GTPP dictonary for standard ePDG-CDR as per specfications and custom38 is the GTPP dictionary for CDRs with above additional fields.

Supported Triggers for ePDG-CDRs Charging Information Addition

The "List of Traffic Volumes" attribute of the ePDG-CDR consists of a set of containers, on encountering the following trigger conditions, the charging information will be added to the container:

Qos Change: A change in the QoS will result to open the "List of Traffic Data Volumes" container being closed and added to the CDR and a new bearer specific container is opened. Also when there is a Change in QoS, the trigger will be sent to accounting module for CDR information addition using the API "sessmgr_acct_api_event(handle, params)" with the params ---> qos_change set from the sessmgr.

Tariff time: On reaching the Tariff Time Change open "List of Traffic Data Volumes" containers is closed and added to the CDR. Tariff-time change is to add charging information to CDR during a particular tariff-time of day.

Record Closure: Open "List of Traffic Data Volumes" containers is closed and added to the ePDG-CDR.

Supported Triggers for ePDG-CDR closure

The following events trigger closure and sending of ePDG-CDR:

Time Limit: CDRs are generated after every x seconds where x is the configured time limit.

Max container Triggers: Maximum number of charging condition changes (QoS/tariff time change). CDRs are generated when the max bucket limit is reached. By default its 4.

Volume limit trigger: CDRs are generated whenever the uplink or downlink data volume for the session crosses the configured uplink, downlink or total limit.

Management Intervention: CDRs can be generated by management intervention such as clear command issued by the operator to cleanup a session.

Assumptions and Limitations

- The AP-MAC address will be populated in ePDG-CDR only when it is supplied by UE during initial IKEv2 exchange in IDi payload as expected by ePDG. Please see the ePDG admin guide to understand the format of IDi payload with AP-MAC address encoded in it.
- The CDF functionality is integrated within ePDG. RF interface is not support.

ePDG P-GW selection

The ePDG selects P-GW node based one of the logic:

- eDNS
- DNS over TCP
- P-GW re-selection on session timeout
- PGW re-selection on call attempt failure due to PGW reject

eDNS

The ePDG supports extended DNS client to handle DNS response larger than 512 bytes.

RFC 1035 limits the size of DNS responses over UDP to 512 bytes. If P-GW discovery is done via DNS, there is a chance of 512 byte limit is hit as there are multiple P-GWs supporting an APN consequently having multiple responses to the DNS query, resulting in truncation of the RRs.

Extended the DNS (RFC 2671) allows the client to advertise a bigger re-assemble buffer size to the DNS server so that the server can send a response bigger than 512 bytes. An interim solution to the truncation issue is to arrange the RRs hierarchically so that the limit is never hit.

DNS over TCP

By default DNS client communicates with the server over UDP port. The client can support eDNS, DNS responses up to 4 K Bytes in size from the server. If FQDN resolves too many RRs, the 4 KB limit could be exhausted.

Use the following approach to resolve this issue:

Use TCP port when the server needs to send bigger responses (up to 64 KB), this needs to be driven by the client. When the server indicates that it is not able to send all the answers to a query by setting the truncation bit in the response header. The client on seeing this would switch to TCP port and re-sends the same query. The client continues to use UDP port for new requests.

P-GW re-selection on session timeout

During dynamic P-GW node selection by ePDG, if the selected P-GW is unreachable, the ePDG will select the next P-GW entry from the P-GW candidate list returned during the S-NAPTR procedure to set up the PDN connection.

PGW re-selection on call attempt failure due to PGW reject

ePDG attempts to select alternate PGW when the first PGW has rejected the call with the below error causes. Maximum alternate PGW selection attempts(0-64) can be configured per APN profile using CLI, default is 3.

- EGTP_CAUSE_ALL_DYNAMIC_ADDR_OCCUPIED (0x54)
- EGTP_CAUSE_NO_RESOURCES_AVAILABLE(73)
- EGTP_CAUSE_SERVICE_DENIED (0x59),
- EGTP_CAUSE_PEER_NOT_RESPONDING-(100)
- EGTP_CAUSE_SERVICE_NOT_SUPPORTED (0x44)

ePDG Service

The ePDG service enables the WLAN UEs in the untrusted non-3GPP IP access network to connect to the E-UTRAN/EPC network via a secure IPSec interface.

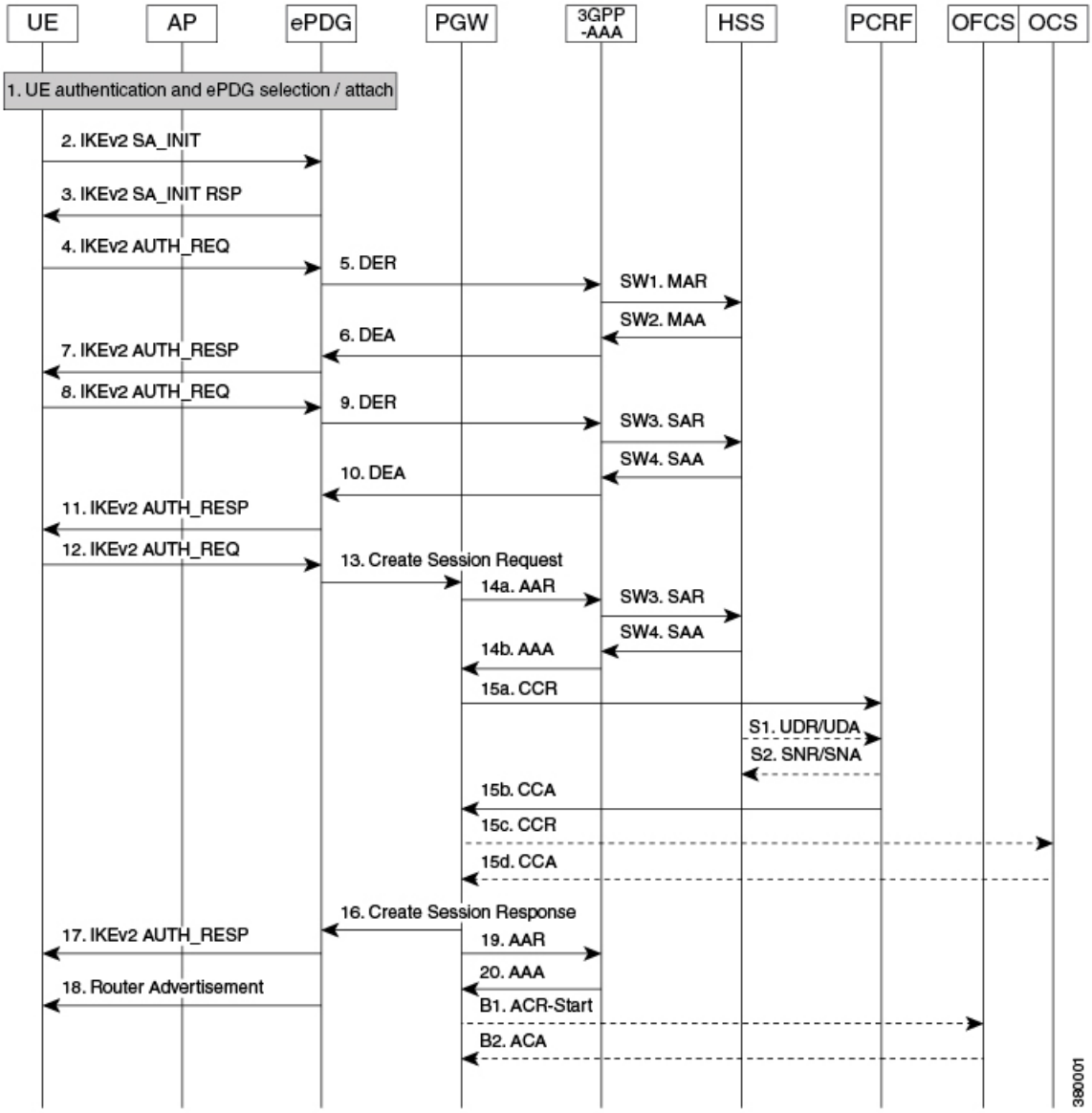
During configuration, you create the ePDG service in an ePDG context, which is a routing domain in the system. Context and service configuration for the ePDG includes the following main steps:

- **Configure the IPv4/IPv6 address for the service:** This is the IP address of the ePDG to which the WLAN UEs attempt to connect, sending IKEv2 messages to this address to establish IPSec tunnels.
- **Configure the name of the crypto template for IKEv2/IPSec:** A crypto template is used to define an IKEv2/IPSec policy. It includes IKEv2 and IPSec parameters for keepalive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per ePDG service.
- **The name of the EAP profile:** The EAP profile defines the EAP authentication method and associated parameters.

- **IKEv2 and IPSec transform sets:** Transform sets define the negotiable algorithms for IKE SAs (Security Associations) and Child SAs to enable calls to connect to the ePDG.
- **The setup timeout value:** This parameter specifies the session setup timeout timer value. The ePDG terminates a UE connection attempt if the UE does not establish a successful connection within the specified timeout period. The default value is 60 seconds.
- **Max-sessions:** This parameter sets the maximum number of subscriber sessions allowed by the ePDG service. The default value is 1,000,000 and is subject to license limitations.
- **DNS client:** DNS client configuration is needed for P-GW selection.

General Call Flow

The following section explains the basic ePDG call flows.



The UE and the ePDG exchange the first pair of messages, known as IKE_SA_INIT and RSP, in which the ePDG and UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

Table 4: General Call Flow

Step	Description
1.	The UE sends IKE_SA_INIT Message.
2.	ePDG responds with IKE_SA_INIT_RSP Message.
3.	The UE sends the user identity (in the IDi payload) and the APN information (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in TS 23.003 containing the IMSI, as defined for EAP-AKA in RFC 4187. The UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain an IPv4 home IP Address and/or a Home Agent Address. When the MAC ULI feature is enabled, the root NAI used will be of the form "0<IMSI>AP_MAC_ADDR:nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org".
4.	The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN.
5.	The 3GPP AAA Server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server shall lookup the IMSI of the authenticated user based on the received user identity (root NAI) and include the EAP-AKA as requested authentication method in the request sent to the HSS. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access. The counter of IKE SAs for that APN is stepped up. If the maximum number of IKE SAs for that APN is exceeded, the 3GPP AAA Server shall send an indication to the ePDG that established the oldest active IKE SA (it could be the same ePDG or a different one) to delete the oldest established IKE SA. The 3GPP AAA Server shall update accordingly the information of IKE SAs active for the APN. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again.
6.	The ePDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations if any. The EAP message received from the 3GPP AAA Server (EAP-Request/AKA-Challenge) is included in order to start the EAP procedure over IKEv2.
7.	The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.
8	The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server.
8a	The AAA checks, if the authentication response is correct.

Step	Description
9.	When all checks are successful, the 3GPP AAA Server sends the final Authentication and Authorization Answer (with a result code indicating success) including the relevant service authorization information, an EAP success and the key material to the ePDG. This key material shall consist of the MSK generated during the authentication process. When the SWm and SWd interfaces between ePDG and 3GPP AAA Server are implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key-AVP, as defined in RFC 4072.
10.	The MSK shall be used by the ePDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified for IKEv2 in RFC 4306. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 4306 [3], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.
11.	The EAP Success/Failure message is forwarded to the UE over IKEv2.
12	The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.
12a	The ePDG checks the correctness of the AUTH received from the UE. At this point the UE is authenticated.
13	On successful authentication the ePDG selects the P-GW based on Node Selection options.The ePDG sends Create Session Request (IMSI, [MSISDN], Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, Bearer Contexts, [Recovery], [Charging characteristics], [Additional Protocol Configuration Options (APCO)]), Private IE (P-CSCF, AP MAC address). Indication Flags shall have Dual Address Bearer Flag set if PDN Type is IPv4v6.Handover flag shall be set to Initial or Handover based on the presence of IP addresses in the IPv4/IPv6_Address configuration requests.Selection Mode shall be set to "MS or network provided APN, subscribed verified". The MSISDN, Charging characteristics, APN-AMBR and bearer QoS shall be provided on S2b interface by ePDG when these are received from AAA on SWm interface.The control plane TEID shall be per PDN connection and the user plane TEID shall be per bearer created.
14.	The P-GW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, P-GW S2b Address C-plane, PAA, APN-AMBR, [Recovery], Bearer Contexts Created, [Additional Protocol Configuration Options (APCO)], Private IE (P-CSCF)) message.
15.	The ePDG calculates the AUTH parameter which authenticates the second IKE_SA_INIT message
16.	The ePDG sends the assigned Remote IP address in the configuration payload (CFG_REPLY).The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

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

ICSR-VoLTE Support

The ePDG does supports VoLTE call marking when the dedicated bearer corresponding to the QCI configured as VoLTE is created.The VoLTE call does have special handling of allowing data during the ICSR pending standby state and during the ICSR audit phase (at new active) which helps in reducing the data outage for the VoLTE calls during planned ICSR switchover.

When sessions are created on the ePDG, there is period of 60 seconds (configurable, explained below) lag before the sessions are check-pointed to the standby chassis. If chassis failure occurs during this period, the sessions that were not check-pointed are lost. Also, in some ICSR switchovers, a large number sessions that were not check-pointed need to be flushed resulting in additional delay in the switchover. This causes significant issues for VoLTE service.

This is critical for IMS sessions. If an IMS session is not synchronized with the standby chassis and an ICSR switchover event occurs, the newly active chassis does not have any information of this session and the ePDG is out of sync with other network elements. This situation cannot be corrected until the UE registers again (max 2 hours) and VoLTE calls cannot be delivered to the UE. Therefore, it is critical to minimize the interval in which the session is not synchronized with the peer.

In maintenance mode it's required that ePDG should automatically delete the VoLTE calls when the VoLTE bearer gets teared down or subscriber becomes non-volte after deletion of all VoLTE bearers.

The "clear subs all non-volte" command allows you to clear non volte calls and "clear subs all non-volte auto-del" command is used to delete non-volte calls and mark the VoLTE calls for auto deletion when the VoLTE bearer is torn down. This helps in avoiding manual intervention from admin to cleanup calls again when VoLTE bearer is torn down and the call becomes non-VoLTE. Once the call is marked for auto-deletion it cannot be reverted.

Non VoLTE sessions data outage reduction

ePDG does allows the data for non-VoLTE calls during ICSR switchover to reduce the data-outage for non-VoLTE calls and is configuration controlled to either allow data traffic for both VoLTE and non-VoLTE calls or only VoLTE calls.

IKEv2 and IPSec Encryption

The ePDG supports IKEv2 (Internet Key Exchange version 2) and IPSec (IP Security) ESP (Encapsulating Security Payload) encryption as per RFCs 4303 and 5996. IKEv2 and IPSec encryption enables network domain security for all IP packet-switched networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are ensured through use of cryptographic techniques.

The data path from the ePDG supports mixed inner IPv4 and IPv6 addresses in the same Child SA for ESP (Encapsulating Security Payload) encapsulation and decapsulation when the Any option is configured in the payload, regardless of the IP version of the outer protocol.

Supported Algorithms

Table 5: Supported Algorithms

Protocol	Type	Supported Options
Internet Key Exchange version 2	IKEv2 Encryption	DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256
	IKEv2 Pseudo Random Function	PRF-HMAC-SHA1, SHA2-256, SHA2-384, SHA2-512, PRF-HMAC-MD5, AES-XCBC-PRF-128
	IKEv2 Integrity	HMAC-SHA1-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192. HMAC-SHA2-512-256, HMAC-MD5-96, AES-XCBC-96
	IKEv2 Diffie-Hellman Group	Group 1 (768-bit), Group 2 (1024-bit), Group 5 (1536-bit), Group 14 (2048-bit)
IP Security	IPSec Encapsulating Security Payload Encryption	NULL, DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256, AES-128-GCM-128, AES-128-GCM-64, AES-128-GCM-96, AES-256-GCM-128, AES-256-GCM-64, AES-256-GCM-96 **Note** AES-GCM algorithms are supported only on VPC-DI and VPC-SI Platform.
	Extended Sequence Number	Value of 0 or off is supported (ESN itself is not supported)
	IPSec Integrity	NULL, HMAC-SHA1-96, HMAC-MD5-96, AES-XCBC-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 **Important** HMAC-SHA2-384-192 and HMAC-SHA2-512-256 are not supported on vPC-DI and vPC-SI platforms if the hardware doesn't have crypto hardware.

x.509 Digital Certificate Handling

A digital certificate is an electronic credit card that establishes a subscriber's credentials when doing business or other transactions on the Internet. The digital certificates used by the ePDG conform to ITU-T standard X.509 for a PKI (Public Key Infrastructure) and PMI (Privilege Management Infrastructure). X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

The ePDG is capable of authenticating itself to the UE using certificates and does so in the response to the first IKE_AUTH Request message from the UE.

ePDG also supports hash and URL based encoding of certificate payloads in IKE exchanges.

The ePDG generates an SNMP notification when the certificate is within 30 days of expiration and approximately once a day until a new certificate is provided. Operators need to generate a new certificate and then configure the new certificate using the system's CLI. The certificate is then used for all new sessions.

Timers

The ePDG includes the following timers for IPSec tunnels:

- **IKE Session Setup Timer:** This timer ensures that an IKE session set up is completed within a configured period. The ePDG tears down the call if it is still in progress when the timer expires. The default value is 120 seconds, and the range is between 1 and 3600 seconds.
- **IKEv2 and IPSec SA Lifetime Timers:** The ePDG maintains separate SA lifetime timers for both IKEv2 SAs and IPSec SAs. All timers are started when an SA is successfully set up. If there is traffic through the SA, the ePDG may initiate rekeying. If there is no traffic and rekey keepalive is not required, the ePDG deletes the SA without rekeying. If there is no traffic and rekey keepalive is required, the ePDG attempts to rekey. The default value of the IKEv2 SA lifetime timer is 86400 seconds and the range is between 60 and 86400 seconds. The default value of the IPSec SA lifetime timer is 86400 seconds and the range is between 60 and 86400 seconds.
- **DPD Timers:** By default, DPD (Dead Peer Detection) is disabled. When enabled, the ePDG may initiate DPD via IKEv2 keepalive messages to check the liveliness of the WLAN UEs. The default value of the DPD timers is 3600 seconds and the range is between 10 and 3600 seconds. The default DPD retry interval is 10 seconds, and the range is between 10 and 3600 seconds. The default number of DPD retries is 2, and the range is between 1 and 100. The ePDG always responds to DPD checks from the UEs.

IKEv2 Fragmentation Support

The IKEv2 Fragmentation feature enables IPSec to fragment large messages at IKEv2 and replace them with a series of smaller messages as defined in RFC 7383. This ensures that fragmentation does not occur at IP level and fragmented packets are not dropped.

For more information on this feature, refer the IKEv2 Fragmentation chapter in the IPSec Reference guide.

IKEv2 Mobility and Multi-homing Protocol

The IKEv2 Mobility and Multi-homing protocol (MOBIKE) is supported on ePDG/IPSec as defined in RFC 4555. MOBIKE allows the IP addresses associated with IKEv2 and tunnel mode IPSec Security Associations (SA) to change. This enables peer hosts to change its point of network attachment and use different interfaces without removing the existing IPSec tunnel.

Note MOBIKE feature is supported only on ASR5500 and Ultra Services platforms.

For more information on this feature, refer the *IKEv2 Mobility and Multi-homing Protocol* chapter in the *IPSec Reference guide*.

IKEv2 RFC 5996 Support

StarOS IKEv2 stack complies to RFC 4306 and is enhanced to comply with newer version of IKEV2 RFC 5996. As part of new version support below features are introduced:

- **New notification payloads:**RFC 5996 introduces two new notification payloads TEMPORARY_FAILURE and CHILD_SA_NOT_FOUND using which certain conditions of the sender can be notified to the receiver.
- **Exchange collisions:** ePDG supports collision handling mechanism as defined in RFC 5996, it makes use of the new notify payloads in RFC5996 to do the same. Collision handling can be enabled using CLI, by default. Collision handling is supported as specified in RFC 4306/4718.
- **Integrity with combined mode ciphers:**StarOS IPSec is enhanced to graciously handle SA payloads containing combined mode cipher. In case an SA payload contains matching payload along with combined mode cipher, the one with combined mode cipher is ignored. Otherwise no proposal chosen is sent.
- **Negotiation parameters in CHILDSA REKEY:** Negotiation parameters in CHILDSA REKEY: According to RFC 5996 on rekeying of a CHILD SA, the traffic selectors and algorithms match the ones negotiated during the setting up of child SA. StarOS IKEv2 is enhanced to not send any new parameters in CREATE_CHILD_SA for a childsa being rekeyed. However StarOS IKEv2 does not enforce any restrictions on the peer for the same; this is done to minimize impact on IOT's with existing peer vendor products, which may not be compliant to RFC 5996.
- **NAT traversal:**The Crypto engine accepts inbound udp-encapsulated IPSec ESP packets even if IKEv2 did not detect NATT. Inbound packets with udp_encap are accepted for processing.
- **Certificates:**RFC 5996 mandates configurability for sending and receiving HTTP method for hash-and-URL lookup with CERT/CERTREQ payloads. If configured and if peer requests for CERT using encoding type as "Hash and URL of X.509 certificate" and send HTTP_CERT_LOOKUP_SUPPORTED using notify payload in the first IKE_AUTH, ASR shall send the URL in the CERT payload instead of sending the entire certificate in the payload. If not configured and CERTREQ is received with encoding type as "hash and URL for X.509 certificate". ASR should respond with entire certificate even if peer had sent HTTP_CERT_LOOKUP_SUPPORTED.

IMEI Validation Failure

If invalid IMEI was received from the UE in CFG payload of the first IKE_AUTH request, multiple SessMgr restart was observed. Graceful handling support is added to avoid SessMgr restart.

- The **sess-disconnect-invalid-imei** bulk statistic is added in the ePDG schema to indicate the total number of sessions disconnected due to Invalid IMEI received from the UE.
- The **Invalid IMEI** field is added to the output of the **show epdg-service statistics** command to indicate the total number of sessions disconnected due to Invalid IMEI received from the UE.

Inter-access Handover Support

The ePDG supports inter-access handovers between two different interfaces, such as a handover between a 3GPP network and an untrusted non-3GPP IP access network, or between two untrusted non-3GPP IP access networks.

When a UE sends an IKE_AUTH Request message with a NULL IPv4/IPv6 address in the CP payload, the ePDG determines that the request is for an initial attach. When a message contains non-null IP address values, the ePDG determines that the request is for a handover attach. On the SWu interface, the UE populates the

INTERNAL_IP4_ADDRESS and/or INTERNAL_IP6_ADDRESS parameter with the previously-assigned IP addresses to indicate that UE supports IP address preservation for handovers.

In case the protocol used on S2b is PMIPv6, per 3GPP TS 29.275, the ePDG indicates an inter-access handover in the S2b Handoff Indicator option of PBU (Proxy-MIP Binding Update) messages. Per RFC 5213, the ePDG indicates the RAT (Radio Access Technology) of untrusted non-3GPP access network in the Access Technology Type option.

In case the protocol used on S2b is GTPv2 then per 3GPP TS 29.274, the ePDG indicates an inter-access handover in the indication flags IE.

Interchassis Session Recovery (ICSR) Support

The ePDG supports Interchassis Session Recovery (ICSR) with fault detection and automatic switch over. The subscriber session details for all ePDG interfaces are replicated in stand by, In case of a switchover, the new chassis processes all subsequent control and data traffic for the subscriber session.

Important Interchassis Session Recovery is supported only on Cisco ASR 5500.

The SWu, SWm and S2b interface are not impacted by the switchovers.

ePDG release 18.0 supports upgrade/down grade from release 18 (N) to 16 (N-2).

Important For more information on ICSR, see the *System Administration Guide.*

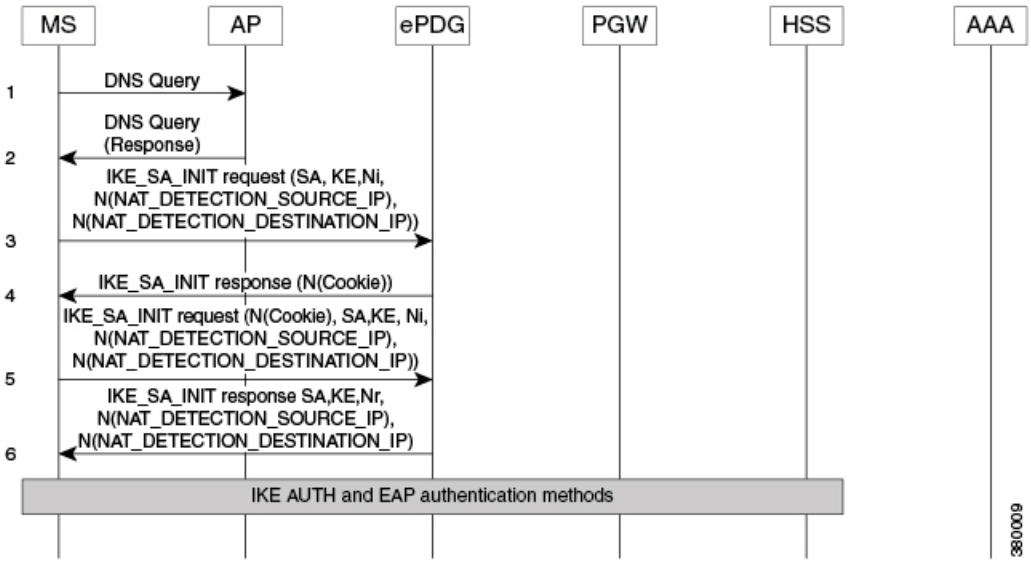
IPSec Cookie Threshold

The ePDG supports IKEv2 Cookie challenge payload, this feature helps protect against opening too many half opened IPSec sessions.

The IKEv2 Cookie feature when enabled will invoke a cookie challenge payload mechanism which ensures that only legitimate subscribers are initiating the IKEv2 tunnel request and not a spoofed attack. Note that this configuration is per ipsecmgr.

The Cookie Challenge mechanism is disabled by default, the number of half open connections over which cookie challenge gets activated is also configurable.

Figure 9: IPSec Cookie Threshold



IPSec Large Support

The IPSec Large feature boosts IPSec crypto performance by enabling the resource manager (RM) task to assign additional IPSec managers to packet processing cards that have sufficient processing capacity. The system can be configured to achieve a higher per SF scale by configuring the **[no] require ipsec-large** command. This configuration is effective during init time only, and system resources are adjusted accordingly for more number of ePDG sessions or IPSec tunnel establishments.

Important When IPSec large and demux on MIO are configured together, enable the IPSec large feature (using the **require ipsec-large** command) before enabling the demux on MIO (using the **require demux management-card** command).

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the System Administration Guide for your deployment.

IPv6 Capabilities

IPv6 addressing enables increased address efficiency and relieves pressures caused by the rapidly approaching IPv4 address exhaustion problem.

The ePDG offers the following IPv6 capabilities:

- Support for any combination of IPv4, IPv6, or dual stack IPv4/v6 address assignment from address pools on the P-GW.
- Support for native IPv6 transport and service addresses on the PMIPv6/GTPv2 S2b interface with the P-GW.

IPv6 transport is supported on the SWm Diameter AAA interface with the external 3GPP AAA server. Note that the ePDG supports IPv6 transport for the UE-ePDG tunnel endpoints on the SWu interface.

IPv6 Router Advertisement Support

The ePDG provides router advertisement support for IPv6 and dual stack PDNs to allow the WLAN UEs to initialize the IPv6 protocol stack. The ePDG sends an unsolicited router advertisement to the UE for an IPv6 PDN connection after sending the final IKE_AUTH Response message. When the ePDG receives a Router Solicitation Request message from the UE, the ePDG intercepts the message and responds to it. This is needed for some UEs that perform address auto-configuration despite receiving the IP address information through the CP payload of the IKE_AUTH Response message.

IPv6 Support on IPSec SWU Interface

When a UE attaches to a WiFi Access Point, the WiFi Access Point always assigns the UE an IPv4 Address. With the IPv6 Support on IPSec SWU Interface feature the UE provides an IPv4 or IPv6 address by the WiFi Access Point for initiating the IPsec connection to the ePDG over IPv4/IPv6 transport accordingly. For IPv6 transport the IPv6 UDP checksum is mandatory and is supported for IKEv2 establishment.

The ePDG now supports incoming IKEv2 requests from UE over an IPv6 transport as well. One epdg-service can now bound to one IPv4 and IPv6 address which acts as IPsec tunnel endpoint addresses. ePDG continues to support the inner IPv4, IPv6 and IPv4v6 traffic in both IPv4 and IPv6 outer IP SWu transport.

IPv6 NAT support is not standardized and there is no requirement to support the IPv6 NAT. If at all NAT related parameters are present in the crypto template during configuration , it should not have any impact on the tunnel setup and the data flow.

Lawful Intercept

Lawful Intercept (LI) is needed to perform electronic surveillance on an individual (a target/subject) as authorized by a judicial or administrative order. There are two types of intercept information that can be reported, Intercept Related Information (IRI) and Content of Communication (CC). The LI can be provisioned on ePDG based on user's IP-Addr, MSISDN, IMSI, NAI or IMEI (IMEI from rel 21.1).

For more information on ePDG's support for LI, refer the LI Configuration Guide.

Local PGW Resolution Support

For PGW selection, ePDG uses PGW address provided by AAA or uses DNS resolution. With local PGW resolution support, PGW address can be configured locally. If the above two methods (static and dynamic) PGW selection fails, or if PGW address were available but not reachable, then only locally configured addresses are referred and used. Also, if there is no PGW address received from AAA or, if no DNS setup is present, then also locally configured PGW addresses are referred. This way the existing functionality of PGW selection is retained, and added an additional backup-mode with local PGW address configuration resolution.

A new CLI is introduced in *ePDG Service Config* mode where epdg-service is associated with "subscriber-map", which is also an indication that "Local PGW Resolution Support" is enabled for epdg-service. The local PGW resolution will take into effect only if the CLI is configured and none of the existing method of PGW resolution method results in session creation.

Below are the Local PGW Resolution Support scenarios:

- PGW address received from AAA, but unreachable
- PGW addresses received by DNS resolution, but all are unreachable
- DNS server is not reachable, or rejects the DNS query
- None of the PGW selection mechanisms(Static/Dynamic) are present, i.e. neither DNS resolution is configured, nor AAA sends any PGW addres

  s

In all of the above scenarios, if local PGW address is configured and ePDG-Service is associated with Subscriber-Map, then PGW address is selected based on weight. In this algorithm the sessions are created approximately in the same ratio of the weights configured with the PGW addresses. For example if the weights are 10, 20 and 30, then 1000 sessions will be distributed in ration 1:2:3 respectively. (same algorithm used as DNS resolution based PGW selection mechanism.)

Only first PGW is selected based on weight based selection algorithm and if the call does not gets established with this selected PGW, rest of the addresses are selected on Round Robin method starting from next available PGW configured rounding upto PGW address configured just before the PGW address selected based on weight. This way none of the addresses are repeated. For example if ten PGW address are configured, based

on weight 7th one is selected as first address, and if it is unreachable then address at 8th index is selected, then 9th, 10th, 1st, 2nd and so on until address present at 6th index.

In a case where PGW resolution is enabled and the existing DNS/AAA server PGW resolution mechanism failed and there is no disconnect reason already set from previous mechanism, further the local PGW resolution failed due to configuration error then new disconnect reason shall be set "ePDG-local-pgw-resolution-failed" for identifying the case.

Also in the case of HO, even if the local PGW resolution is enabled and there is no or unreachable PGW address provided by AAA server, or PGW FQDN provided results in no or unreachable PGW address, then ePDG will not use local PGW resolution mechanism for establishing the call.

Local configuration as preferred PGW selection mechanism

The ePDG is further enhanced to support local configuration based PGW selection as the preferred method for PGW node selection.

The ePDG service should be configured indicating preferred method of PGW selection, whether local configuration or DNS/AAA server based PGW selection. Local Configuration based PGW selection as fallback mechanism is default configuration behavior.

This preferred PGW selection mechanism feature provides more control and flexibility to customer for routing/load balancing the sessions on desired PGW.

The feature shall be applicable only for initial attach and for Hand-Off calls ePDG shall use the PGW address provided by AAA server even if the feature is enabled as the PGW selected by local configuration may be different from one have the session on LTE.

Maximum IPSec Managers Supported per Card in vPC

The number of IPSec managers per card has been increased to 48 from 22 subject to availability of hardware resources such as vCPU and RAM. Customers can utilize more hardware resources to enhance capacity and performance.

Mobile Access Gateway Function

The ePDG hosts a MAG (Mobile Access Gateway) function, which acts as a proxy mobility agent in the E-UTRAN/EPC network and uses Proxy Mobile IPv6 signaling to provide network-based mobility management on behalf of the UEs attached to the network. The P-GW also uses Proxy Mobile IPv6 signaling to host an LMA (Local Mobility Anchor) function to provide network-based mobility management. With this approach, the attached UEs are no longer involved in the exchange of signaling messages for mobility.

The MAG function on the ePDG and the LMA function on the P-GW maintain a single shared tunnel. To distinguish between individual subscriber sessions, separate GRE keys are allocated in the PBU (Proxy-MIP Binding Update) and PBA (Proxy-MIP Binding Acknowledgement) messages between the ePDG and the P-GW. If the Proxy Mobile IP signaling contains PCOs (Protocol Configuration Options), it can also be used to transfer P-CSCF or DNS addresses.

The S2b interface uses IPv6 for both control and data. During PDN connection establishment, the P-GW uses Proxy Mobile IPv6 signaling to allocate the IPv6 HNP (Home Network Prefix) to the ePDG, and the ePDG returns the HNP to the UE in an IPv6 router advertisement.

Note that the MAG function on the ePDG does not support multiple PDN connections for the same APN and UE combination. The ePDG establishes each subsequent connection from the same UE to the same APN via a new session and deletes the previous session before the new session gets established.

Multiple PDN Support

The multiple PDN feature enables the WLAN UEs to simultaneously establish multiple PDN connections towards the P-GW. Each PDN connection has a separate IKE tunnel established between the UE and the ePDG.

Note that the ePDG supports multiple PDN connections to different APNs only and multiple PDN connections from the same UE to the same APN are not allowed. The ePDG establishes each subsequent connection from the same UE to the same APN via a new session and deletes the previous session before the new session gets established. These new PDN connections use different IPSec/PMIPv6/GTPv2 tunnels.

To request a new session, the UE sends the APN information (in the IDr payload) along with the user identity (in the IDi payload) in this first IKE_AUTH Request message, and begins negotiation of Child SAs. The ePDG sends the new APN information in the Service Selection Mobility Option towards the P-GW, which treats each MN-ID+APN combination as a separate binding and allocates a new IP address/prefix for each new binding.

In case of S2b protocol being used as GTPv2 IMSI + APN is used for identifying the unique session.

Narrowing Traffic Selectors

During traffic selector negotiation, ePDG by default responds with wildcard IP address, even if the UE is requesting specific range in the TSr. The ePDG should allow to use specific sets of TSs to send traffic to specific sets of address ranges for specific client policies. The ePDG also should respect the range requested by UE and it should (according to the IKEv2 spec) be able to narrow down the UE's request.

IKE Responder performs narrowing As per RFC5996 as shown below:

1. If the responder's policy does not allow it to accept any part of the proposed Traffic Selectors, it responds with a TS_UNACCEPTABLE Notify message.
2. If the responder's policy allows the entire set of traffic covered by TSi and TSr, no narrowing is necessary, and the responder can return the same TSi and TSr values.
3. If the responder's policy allows it to accept the first selector of TSi and TSr, then the responder MUST narrow the Traffic Selectors to a subset that includes the initiator's first choices.
4. If the responder's policy does not allow it to accept the first selector of TSi and TSr, the responder narrows to an acceptable subset of TSi and TSr.

All these 4 cases will be supported with the exception that at any point of time maximum of four traffic selector per protocol (combination of IPv4 and/or IPv6) will be supported in a single CHILD SA.

When narrowing is done, if there are several subsets are acceptable, GW will respond back with first 4 acceptable subsets and it will not support ADDITIONAL_TS_POSSIBLE notification.

.

Non-MCDMA Cores for Crypto Processing

The cores in the VPC-DI/VPC-SI platforms are used for crypto processing to limit the throughput while using software path for encryption/decryption. The SA index will be used to distribute the sessions across all

non-MCDMA cores present in the system for crypto processing. The performance will be proportionally improved with the number of non-MCDMA IFTASK cores present in the system.

In releases prior to 21.8, the core allocation for a particular SA was done based on its IPSec policy number and distributed among four or lesser number of cores for crypto processing.

The following configuration is added to limit the number of cores to be used for crypto.

IFTASK_MAX_CRYPTO_CORES=<percentage>

By default, all non-MCDMA cores will be used. The value is configured in percentage of the maximum number of IFTASK cores present in the system. This configuration is added in the */boot1/param.cfg* file under the debug shell of each SF before reload.

Non UICC Device Support Using Certificate Based Authentication

ePDG is enhanced to support the non UICC devices connectivity to EPC via ePDG using certificate based UE authentication following authorization by AAA server.

ePDG already supports UICC devices connectivity using EAP-AKA based device authentication. However as non UICC devices cannot do EAP-AKA based authentication, alternate method of using certificates is used.

ePDG supports the X.509 certificate based authentication and also communicates with OCSP (Online Certificate Status Protocol) server for completing the authentication. Once the authentication is done ePDG communicates with AAA server for ensuring the authorization of the device.

As non UICC devices do not have IMSI, customized vIMSI in format similar to UICC IMSI uniquely identifying the non UICC device needs to be shared by the device. The device IMSI is shared as part of peer (device) certificate to ePDG. ePDG extracts serial number, issuing authority and OCSP responder address details from the certificate and communicates with OCSP responder. In case the OCSP responder detail is absent in the certificate the ePDG configuration is used for extracting the same. The OCSP client (ePDG) to the OCSP responder interaction will be over HTTP. A TCP socket connection will be established to the OCSP responder. OCSP responder communicates with the associated CA (certification authority) and gets the certificate revocation status which can be "good" or "revoked" or "unknown". The ePDG behavior in case of "unknown" is similar to "revoked". When the OCSP response reaches ePDG, it validates if the response is received from genuine entity and post validation checks the certificate status. If the certificate status is good then proceeds with device authorization.

ePDG expects the SUBJECT/CN field of UE certificate to contain the IMSI or NAI and detects that its NAI with presence of " else its IMSI. This extracted CN fields is accordingly verified with the IDi payload received from UE in IKE_AUTH_REQ message. The certificate identity is more reliable and also the IKE_AUTH_REQ identity does have significance is AUTH payload verification hence this functionality of comparison is in place. ePDG sends the NAI identity as received in the IKE_AUTH_REQ message to the AAA server and once AAA server sends back the authorization success then ePDG does PGW selection and communicates with PGW over S2b interface to establish the call.

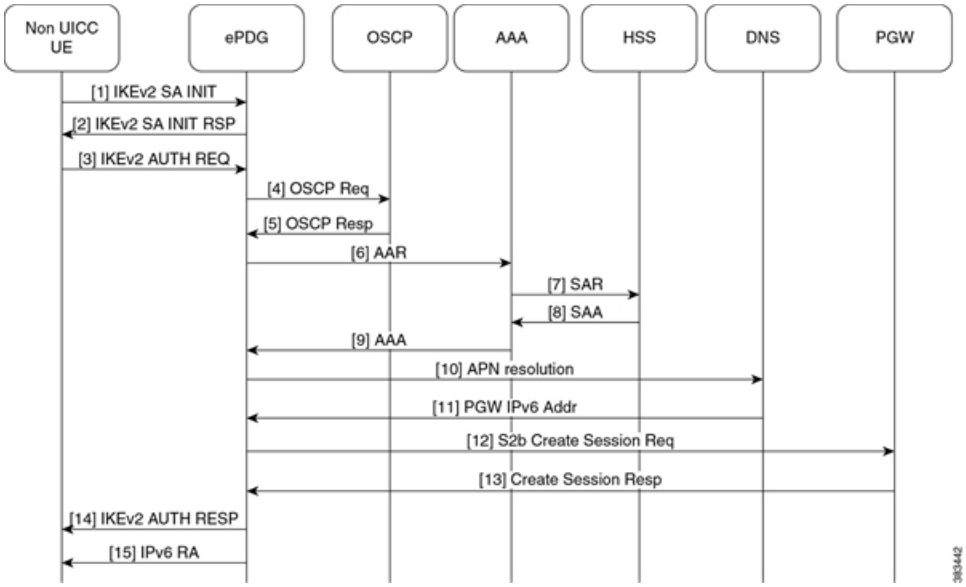
IPsec subsystem does comply with RFC 2560 and uses open SSL 0.9.7 for certificate based authentication, therefore ePDG inherently complies with same.

ePDG supports both UICC and non-UICC devices simultaneously for same ePDG service. ePDG service does have single crypto template association with the service IP address and hence IPsec subsystem is enhanced for supporting the multiple authentication methods per crypto template. ePDG identifies whether certificate based authentication needs to be used or not by the presence of AUTH payload. If the AUTH parameter is absent in initial IKE_AUTH_REQ message it indicates that EAP-AKA based authentication is to be used. If

the AUTH payload is present and the CERT payload is also present it indicates certificate based mechanism is to be used.

OCSP communication is optional and if not configured then ePDG validates based on the configured CA certificates.

Figure 10: NON UICC device Call flow



1. UE ePDG: IKEv2 SA_INIT UE sends IKE_SA_INIT Request (SA, KE, Ni, NAT-DETECTION Notify).
2. ePDG UE: IKEv2 SA_INIT RSP The ePDG responds with an IKE_SA_INIT Response (SA, KE, Nr payloads, NAT-Detection Notify, [CERTREQ]).
3. UE ePDG: IKEv2 AUTH_REQ UE sends IKE_AUTH_REQ (IDi, AUTH, CERT, [CERTREQ], IDr, SA, CP (CFG_REQUEST (INTERNAL_IP6_ADDRESS, [INTERNAL_IP6_DNS], [INTERNAL_IP6_PCSCF]), TSi, TSr)). The UE does include AUTH and CERT payload to indicate that it will use the certificates (X.509) for authenticating itself. Presence of AUTH payload indicates EAP-AKA is not used. IDi contains the NAI and IDr does contain the APN name. Root NAI is of format X<IMSI> nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org so IMSI (virtual IMSI used for non UICC device IMSI) is required which should be of decimal digit UICC IMSI format. One proposed approach is to use <device prefix><MSISDN> where MSISDN is common for the associated non UICC and UICC devices but its operator decision and ePDG shall be able to handle it until its unique per non UICC device and is in UICC IMSI format. The certificate SUBJECT/CN field shall be containing the IMSI or NAI as it's identifier. ePDG uses received public key as part of certificates for authenticating the UE. OCSP shall be used for checking the revocation status during the certificates based device authentication. OCSP communication is optional means if the OCSP responder is absent in operator infrastructure then the ePDG shall be authenticating the device using the configured Root CA certificate.**Note** :The device can share the certificates (X.509) or can communicate the URL to ePDG for downloading the device certificates. Both the mechanism are supported on ePDG.
4. ePDG OCSP responder : OCSP request ePDG sends the OCSP request containing the certificate identifier.
5. OCSP responder ePDG :OCSP Response OCSP responder checks and returns back the revocation status of the certificate. At this stage ePDG completes the authentication of the device.
6. ePDG AAA server :AAR The ePDG sends the AA-Request (Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, Auth-Request-Type

(AUTHORIZE_AUTHENTICATE), User-Name (NAI)) message to the 3GPP AAA server. ePDG communicates the NAI for AAA to check UE identity and authorize the same.

7. AAA server HSS :SAR The 3GPP AAA updates the HSS with the 3GPP AAA Server Address information for the user. The AAA sends Server-Assignment-Request (Session-Id, Auth-Session-State (NO_STATE_MAINTAINED), Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, User-Name (IMSI-NAI), Server-Assignment-Type (REGISTRATION)). **Note** :As this call flow is not defined in 3GPP yet so the proposed message between AAA to HSS is to be decided by AAA and HSS vendors however based on existing SWx interface messages have proposed the usage of SAR.
8. HSS AAA server :SAA The HSS sends Server-Assignment-Answer (Session-Id, Result-Code, Experimental-Result (Vendor-Id, Experimental-Result-Code), Non-3GPP-User-Data {Subscription-ID (END_USER_E164, MSISDN), Non-3GPP-IP-Access (NON_3GPP_SUBSCRIPTION_ALLOWED), Non-3GPP-IP-Access-APN (Non_3GPP_APNS_ENABLE), APN-Configuration , ANID (WLAN)}, APN-OI-Replacement, APN-Configuration})
9. AAA server ePDG: AA-Answer The 3GPP AAA Server responds with AAA (Session-Id, Auth-Application-Id, Auth-Request-Type, Origin-Host, Origin-Realm, Result-Code, User-Name, APN-Configuration, 3GPP-Charging-Characteristics, Subscription-ID)
10. ePDG DNS server: DNS(NAPTR/AAAA) query ePDG sends DNS query to DNS server with APN/PGW FQDN for PGW resolution.
11. DNS server ePDG:DNS query response DNS server returns the PGW address to ePDG as part of DNS AAAA/A response.
12. ePDG PGW: S2b Create Session Req ePDG selects PGW based on DNS mechanism using APN/PGW FQDN. The ePDG sends Create Session Request (IMSI, [MSISDN],Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, [APCO], Bearer Contexts(), [Recovery], [Private IE (P-CSCF)]). Selection Mode shall be set to "MS or network provided APN subscribed verified". Private IE is populated if the UE request P-CSCF addresses. The PGW performs the necessary interactions with 3GPP-AAA, PCRF and OCS/OFCS.
13. PGW ePDG: Create Session Resp The PGW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, PGW S2b F-TEID, PAA, [APN-AMBR],[APCO],Bearer Contexts Created (EPS Bearer ID, Cause, [TFT], S2b-U PGW F-TEID, Bearer Level QoS), [Recovery], [Private IE (P-CSCF)]) message.
14. ePDG UE: IKEv2 AUTH_RESP ePDG sends IKE_AUTH_RESP (AUTH, IDr, [CERT (X509 CERTIFICATE SIGNATURE)], CP, SA, CFG_REPLY ([INTERNAL_IP4_ADDRESS], [INTERNAL_IP4_NETMASK], [INTERNAL_IP4_DNS], INTERNAL_IP6_ADDRESS, INTERNAL_IP6_SUBNET, INTERNAL_IP6_DNS, [P-CSCF]) TSi, TSr)
15. ePDG UE: IPv6 RA The assumption is that the IP stack needs the RA to initialize the address.

P-CSCF Request Support

To connect to the IMS core network, the WLAN UEs perform P-CSCF discovery as part of session establishment. This feature supports P-CSCF attributes in CFG_REQUEST and CFG_REPLY messages as part of the CP payload in the IKE_AUTH Request and Response messages the ePDG sends and receives from the UEs. The P-CSCF attribute can be sent on SWu as private or with standard value.

The WLAN UEs request a P-CSCF address in IKE_AUTH messages to establish IMS PDN connections. The ePDG receives the P-CSCF attribute in the CP payload (CFG_REQUEST) of the first IKE_AUTH message exchange and includes a P-CSCF Request message in the PBU (Proxy-MIP Binding Update) message to the P-GW. The ePDG sends the PBU message by framing the MIPv6 PCO VSE (Protocol Configuration Options Vendor Specific Extension) within the P-CSCF Request message to the P-GW. Once the ePDG receives the response from the PGW with the list of P-CSCF addresses, the ePDG shall include the P-CSCF addresses in the CP payload (CFG_REPLY) of the final IKE_AUTH Response message sent to the UE.

In case protocol used on S2b is GTPV2 ePDG has flexibility to use either APCO IE or Private Extension IE based on ePDG configuration. Once the ePDG receives the response from the P-GW with the list of P-CSCF addresses in the APCO / Private Extension IE, the ePDG includes the P-CSCF addresses in the CP payload (CFG_REPLY) of the final IKE_AUTH Response message sent to the UE.

On SWu interface the ePDG is able to handle the private attribute value for the P-CSCF address and this private attribute value is configurable on ePDG. By default 16384 is used for P-CSCF IPv4 address and 16390 is used for the IPv6 P-CSCF address. The values 16384-32767 are for private use among mutually consenting parties.

The P-CSCF v4 and v6 are recently assigned values by IANA so ePDG shall be supporting those values as well in addition to the private configured value. ePDG should respond to UE with same attribute value as received in the request. Private values are maintained for the devices which are already in market as they may not comply to standard values.

UE should include P-CSCF_V4_ADDR attribute only once in IKE_AUTH request and no specific P-CSCF address is included because it is a request. ePDG is enhanced to support both IPv4 and IPv6 P-CSCF address handling together. ePDG also supports maximum of 3 IPv4 and 3 IPv6 P-CSCF addresses. The exceeding P-CSCF address will be ignored. In case of invalid P-CSCF address are received the P-CSCF address is ignored and have no impact on the call establishment.

On S2b interface the P-CSCF is enhanced to support both APCO IE and private Extension IE. ePDG continues to use existing "vendor-specific-attribute" configuration present under epdg-service to decide whether to use APCO IE or private extension IE. The feature scope shall be limited to GTPv2 and shall not cover PMIPv6 as most of the customers are showing interest in GTPv2 based deployment.

Passing on UE Tunnel Endpoint Address over SWm Support

Mobile operators would like to be able to block VoWiFi calls from users while roaming. It is required that the tunnel end-point (WLC or AP) IP address to be passed on from ePDG. This is very important to the operator as it generates a huge amount of revenue from roaming calls and would like to minimize the revenue leakage from users making VoWiFi calls while roaming.

How Passing on UE tunnel Endpoint Address over SWm works

The provisioning of UE Tunnel Endpoint-IP (IKEv2 tunnel endpoint incase of NAT) to AAA server will help the operator in identifying the UE's location at AAA server. The operator uses this information to control the access or to decide the UE connections. For example, Operator can lookup the GeoIP database (GeoDB) against the UE tunnel endpoint IP to identify the country from where the UE is connecting from. Based on this information operator can allow the call or reject it(using auth-failure) according to the policy configured. Lets say the policy dictates that the VoWiFi calls are allowed only for UEs connecting from home country but not allowed while roaming outside the country, they can save the revenue leakage using this information.

The value will be sent in UE-Local-IP-Address AVP(IPv4/IPv6) in all the DER messages to AAA server in SWm interface. The AVP is sent as part of standard SWm dictionary (aaa-custom16). In case of AAA server rejects the call based on the tunnel endpoint IP, ePDG will send AUTHENTICATION_FAILED/24 as NOTIFY error message in IKEv2 message to communicate the same to UE.

This feature is supported for EAP based authentication mechanism and not for non UICC deployment using certificate based device authentication.

Passing on IMEI to AAA for EIR Support on WiFi

ePDG receives the IMEI information from the UE over SWu interface and communicates the same to AAA server over the SWm interface.

The IMEI information is communicated to ePDG from UE as part of the CFG_REQUEST payload of the IKE_AUTH_REQ message. A new private attribute is added for the UE to communicate the IMEI information to ePDG. Also ePDG encodes and sends the received IMEI as Terminal Information AVP on the SWm interface.

ePDG is configured to have the private attribute value as configurable for the IMEI which gives the operator the flexibility of choosing the private attribute value for its deployment.

Important Refer *User Equipment Identity in IKE_Auth Message* feature for 3GPP defined passing on IMEI to the AAA server in the Diameter EAP Request (DER) message over the SWm interface.

Configuring Passing on IMEI to AAA for EIR Support on WiFi

Use the **pgw-address** command under the APN Profile Configuration Mode to define local P-GW addresses for load balancing.

```
configure
    context context_name
       crypto template template_name ikev2-vendor
       configuration-payload private-attribute-type imei imei_value
         end
```

- Use the **crypto template** *template_name* command to disable the P-GW address(es) configured for an APN profile.
- Use the **ikev2-vendor** command to disable the P-GW address(es) configured for an APN profile.
- Use the **configuration-payload** command to configure mapping of the configuration payload attributes.
- Use the **private-attribute-type** command to define the private payload attribute.
- Use the **imei** *imei_value* command to define IMEI payload attribute value. This is an integer value from 16384 to 32767. The default value is 16391.
- When multiple P-GW addresses are configured, only the first P-GW will be selected based on the weight. The rest of the P-GW addresses are selected using the round-robin mechanism

S2b GTPv2 support

ePDG supports PDN connection, session establishment and release, along with support for dedicated bearer creation, deletion and modification that is initiated by the P-GW.

During the initial attachment, the ePDG "default EPS QOS", and "APN-AMBR" values are populated in the create session request based on the values received from the SWm interface. If these values are missing in the messages received on the SWm interface, ePDG encodes the mandatory or conditional IE with the values set to zero.

When a new PDN connection is established, ePDG allocates and sends a default EPS bearer ID to the PDN gateway. After the initial attach, a default bearer is created for the session, and the IP address is allocated and communicated to the UE.

A GTP-C and GTP-U tunnel is successfully established between the ePDG and P-GW, and an IPSec tunnel is established between the UE and ePDG. Traffic is allowed to flow between these established tunnels.

ePDG sends a "delete session request" message to P-GW, and handles the corresponding "delete session response" message from the P-GW during the following scenarios:

- UE/ePDG initiated detach with GTP on S2b
- UE requested PDN disconnection with GTP on S2b
- AAA initiated detach with GTP on S2b

ePDG handles the received "create bearer request" message and sends a "create bearer response" message for the dedicated bearer creation triggered from the P-GW.

After the dedicated bearer is created, a new GTP-U tunnel is established between ePDG and P-GW, and traffic mapping to the TFT of this bearer occurs. ePDG supports up to 16 packet filters per bearer.

ePDG also stores mapping information between the uplink packet filters received from the P-GW (For example; in the Create Bearer Request message), and the corresponding S2b bearer. ePDG matches these filters and decides if the uplink packets should be allowed or dropped.

ePDG receives the "delete bearer request" message and sends a "delete bearer response" message for the dedicated bearer deletion triggered by the P-GW.

ePDG clears the bearer path (GTP-U tunnel) corresponding to the EBI received. In the case of a linked EBI, the PDN connection and its associated bearers are deleted. The TFT mapping for the deleted bearer is also deleted.

ePDG handles the received "update bearer request" message and sends a "update bearer response" message for dedicated bearer modification triggered from the P-GW. ePDG updates the UL TFT mapping for the associated bearer using the "bearer context" information.

ePDG supports path failure detection for control plane by using Echo Request and Echo Response messages. A peer's IP address-specific counter is reset every time an Echo Response message is received from the peer's IP address. The counter is incremented when the T3-RESPONSE timer expires for an Echo Request message sent to the peer's IP address. The path is considered as down if the counter exceeds the value of N3-REQUESTS.

ePDG initiates the Echo requests once retransmission timeout occurs for the request sent to the P-GW. The retransmission for GTP messages is handled by running the retransmission timer (T3-RESPONSE) and for N3-REQUESTS timer, the message is retransmitted after the retransmission timer expires. After all the retransmissions are over, echo handling is initiated.

The GTPC configuration has the configuration command, no gtpc path-failure detection-policy <CR> using which on path failure detection, SNMP traps/alarms are generated notifying that P-GW has gone down, but the sessions are not deleted. The SNMP trap is sent only once per peer, and not for every session. When this command is not configured, path failure detection and the subsequent cleanup action is enabled by default.

Detection of path failure for user plane is supported using the Echo Request/ Echo Response messages. A path counter is reset every time an Echo Response is received and incremented when the T3-RESPONSE timer expires for any Echo Request message sent. The path is considered as down if the counter exceeds the value of N3-REQUESTS.

Note By default, path failure detection is not configured for ePDG.

Session Recovery Support

Session recovery provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system, preventing a fully connected user session from being disconnected. The ePDG supports session recovery for IPv4, IPv6, and IPv4/v6 sessions and ensures that data and control planes are re-established as they were before the recovery procedure.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior, including DNS, P-GW, and P-CSCF addresses.
- Subscriber data statistics that are required to ensure that accounting information is maintained.
- A best-effort attempt to recover various timer values, such as call duration, absolute time, and others.

Note that for the recovered sessions, the ePDG recreates counters only and not statistics.

Session recovery is also useful for in-service software patch upgrade activities. If session recovery is enabled during the software patch upgrade, it helps to preserve existing sessions on the active hardware during the upgrade process.

Important For more information on session recovery support, see the *System Administration Guide*.

Support for MAC Address of WiFi Access Points

The ePDG can propagate the MAC (Media Access Control) address of each WiFi access point to the P-GW. The ePDG sends this information using the PMIP Location AVP (Attribute-Value Pair) in the User-Location-Info Vendor Specific Option of PBU (Proxy-MIP Binding Update) messages over the S2b interface. In case the protocol used on S2b is GTPv2 then this information is communicated using the Private Extension IE in Create Session Request message.

The WLAN UEs send the MAC address of each WiFi access point to the ePDG embedded in the NAI (Network Access Identifier). When the ePDG receives an NAI that includes a MAC address, the ePDG checks the MAC address and if the validation is successful, the ePDG removes the MAC address from the NAI before sending it to the AAA server in the User-Name AVP of DER (Diameter EAP Request) messages.

Note that the ePDG can be configured to allow IPSec connection establishment without the MAC address present. If the MAC address is not present and the ePDG is configured to check for the MAC address, the ePDG fails the IKE negotiation and returns Notify payload 24 (AUTHENTICATION_FAILED).

Static and Dynamic P-GW Selection

The P-GW selection function enables the ePDG to allocate a P-GW to provide PDN connectivity to the WLAN UEs in the untrusted non-3GPP IP access network. The P-GW selection function can employ either static or dynamic selection.

Static Selection

The PDN-GW-Allocation-Type AVP indicates whether the P-GW address is statically allocated or dynamically selected by other nodes, and is considered only if MIP6-Agent-Info is present. When the PDN-GW-Allocation-Type AVP is absent or is STATIC, and an initial attach occurs, or is DYNAMIC and a handoff attach occurs, the ePDG performs static selection of the P-GW.

The figure below shows the message exchange for static selection. The table that follows the figure describes each step in the flow.

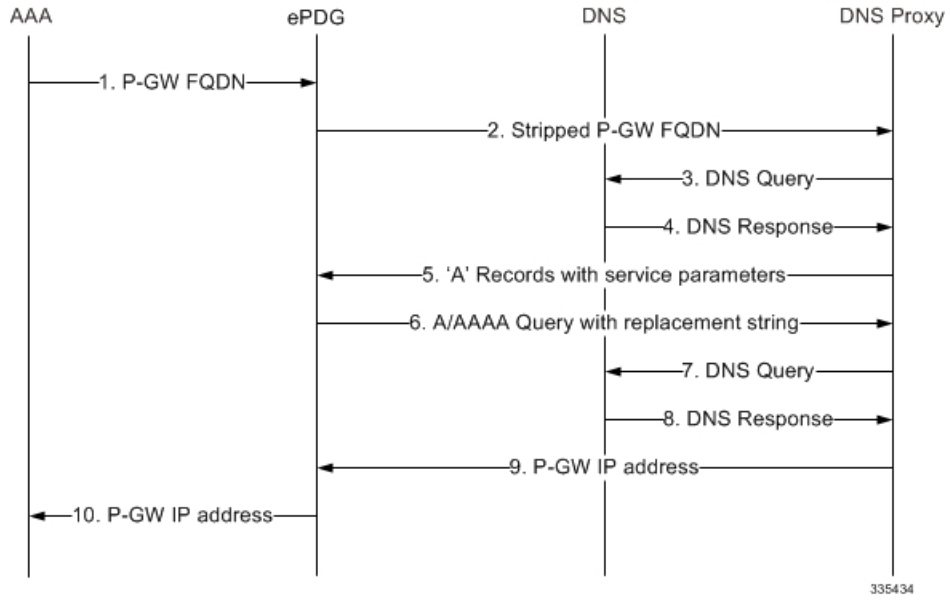


Table 6: P-GW Static Selection

Step	Description
1.	The AAA server sends the P-GW FQDN (Fully Qualified Domain Name) to the ePDG.
2.	The ePDG receives the P-GW FQDN from the AAA server as part of the MIP-Home-Agent-Host AVP in a Diameter EAP Answer message. The ePDG removes the first two labels of the received P-GW FQDN (if the FQDN starts with 'topon') to obtain the Canonical Node Name ID of the P-GW. The ePDG uses this P-GW ID to send an S-NAPTR (Server-Name Authority Pointer) query to the DNS proxy.
3.	The DNS proxy send the S-NAPTR query to the DNS.
4.	The DNS may return multiple NAPTR resource records with an 'A' flag (for an address record) with the same or different service parameters.
5.	The DNS proxy forwards the two NAPTR resource records to the ePDG.
6.	The ePDG selects the replacement string (the P-GW FQDN) that matches the service parameter if ePDG is configured as MAG for PMIPv6 protocol or service parameter 'x-3gpp-pgw:x-s2b-gtp' when ePDG is configured for GTP protocol support. The ePDG then performs an A/AAAA query with the selected replacement string (the P-GW FQDN).

Step	Description
7.	The DNS proxy send the A/AAAA query to the DNS.
8.	The DNS returns the IP address of the P-GW.
9.	The DNS proxy forwards the P-GW IP address to the ePDG.

Dynamic Selection

For a given APN, when the HSS returns Dynamic Allocation Allowed for the P-GW ID and the selection is not for a 3GPP-to-non-3GPP handover, the ePDG ignores the P-GW ID and instead performs dynamic selection.

The figure below shows the message exchange for dynamic selection. The table that follows the figure describes each step in the flow.

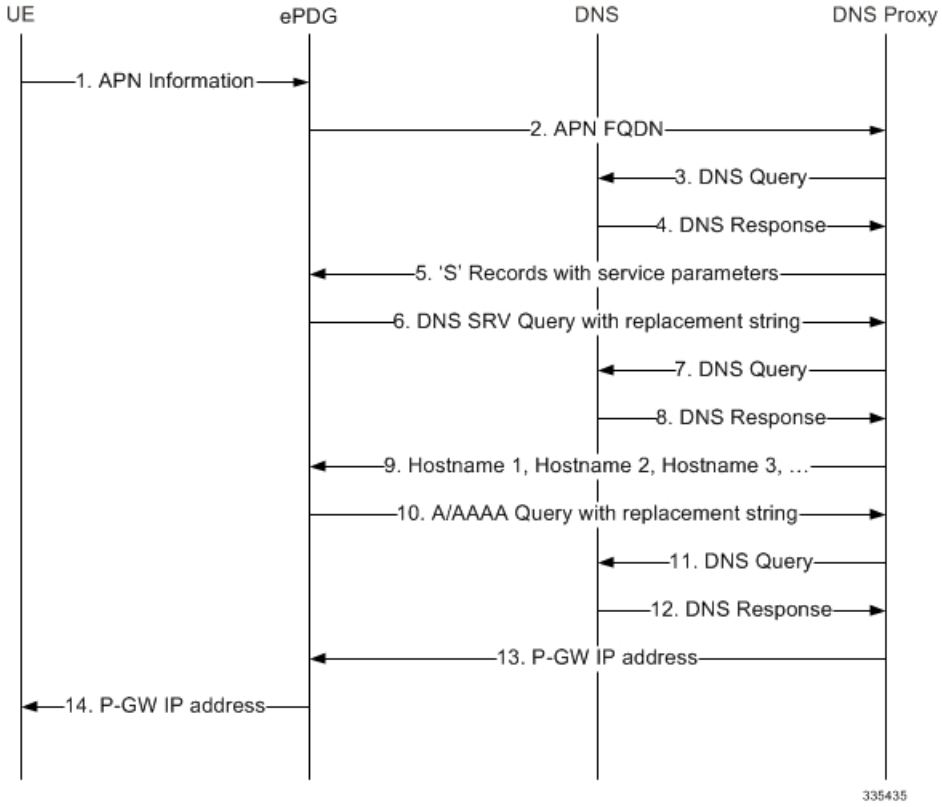


Table 7: P-GW Dynamic Selection 4

Step	Description
1.	The WLAN UE sends the APN name to the ePDG.
2.	The ePDG constructs the APN FQDN from the received APN name. The ePDG uses this query string to send an S-NAPTR (Server-Name Authority Pointer) query to the DNS proxy.
3.	The DNS proxy sends the S-NAPTR query to the DNS.

Step	Description
4.	The DNS may return multiple NAPTR resource records with an 'S' flag (for SRV records) with the same or different service parameters.
5.	The DNS proxy forwards the NAPTR resource records to the ePDG.
6.	The ePDG selects the replacement strings (the APN FQDNs) that matches the service parameter if ePDG is configured as MAG for PMIPv6 protocol or service parameter 'x-3gpp-pgw:x-s2b-gtp' when ePDG is configured for GTP protocol support. The ePDG then performs a DNS SRV query with a replacement string (the APN FQDN) for each of the selected replacement strings.
7.	The DNS proxy sends each DNS SRV query to the DNS.
8.	For each SRV query, the DNS returns the SRV resource records with the target strings.
9.	The DNS proxy forwards the SRV response to the ePDG. The ePDG compares the P-GW FQDNs against the configured ePDG FQDN and selects longest suffix matching entry.
10.	The ePDG performs an A/AAAA query with the selected P-GW FQDN.
11.	The DNS proxy sends the A/AAAA query to the DNS.
12.	The DNS returns the IP address of the P-GW.
13.	The DNS proxy forwards the P-GW IP address to the ePDG.

P-GW Initiated Bearer Modification

The following section covers the P-GW initiated default/dedicated bearer modification procedure.

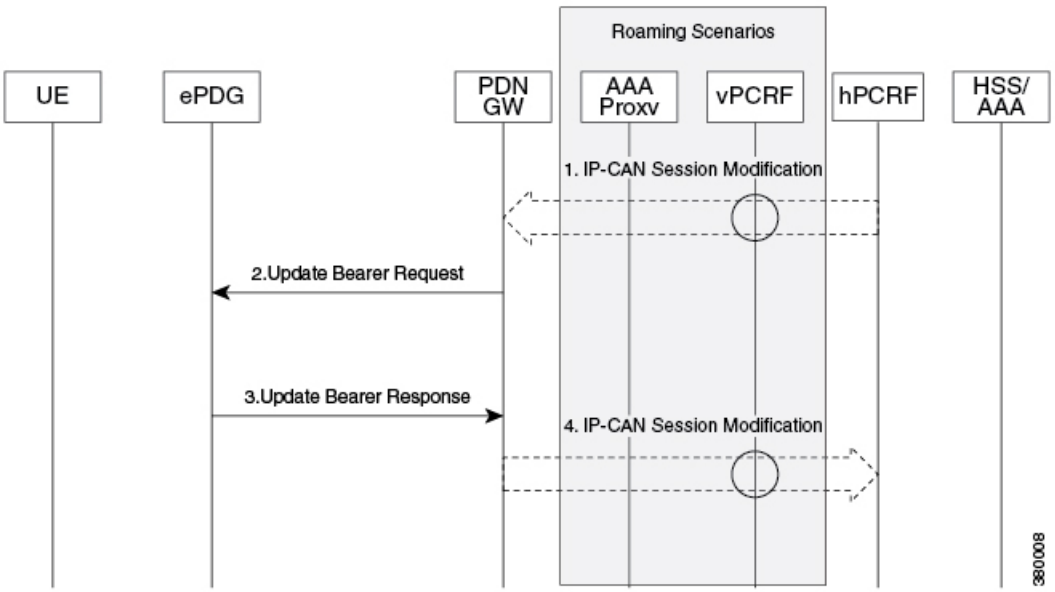

Roaming Scenarios
UE
ePDG
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
1. IP-CAN Session Modification
2.Update Bearer Request
3.Update Bearer Response
4. IP-CAN Session Modification
380008

Table 8: P-GW initiated bearer modification

Step	Description
1.	If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure, up to the point that the PDN GW requests IP CAN Bearer Signalling. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.
2.	The PDN GW uses this QoS policy to determine that a service data flow shall be aggregated to or removed from an active S2b bearer or that the authorized QoS of a service data flow has changed. The PDN GW generates the TFT and updates the EPS Bearer QoS to match the traffic flow aggregate. The PDN GW then sends the Update Bearer Request (APN AMBR, Bearer Context (EPS Bearer Identity, EPS Bearer QoS, TFT)) message to the ePDG.
3.	The ePDG uses the uplink packet filter (UL TFT) to determine the mapping of traffic flows to the S2b bearer and acknowledges the S2b bearer modification to the P-GW by sending an Update Bearer Response (EPS Bearer Identity) message. Also the QCI values received in QoS shall be updated and utilized for the UL traffic DSCP mapping/marking.

Topology/Weight-based Selection

Topology/weight-based selection uses DNS requests to enable P-GW load balancing based on topology and/or weight.

For topology-based selection, once the DNS procedure outputs a list of P-GW hostnames for the APN FQDN, the ePDG performs a longest-suffix match and selects the P-GW that is topologically closest to the ePDG and subscriber. If there are multiple matches with the same suffix length, the Weight and Priority fields in the NAPTR resource records are used to sort the list. The record with the lowest number in the Priority field is chosen first, and the Weight field is used for those records with the same priority.

For weight-based selection, once the DNS procedure outputs a list of P-GW hostnames for the APN FQDN, if there are multiple entries with same priority, calls are distributed to these P-GWs according to the Weight field in the resource records. The Weight field specifies a relative weight for entries with the same priority. Larger weights are given a proportionately higher probability of being selected. The ePDG uses the value of (65535 minus NAPTR preference) as the statistical weight for NAPTR resource records in the same way as the SRV weight is used for SRV records, as defined in RFC 2782.

When both topology-based and weight-based selection are enabled on the ePDG, topology-based selection is performed first, followed by weight-based selection. A candidate list of P-GWs is constructed based on these, and the ePDG selects a P-GW from this list for call establishment. If the selected P-GW does not respond, the ePDG selects the alternate P-GW(s) from the candidate list.

Static IP Address Allocation Support

ePDG supports the static UE IP address communicated by AAA to ePDG over SWm interface (as Served-Party-IP-Address AVP in DEA) and ePDG communicates the same to PGW over S2b interface (as PAA IE of create session request GTP message and Home Network Prefix/IPv4 Home Address in PBU for PMIPv6 case).

This feature is applicable for both GTPv2 and PMIPv6 based implementation.

It shall be AAA server functionality to provide the static PGW IP address, when the UE IP address is provided statically so that same PGW is selected which have the static IP pool corresponding to UE address. ePDG will continue with call establishment and will not be validating the AAA provided PGW allocation type. It is the discretion of PGW to accept/reject call in case the requested static IP address is not available at the PGW.

During handoff calls the priority should be given to UE provided IP address over the ones statically provided by AAA server as the subscribed QoS profile at AAA may not be updated. When UE is offloaded from LTE the IP address provided in LTE to UE should be given priority in WiFi over the AAA provided values. WiFi to WiFi handoff is not a requirement so inter ePDG service handoff is not a valid use-case.

All the three PDN Types UE static IP address are supported including the IPv4, IPv6 and IPv4v6.

Table 9: ePDG Static IP Address support failure matrix

S.N	UE requested PDN Type	AAA provided PDN type	AAA provided Static IP address type	ePDG Action
1	v4	v4	v4	Call established for v4 PDN type using the AAA provided static IP address.
2	v4	v4	v6	Call established for v4 PDN type but ignoring the AAA provided IP address.
3	v4	v4	v4v6	Call established for v4 PDN type and using v4 address provided by AAA.
4	v4	v4v6	v4	Call established for v4 PDN type and using v4 address provided by AAA.
5	v4	v4v6	v4v6	Call established for v4 PDN type and using v4 address provided by AAA.
6	v4	v4v6	v6	Call established for v4 PDN type but ignoring the AAA provided IP address.
7	v4	v6	v6	Call released due to invalid-pdn-type reason.
8	v4	v6	v4v6	Call released due to invalid-pdn-type reason.
9	v4	v6	v4	Call released due to invalid-pdn-type reason.
10	v6	v4	v4v6	Call released due to invalid-pdn-type reason.

S.N	UE requested PDN Type	AAA provided PDN type	AAA provided Static IP address type	ePDG Action
11	v6	v4	v4	Call released due to invalid-pdn-type reason.
12	v6	v4	v6	Call released due to invalid-pdn-type reason.
13	v6	v6	v4	Call established but ignoring the AAA provided IP address.
14	v6	v6	v4v6	Call established for v6 PDN type and using v6 address provided by AAA and v4 address is ignored.
15	v6	v6	v6	Call established for v6 PDN type and using v6 address provided by AAA.
16	v6	v4v6	v6	Call established for v6 pdn and using v6 address provided by AAA.
17	v6	v4v6	v4v6	Call established for v6 PDN and using v6 address provided by AAA and ignoring the v4 address.
18	v6	v4v6	v4	Call established but ignoring the AAA provided IP address.
19	v4v6	v4	v6	Call established using PDN type v4 and the static address provided by AAA is ignored.
20	v4v6	v4	v4	Call established using PDN type v4 and the static address provided by AAA is used.
21	v4v6	v4	v4v6	Call established using PDN type v4 and the static address v4 provided by AAA is used.
22	v4v6	v6	v4	Call established using PDN type v6 and the static address provided by AAA is ignored.
23	v4v6	v6	v6	Call established using PDN type v6 and the static address provided by AAA is used.

S.N	UE requested PDN Type	AAA provided PDN type	AAA provided Static IP address type	ePDG Action
24	v4v6	v6	v4v6	Call established using PDN type v6 and the static address v6 provided by AAA is used.
25	v4v6	v4v6	v4	Call established using PDN type v4v6 and static IP address provided by AAA is used.
26	v4v6	v4v6	v6	Call established using PDN type v4v6 and static v6 IP address provided by AAA is communicated to PGW over S2b.
27	v4v6	v4v6	v4v6	Call established using PDN type v4v6 and static IP address v4v6 both are communicated to PGW over S2b.

In case of mismatch in the PDN type between UE requested and the one provided by AAA server the call shall be released by ePDG with "invalid-pdn-type" as the disconnect reason.

IPv4 and IPv6 Notification for IP Address Alignment

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

The table below details the IPv4 and IPv6 notification alignment.

Table 10: IPv4 and IPv6 Notification for Alignment

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

Threshold Crossing Alerts

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outages. Typically, these conditions are temporary (high CPU utilization or packet collisions on a network, for example) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports threshold crossing alerts for certain key resources such as CPU, memory, etc. With this capability, the operator can configure a threshold on these resources whereby, should the resource depletion cross the configured threshold, an SNMP trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated, then generated and/or sent again at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated, then generated and/or sent again at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Generation of specific traps can be enabled or disabled on the chassis, ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.
- **Logs:** The system provides a facility for which active and event logs can be generated. As with other system facilities, logs are generated messages pertaining to the condition of a monitored value and are generated with a severity level of WARNING. Logs are supported in both the Alert and the Alarm models.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered outstanding until a condition no longer exists or a condition clear alarm is generated. Outstanding alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

Important For more information about threshold crossing alerts, see the *Thresholding Configuration Guide.*

UE Local IP Address IE in the S2B Interface over GTPv2

This chapter describes UE Local IP Address IE in the S2B Interface over GTPv2 feature, below are the links to main sections of the document:

The location of the UE initiating a VoWifi call via ePDG will be identified based on the UE local IP address reported on s2b interface. This location information can be used for multiple purposes like billing and lawful interception etc.

Below is the specifications of the "UE Local IP Address IE in the S2B Interface over GTPv2" feature:

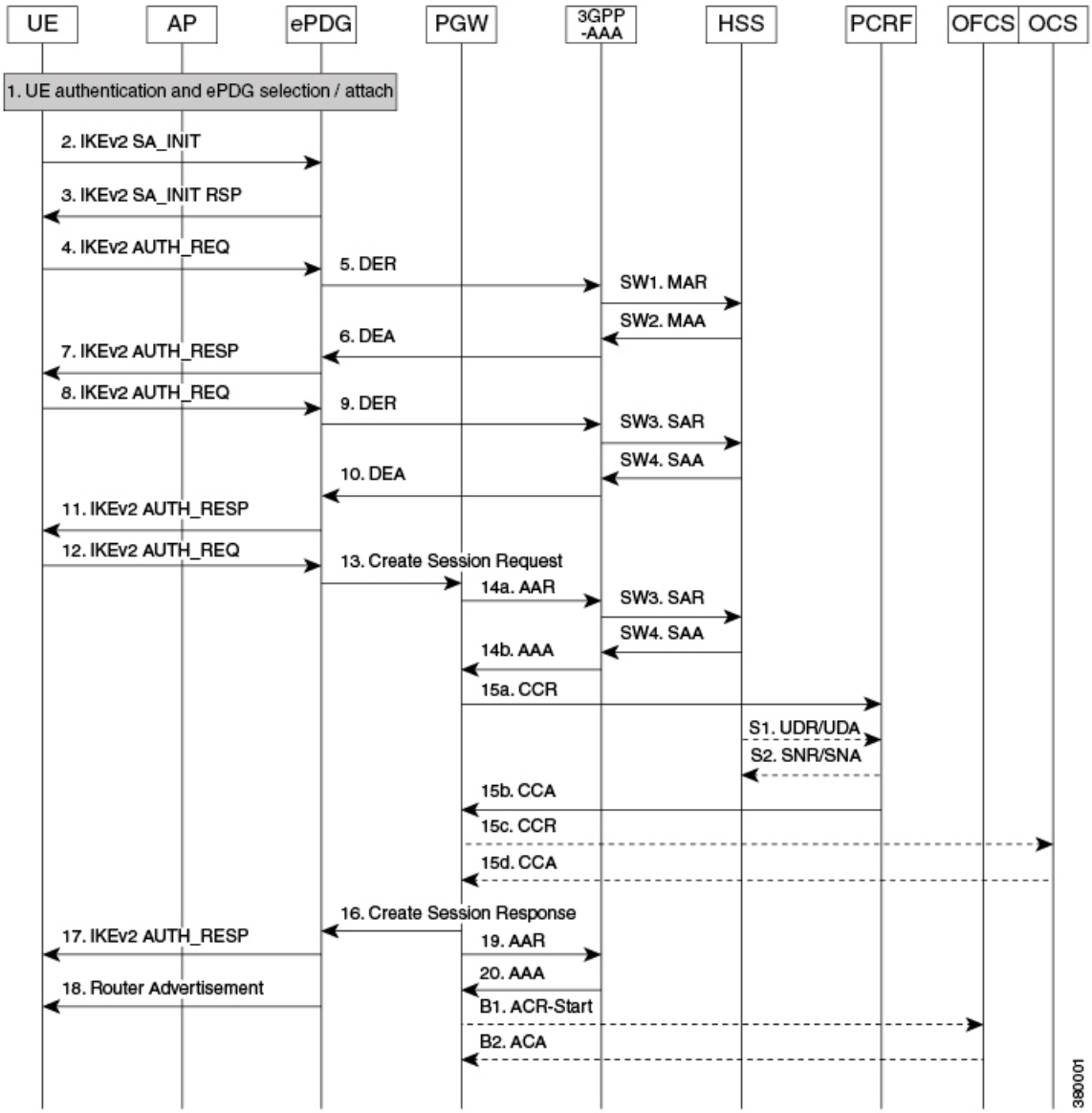
- ePDG saves the UE local IP address (SRC address of the IKE messages received from UE) and the port (SRC port of the IKE message received from UE) and send them to PGW over S2B interface.

- The port information must be sent on S2B interface only when a NAT is detected between UE and ePDG (UE is behind a NAT).
- CLI configuration is supported to control the inclusion of the UE local IP Address and port on the S2B interface.
- The above functionality needs to be supported only for GTPv2 based S2B interface.

How It Works

This section describes signaling flow during an ePDG session setup procedure.

Figure 11: ePDG Session Setup Procedure



The above figure shows the signaling flow during an ePDG session setup procedure:

1. The IKEv2 procedure starts with the IKE_INIT (step 2) message received at ePDG from UE. The SRC address and port of the IKE_INIT message is recorded at ePDG and NAT detection is done as defined in RFC 5996.
2. The IKE_INIT message triggers the IKEv2 tunnel setup and after the IKE_INIT_RESP in step 3, the UE sends IKE_AUTH message (step 4).
3. This IKE_AUTH_REQ from UE triggers the multi round authentication with AAA server on SWm interface.
4. ePDG sends IKE_AUTH_RESP in step 11 to complete the EAP authentication.
5. The next IKE_AUTH_REQ from UE triggers the session setup towards the PGW over s2b interface and ePDG should include the "UE Local IP Address" and "UE UDP Port" (only if NAT detected) AVPs in the Create Session Request message.

Important UE Local IP Address IE in the S2B Interface over GTPv2" supports only for GTPv2 based s2b interface.

Detailed Description

Following table summarizes the expected behavior for UE Local IP Address IE in the S2B Interface over GTPv2 feature.

SR.No	AVP Inclusion via configuration	NAT detected on SWu Interface	Expected Behavior
1.	Enabled	Yes	Both "UE Local IP Address" and "UE UDP Port" AVPs are sent in Create Session Request message to PGW.
2.	Enabled	No	Only "UE Local IP Address" AVP is sent in Create Session Request message to PGW.
3.	Disabled	Yes	Both "UE Local IP Address" and "UE UDP Port" AVPs are NOT sent in Create Session Request message to PGW.
4.	Disabled	No	Both "UE Local IP Address" and "UE UDP Port" AVPs are NOT sent in Create Session Request message to PGW.

External Interfaces

This feature impacts the GTPv2 based s2b interface towards PGW. The following two AVPs as defined in 3GPP 29.274 are included in the Create Session Requested message as per the conditions mentioned in the above table.

Table 11: GTPv2 IE Definition for UE Local IP Address and UE UDP Port

Attribute	Condition	Description	Content
UE Local IP Address	CO	The ePDG should include this IE on S2b interface based on local policy for Fixed Broadband access network interworking see 3GPP in TS 23.139 [51].	IP Address
UE UDP Port	CO	The ePDG shall include this IE on S2b interface if NAT is detected and UE Local IP Address is present for Fixed Broadband access network interworking see 3GPP in TS 23.139 [51].	Port Number

Note: Even though the 3GPP specification mentions the usage of the AVPs in the context of Fixed Broadband access network, they are being used for untrusted WiFi access in this case.

How the ePDG Works

This section describes the ePDG during session establishment and disconnection.

ePDG Session Establishment

The figure below shows an ePDG session establishment flow. The table that follows the figure describes each step in the flow.

Figure 12: ePDG Session Establishment

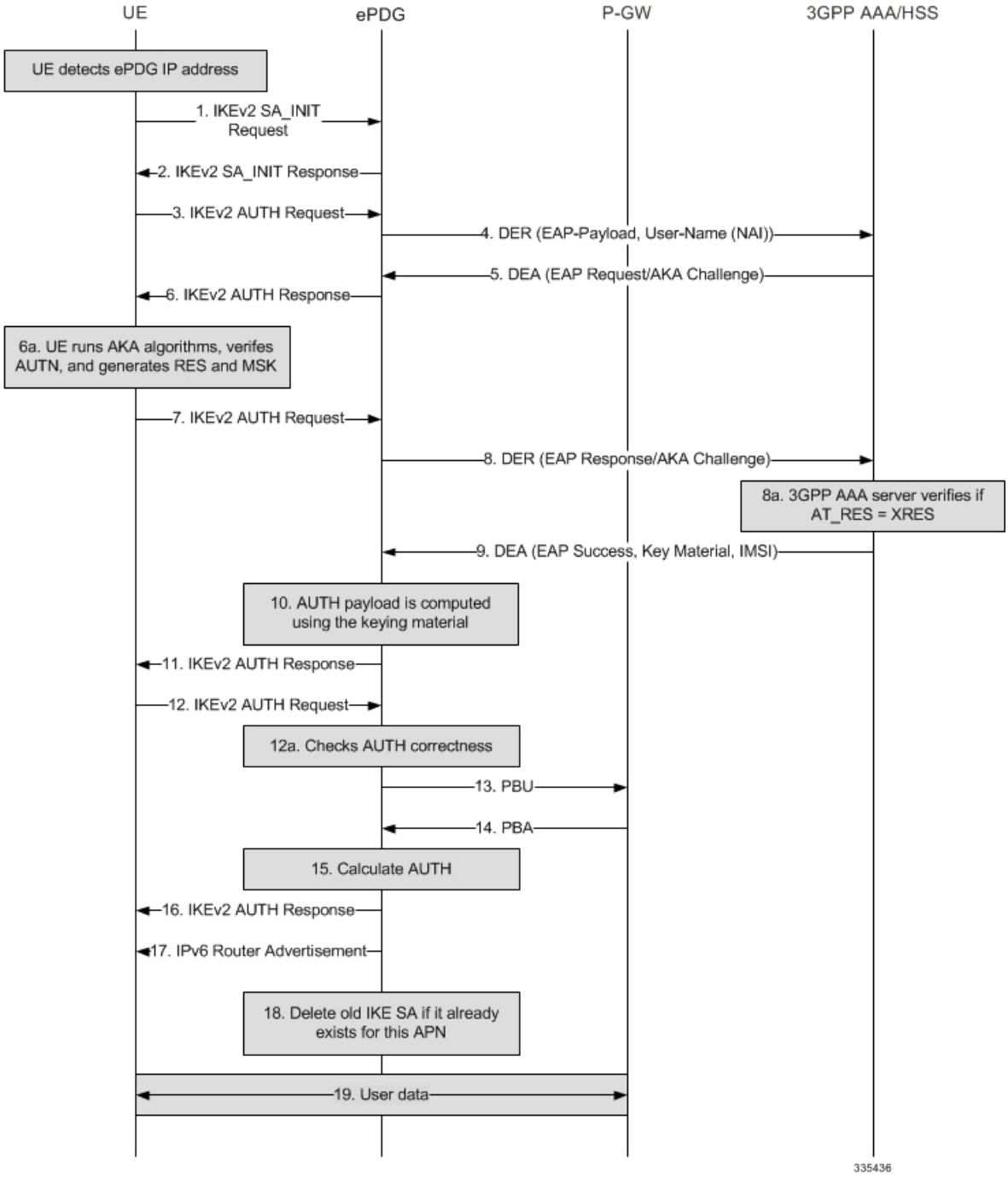


Table 12: ePDG Session Establishment 8

Step	Description
1.	The WLAN UE initiates an IKEv2 exchange with the ePDG by issuing an IKEv2 SA_INIT Request message to negotiate cryptographic algorithms, exchange nonces, and perform a Diffie-Hellman exchange with the ePDG.
2.	The ePDG returns an IKEv2 SA_INIT Response message.
3.	The UE sends the user identity in the IDi payload and the APN information in the IDr payload in the first message of the IKE_AUTH phase and begins negotiation of Child SAs. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity is compliant with the NAI (Network Access Identifier) format specified in TS 23.003 and contains the IMSI as defined for EAP-AKA in RFC 4187. The UE sends the CP payload (CFG_REQUEST) within the IKE_AUTH Request message to obtain an IPv4 and/or IPv6 home IP address and/or a home agent address. The root NAI is in the format "0<IMSI>nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org".
4.	The ePDG sends a DER (Diameter EAP Request) message containing the user identity and APN to the 3GPP AAA server.
5.	The 3GPP AAA server fetches the user profile and authentication vectors from the HSS/HLR if these parameters are not available on the 3GPP AAA server. The 3GPP AAA server looks up the IMSI of the authenticated user based on the received user identity (root NAI) and includes EAP-AKA as the requested authentication method in the request sent to the HSS. The HSS generates the authentication vectors with the AMF separation bit = 0 and sends them back to the 3GPP AAA server. The 3GPP AAA server checks the user's subscription information to verify that the user is authorized for non-3GPP access. The 3GPP AAA server increments the counter for IKEv2 SAs. If the maximum number of IKE SAs for the associated APN is exceeded, the 3GPP AAA server sends an indication to the ePDG that established the oldest active IKEv2 SA (it could be the same ePDG or a different one) to delete the oldest IKEv2 SA. The 3GPP AAA server updates its total active IKEv2 SAs for the APN. The 3GPP AAA server initiates the authentication challenge and responds with a DEA (Diameter EAP Answer). The user identity is not requested again.
6.	The ePDG responds with its identity (a certificate) and sends the AUTH parameter to protect the previous message it sent to the UE in the IKEv2 SA_INIT exchange. It completes the negotiation of the Child SAs, if any. The EAP Request/AKA Challenge message received from the 3GPP AAA server is included in order to start the EAP procedure over IKEv2.
6a.	The UE checks the authentication parameters.
7.	The UE responds to the authentication challenge with an IKEv2 AUTH Request message. The only payload apart from the header in the IKEv2 message is the EAP Response/AKA Challenge message.
8.	The ePDG forwards the EAP Response/AKA Challenge message to the 3GPP AAA server in a DER message.
8a.	The 3GPP AAA server checks if the authentication response is correct.

Step	Description
9.	When all checks are successful, the 3GPP AAA server sends the final DEA (with a result code indicating EAP success) that includes the relevant service authorization information and key material to the ePDG. The key material consists of the MSK generated during the authentication process. The MSK is encapsulated in the EAP-Master-Session-Key-AVP as defined in RFC 4072.
10.	The MSK is used by the ePDG to generate the AUTH parameters in order to authenticate the IKEv2 SA_INIT messages as specified for IKEv2 in RFC 4306. These first two messages had not been authenticated earlier as there was no key material available yet. Per RFC 4304, the shared secret generated in an EAP exchange (the MSK) when used over IKEv2 must be used to generate the AUTH parameters.
11.	The EAP Success/Failure message is forwarded to the UE over IKEv2.
12.	The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKEv2 SA_INIT message. The AUTH parameter is sent to the ePDG.
12a.	The ePDG checks the correctness of the AUTH parameter received from the UE. At this point the UE is authenticated.
13.	On successful authentication, the ePDG establishes the PMIP tunnel towards the P-GW by sending a PBU (Proxy-MIP Binding Update), which includes the NAI and APN and the Home Network Prefix or IPv4 Home Address option.
14.	The P-GW allocates the requested IP address (IPv4/IPv6 or both) session and responds back to the ePDG with a PBA (Proxy-MIP Binding Acknowledgement).
15.	The ePDG calculates the AUTH parameter that authenticates the second IKEv2 SA_INIT message.
16.	The ePDG sends the AUTH parameter, the assigned remote IP address in the CP payload, the SAs, and the rest of the IKEv2 parameters to the UE, and IKEv2 negotiation is complete.
17.	The ePDG sends an IPv6 Router Advertisement to the UE to ensure that the IPv6 stack is fully initialized.
18.	If the ePDG detects that an old IKEv2 SA for the APN already exists, it deletes the IKEv2 SA and sends an INFORMATIONAL exchange with a DELETE payload to the UE to delete the old IKEv2 SA in the UE as specified in RFC 4306.
19.	The ePDG session/IPSec SA is fully established and ready for data transfer.

UE-initiated Session Disconnection

The figure below shows the message flow during a UE-initiated session disconnection. The table that follows the figure describes each step in the message flow.

Figure 13: UE-initiated Session Disconnection

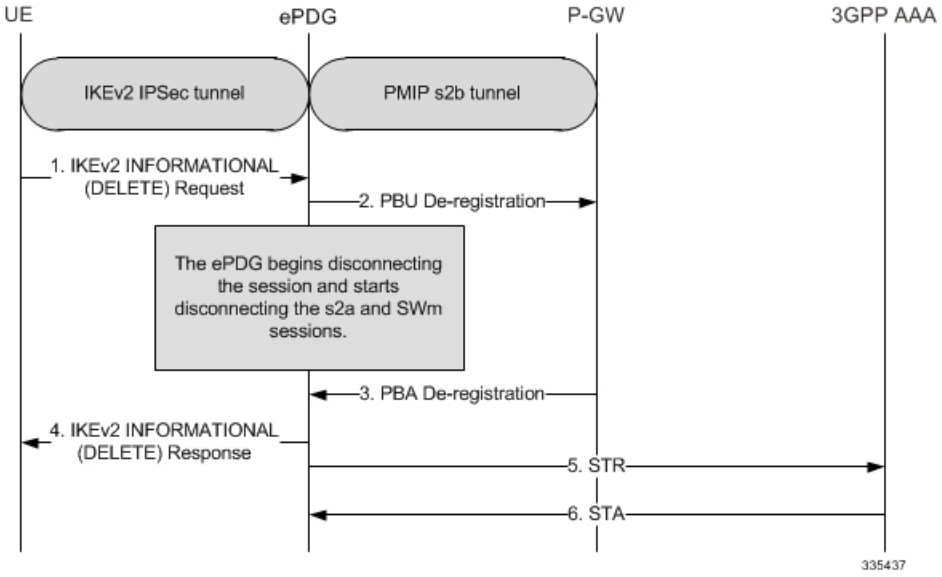


Table 13: UE-initiated Session Disconnection

Step	Description
1.	The UE sends an INFORMATIONAL Request. The Encrypted Payload has a single Delete Payload which contains the SPI of the IKEv2 SA corresponding to the WLAN UE session to be disconnected.
2.	On receiving the IKEv2 INFORMATIONAL Request with Delete from the UE, the ePDG begins the disconnection of the WLAN UE session. It begins the tear down the session by sending PBU for deregistration to P-GW to disconnect the session.
3.	P-GW sends back the PBA message acknowledging the session deletion.
4.	The ePDG responds back to the UE's IKEv2 INORMATION request with a IKEv2 INFORMATIONAL RSP.
6.	3GPP AAA clears the SWn sessions and responds back to the ePDG with a Session-Terminate-Ack (STA).

Figure 14: UE initiated Session Disconnection - GTPv2

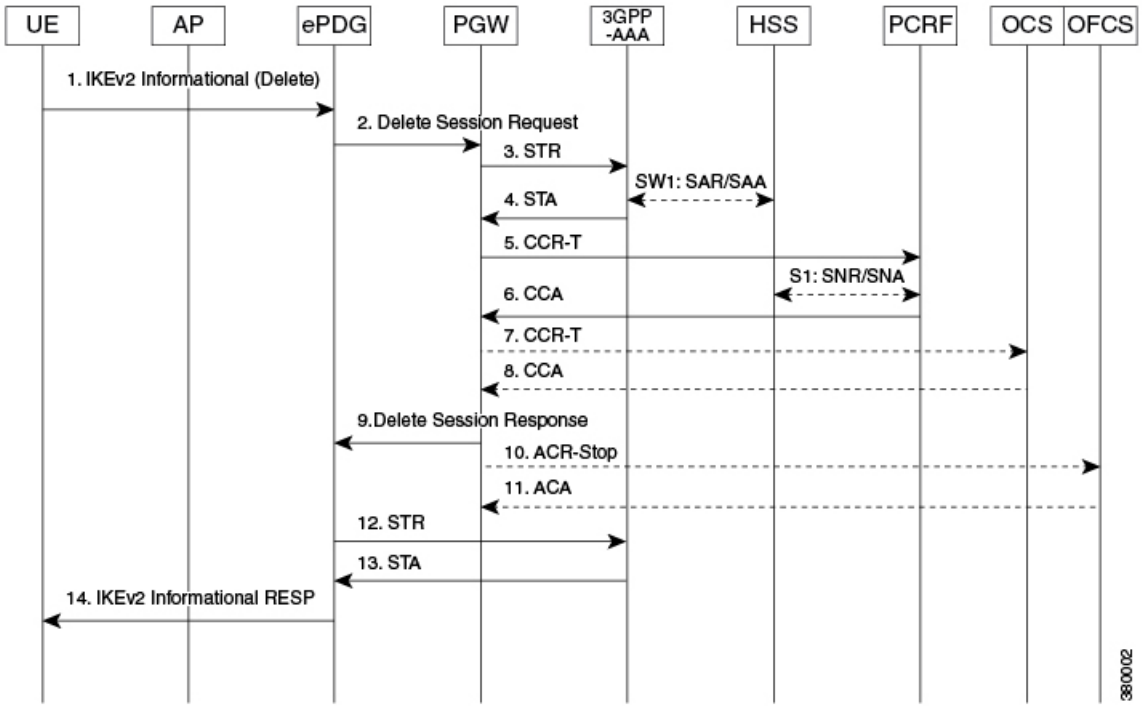


Table 14: UE-initiated Session Disconnection GTPv2

Step	Description
1.	The UE sends an INFORMATIONAL Request. The Encrypted Payload has a single Delete Payload which contains the SPI of the IKEv2 SA corresponding to the WLAN UE session to be disconnected.
2.	On receiving the IKEv2 INFORMATIONAL Request with Delete from the UE, the ePDG begins the disconnection of the WLAN UE session. It begins the tear down the session by sending Delete quest (Linked Bearer ID) to P-GW to disconnect the session.
3.	P-GW sends back the Delete Session Response message acknowledging the session deletion.
4.	ePDG disconnects the SWm session with sending a Session-Terminate-Request (STR) to the 3GPP AAA.
5.	3GPP AAA clears the SWn sessions and responds back to the ePDG with a Session-Terminate-Ack (STA).
6.	The ePDG responds back to the UE's IKEv2 INORMATION request with a IKEv2 INFORMATIONAL RSP.

ePDG-initiated Session Disconnection

The figure below shows the message flow during an ePDG-initiated session disconnection. The table that follows the figure describes each step in the message flow.

Figure 15: ePDG-initiated Session Disconnection

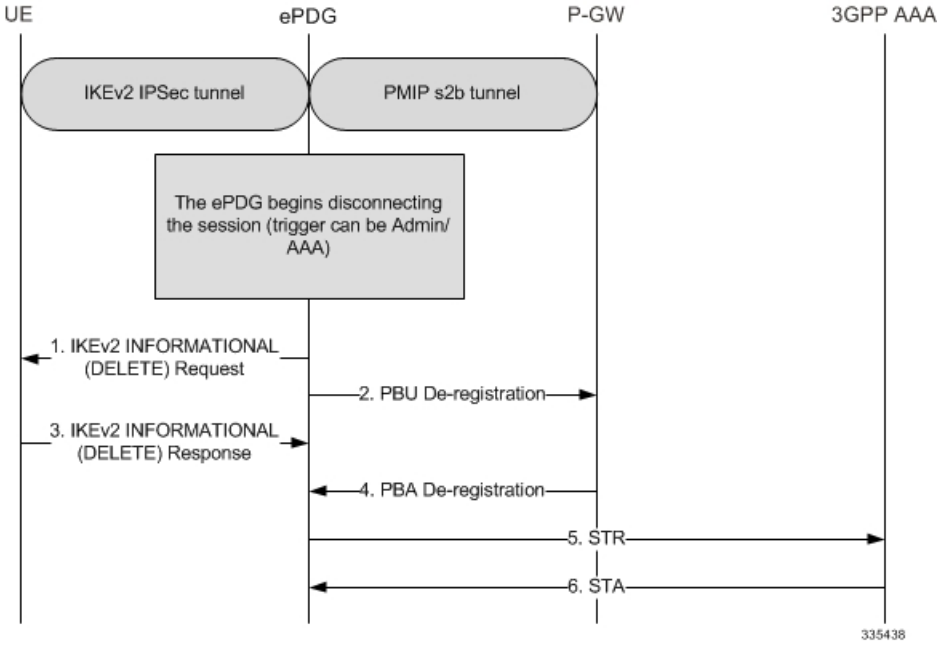


Table 15: ePDG-initiated Session Disconnection

Step	Description
1.	An Admin/AAA trigger causes the ePDG to start disconnecting the WLAN UE session by sending an IKEv2 INFORMATIONAL (DELETE) Request message. The encrypted payload has a single DELETE payload that contains the SPI of the IKEv2 SA corresponding to the WLAN UE session being disconnected.
2.	The ePDG also begins to tear down the S2b PMIP session by sending a PBU (Proxy-MIP Binding Update) De-registration message to the P-GW. **Note** In case the protocol used on S2b is GTPv2 then the "Delete Session Request" message shall be used instead of PBU.
3.	The ePDG responds to the UE's IKEv2 INFORMATIONAL (DELETE) Request message with an IKEv2 INFORMATIONAL (DELETE) Response message.
4.	On receiving the PBU (Proxy-MIP Binding Update) De-registration message, the P-GW disconnects the UE session and releases local resources. The P-GW completes the disconnection of the WLAN UE session and responds to the ePDG with a PBA De-registration message. **Note** In case the protocol used on S2b is GTPv2 then the "Delete Session Response" message shall be used instead of PBA.
5.	The ePDG disconnects the SWu session by sending an STR (Session Terminate Request) message to the 3GPP AAA/HSS.
6.	The 3GPP AAA clears the SWu sessions and responds to the ePDG with an STA (Session Terminate Acknowledgment) message.

P-GW-initiated Session Disconnection

The figure below shows the message flow during a P-GW-initiated session disconnection. The table that follows the figure describes each step in the message flow.

Figure 16: P-GW-initiated Session Disconnection

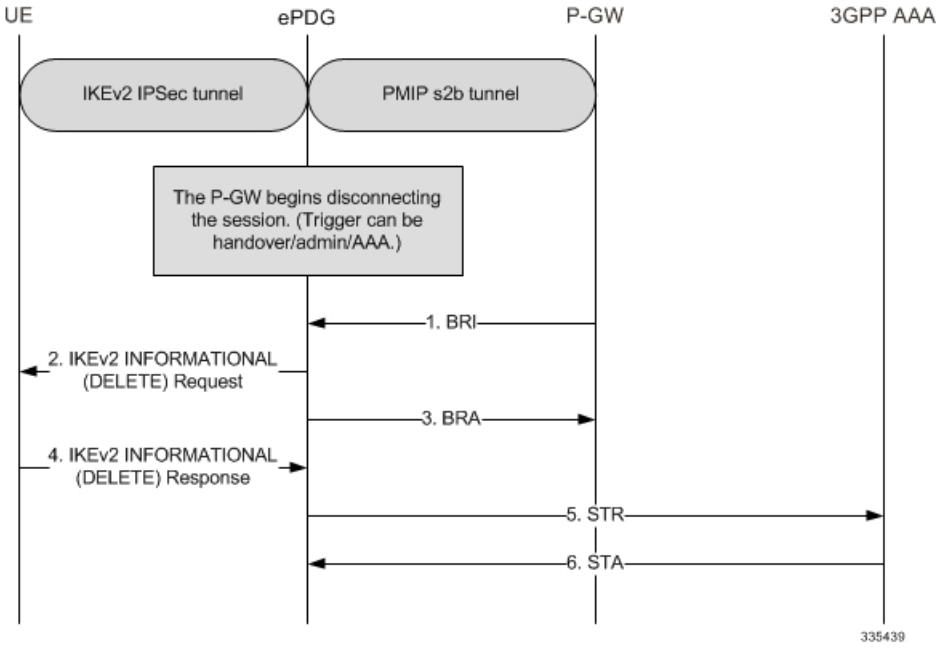


Table 16: P-GW-initiated Session Disconnection

Step	Description
1.	The PGW sends BRI (Binding revocation indication) to ePDG for disconnecting the session.
2.	The ePDG sends IKEv2 Informational Delete Request () to UE to disconnect the session.
3.	The ePDG sends BRA (Binding revocation acknowledgement) to PGW acknowledging the session disconnect
4.	The UE sends IKEv2 Informational Delete Response ().
5.	ePDG sends STR (Session ID, Base AVPs, Termination Cause) to the 3GPP AAA.
6.	3GPP AAA clears the SWn sessions and responds back to the ePDG with a STA (Session ID, Base AVPs).

WiFi-to-WiFi Re-Attach With Same ePDG

The figure below shows the message flow If the UE looses connection to the ePDG and then reconnects using the same ePDG. The table that follows the figure describes each step in the message flow.

Figure 17: WiFi-to-WiFi Re-Attach

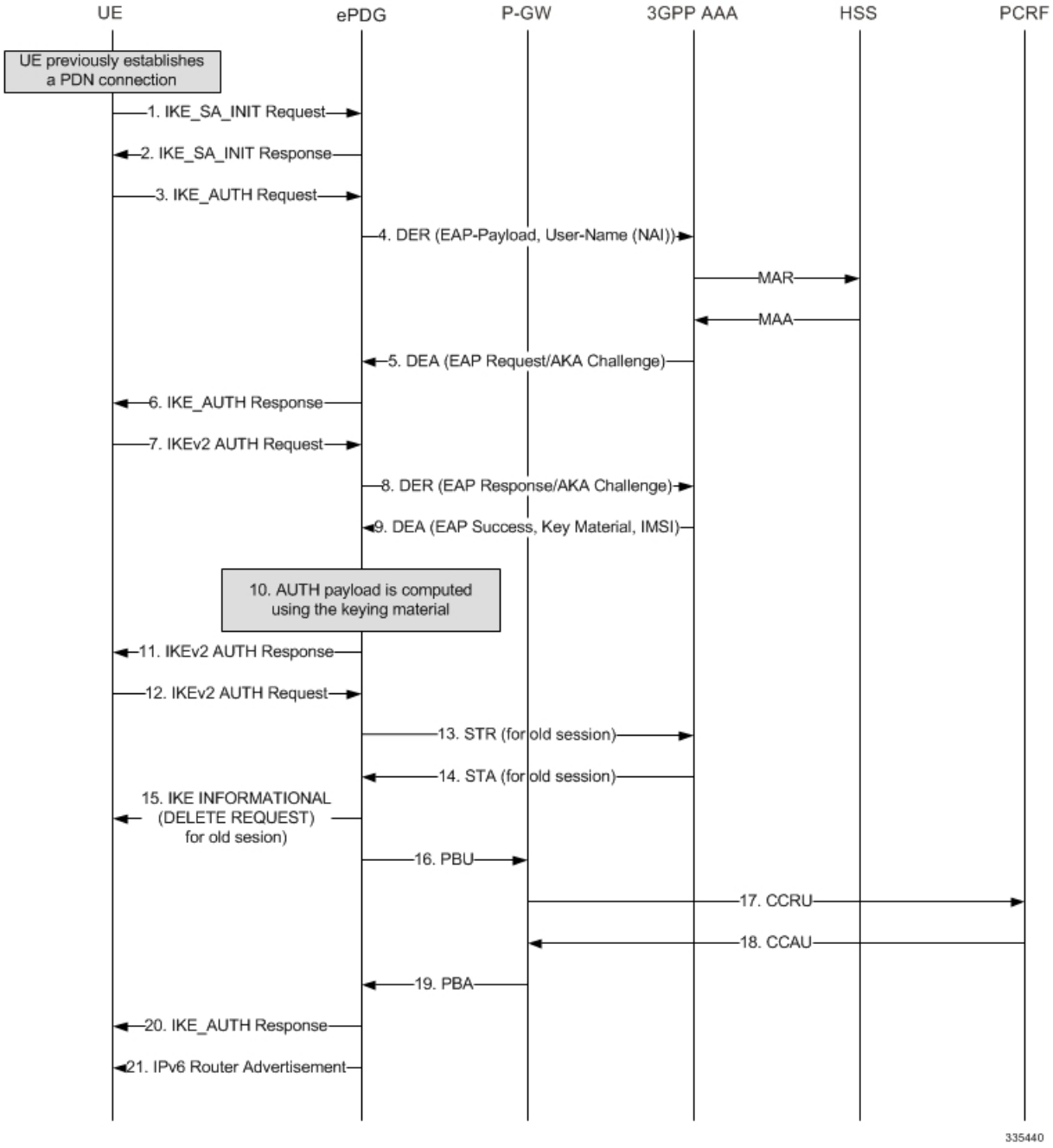
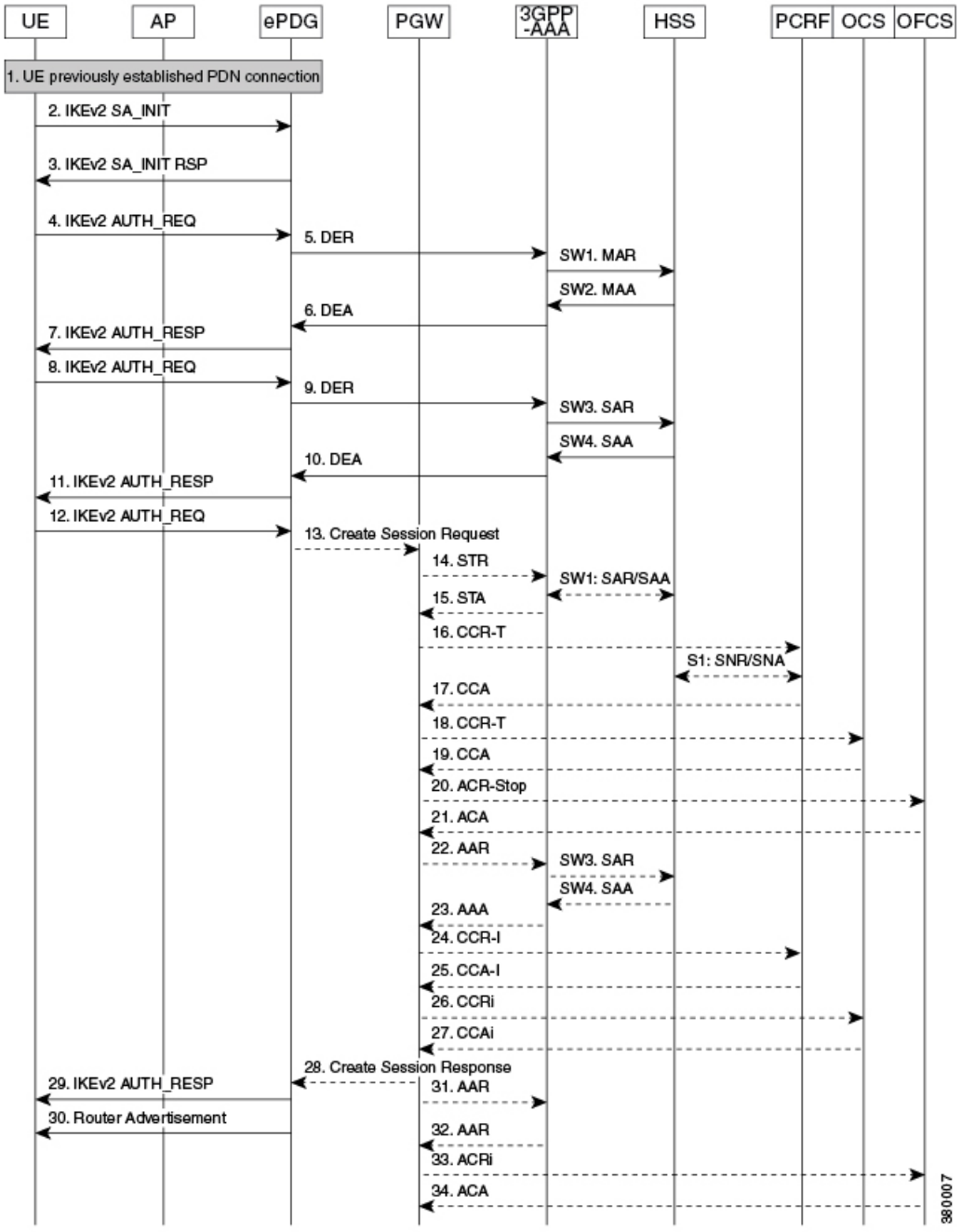


Table 17: WiFi-to-WiFi Re-Attach

Step	Description
1.	The UE is authenticated and a PDN connection is established. This scenario addresses a case where the UE has ungracefully disconnected from the network and is reattaching to the network again.

Step	Description
2.	The session is still active in the ePDG and P-GW along with AAA, PCRF and AAA.
3.	The step 2 through 12 are identical to the UE initial attach scenario defined in section 3.2.1. It is assumed that the UE will not populate the IP Addresses in the IKE Config Request.
4.	The ePDG shall be detecting the duplicate session and clearing the previous established session at its ends. Further ePDG shall be establishing new session on P-GW following below steps
15.	ePDG UE: IKE_AUTH - The ePDG sends IKE_AUTH (AUTH, CP, SA, CFG_REPLY ([INTERNAL_IP4_ADDRESS], [INTERNAL_IP4_NETMASK], [INTERNAL_IP4_DNS], INTERNAL_IP6_ADDRESS, INTERNAL_IP6_SUBNET, INTERNAL_IP6_DNS, P-CSCF) TSi, TSr). The ePDG calculates the AUTH parameter, which authenticates the second IKE_SA_INIT message. The ePDG sends the assigned IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.
16.	ePDG P-GW: PBU (Proxy-MIP Binding Update) - The ePDG selects the P-GW based on DNS response from the APN-FQDN.The ePDG sends PBU (IMSI, [MSIDSN], Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, Bearer Contexts), [Recovery], [Charging Characteristics], Private IE (P-CSCF). The F-TEID shall be set to zero so that P-GW shall handle the same as create-on-create case.
19.	P-GW ePDG: PBA (Proxy-MIP Binding Acknowledgement) - The P-GW terminates the previous session by handling it as create on create case and establishes a new session. The P-GW allocates the requested IP address session and responds back to the ePDG with a PBA (Cause, P-GW S2b Address C-plane, PAA, [Recovery], APN-AMBR, Additional Protocol Configuration Option (APCO) Bearer Contexts Created, Private IE (P-CSCF)) message.
21.	ePGD UE: Router Advertisement - The ePDG sends Router Advertisement to ensure IP Stack is fully initialized.

Figure 18: WiFi-to-WiFi Re-Attach - GTPv2



Description:

The UE is authenticated and a PDN connection is established. This scenario addresses a case where the UE has ungracefully disconnected from the network and is reattaching to the network again.

The session is still active in the ePDG and P-GW along with AAA, PCRF and AAA.

The step 2 through 12 are identical to the UE initial attach scenario defined in section 3.2.1. It is assumed that the UE will not populate the IP Addresses in the IKE Config Request.

The ePDG detects the duplicate session and clears the previous established session at its ends. Then the ePDG establishes a new session on the P-GW using the following steps:

Table 18: WiFi-to-WiFi Re-Attach - GTPv2

Step	Description
13.	ePDG -> P-GW: Create Session Request - The ePDG selects the P-GW based on DNS response from the APN-FQDN.The ePDG sends Create Session Request (IMSI, [MSIDSN], Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, Bearer Contexts), [Recovery], [Charging Characteristics], Private IE (P-CSCF). The TEID shall be set to zero so that P-GW shall handle the same as create-on-create case.
14.	P-GW -> ePDG: Create Session Response - The P-GW terminates the previous session by handling it as create on create case and establishes a new session. The P-GW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, P-GW S2b Address C-plane, PAA, [Recovery], APN-AMBR, Additional Protocol Configuration Option (APCO) Bearer Contexts Created, Private IE (P-CSCF)) message.
29.	ePDG -> UE: IKE_AUTH - The ePDG sends IKE_AUTH (AUTH, CP, SA, CFG_REPLY ([INTERNAL_IP4_ADDRESS], [INTERNAL_IP4_NETMASK], [INTERNAL_IP4_DNS], INTERNAL_IP6_ADDRESS, INTERNAL_IP6_SUBNET, INTERNAL_IP6_DNS, P-CSCF) TSi, TSr). The ePDG calculates the AUTH parameter, which authenticates the second IKE_SA_INIT message. The ePDG sends the assigned IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.
30.	ePDG -> UE: Router Advertisement - ePDG sends Router Advertisement to ensure IP Stack is fully initialized.

WiFi to LTE Handoff with Dedicated Bearer (UE initiated)

When a VoLTE call is ongoing, the P-GW will install the bearers on the LTE network using piggyback procedure.

Figure 19: WiFi to LTE Handoff with Dedicated Bearer - Part 1

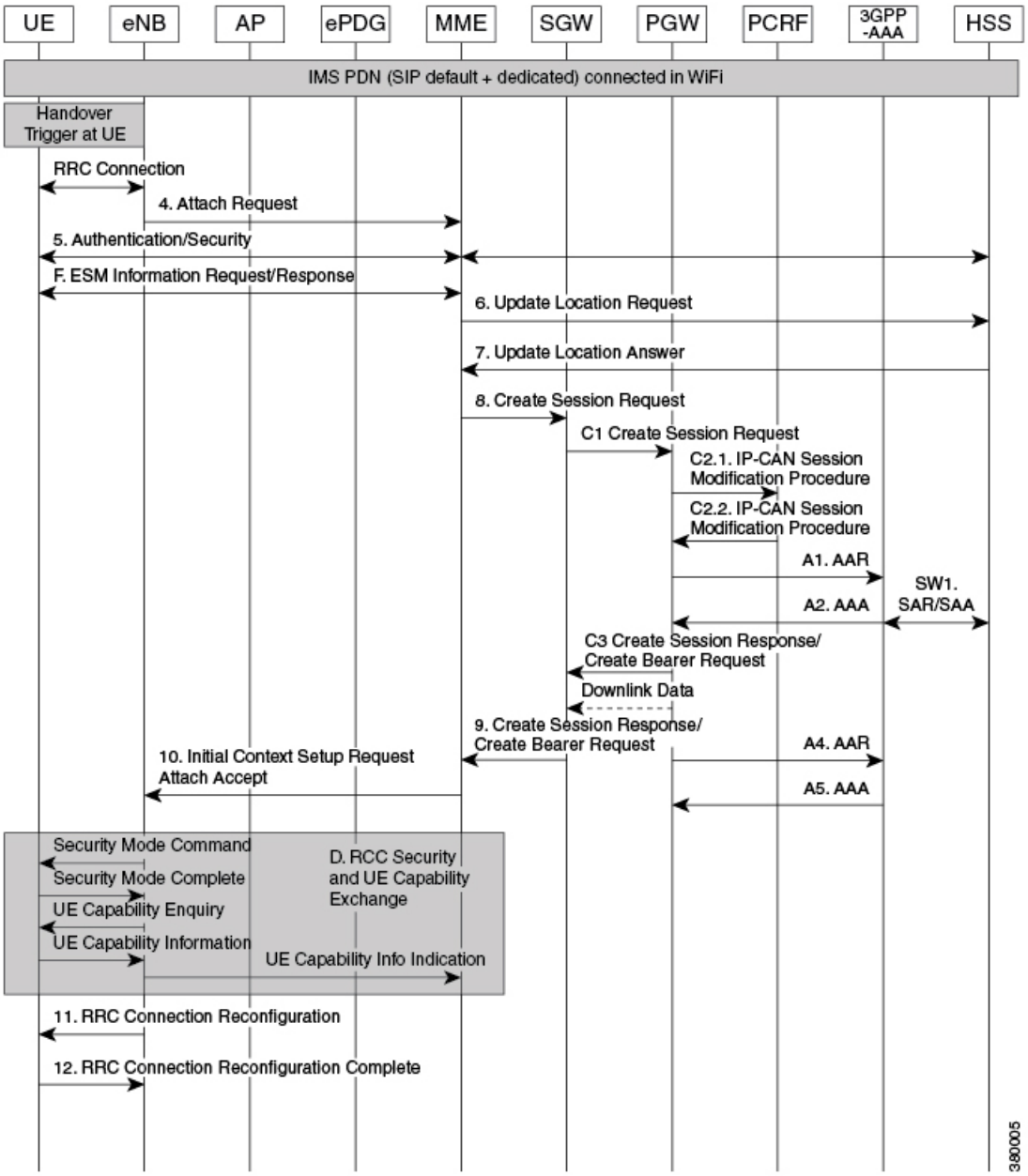
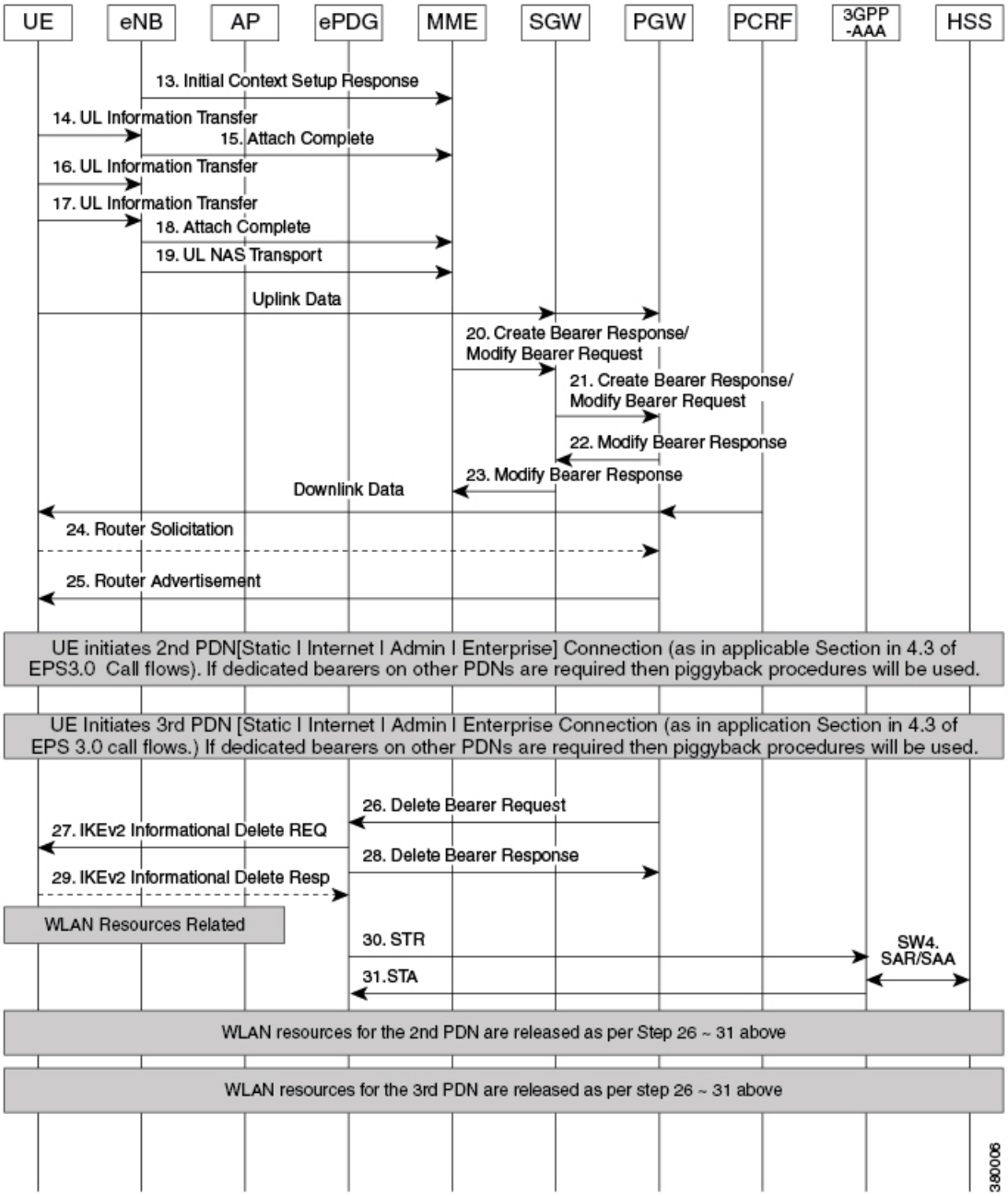


Figure 20: WiFi to LTE Handoff with Dedicated Bearer - Part 2



Note This call flow is the similar as that for IMSI/GUTI-based EUTRAN Attach, except for the additional steps for session clean up on WiFi network and multiple dedicated bearers are set up if voice and video media bearers are present. The critical difference is that the Handover Indication bit shall be set in Create Session Request message.

The UE which was previously having a WiFi call attaches to the LTE.

Table 19: WiFi to LTE Handoff with Dedicated Bearer

Step	Description
26.	P-GW -> ePDG: Delete Bearer Request - The P-GW sends Delete Bearer Request (EPS Bearer ID / LBI, Cause) to ePDG to disconnect the session. If releasing all the bearers LBI shall be set to the identity of the default bearer associated with the PDN connection. Cause shall be set to "Access changed from Non-3GPP to 3GPP".
27.	ePDG -> UE: IKEv2 Information Delete Request - The ePDG sends IKEv2 Informational Delete Request () to UE to disconnect the session.
28.	ePDG -> P-GW: Delete Bearer Response - The ePDG sends Delete Bearer Response (Cause, Linked EPS Bearer Identity, Bearer Context, [Recovery]) to P-GW.
29.	UE -> ePDG: IKEv2 Informational Delete Response - UE responds with IKEv2 Information Delete Response () and initiates air interface resource releaseStep is conditional and UE may not send this response.
30.	ePDG -> AAA: Session Termination Request - The ePDG sends STR (Session ID, User-Name (IMSI-NAI), Termination-Cause) to the 3GPP AAA.
31.	AAA -> ePDG: Session Termination Answer - The AAA sends STA (Session ID, Result-Code) to the ePDG.

LTE to WiFi Hand Off - With Dedicated bearer (UE initiated)

In this call flow we use the IMS PDN with an ongoing VoLTE call with the associated dedicated bearers.

The UE detects suitable WiFi access point and connects to AP as per node selection.

Figure 21: LTE to WiFi Hand Off - With Dedicated Bearer

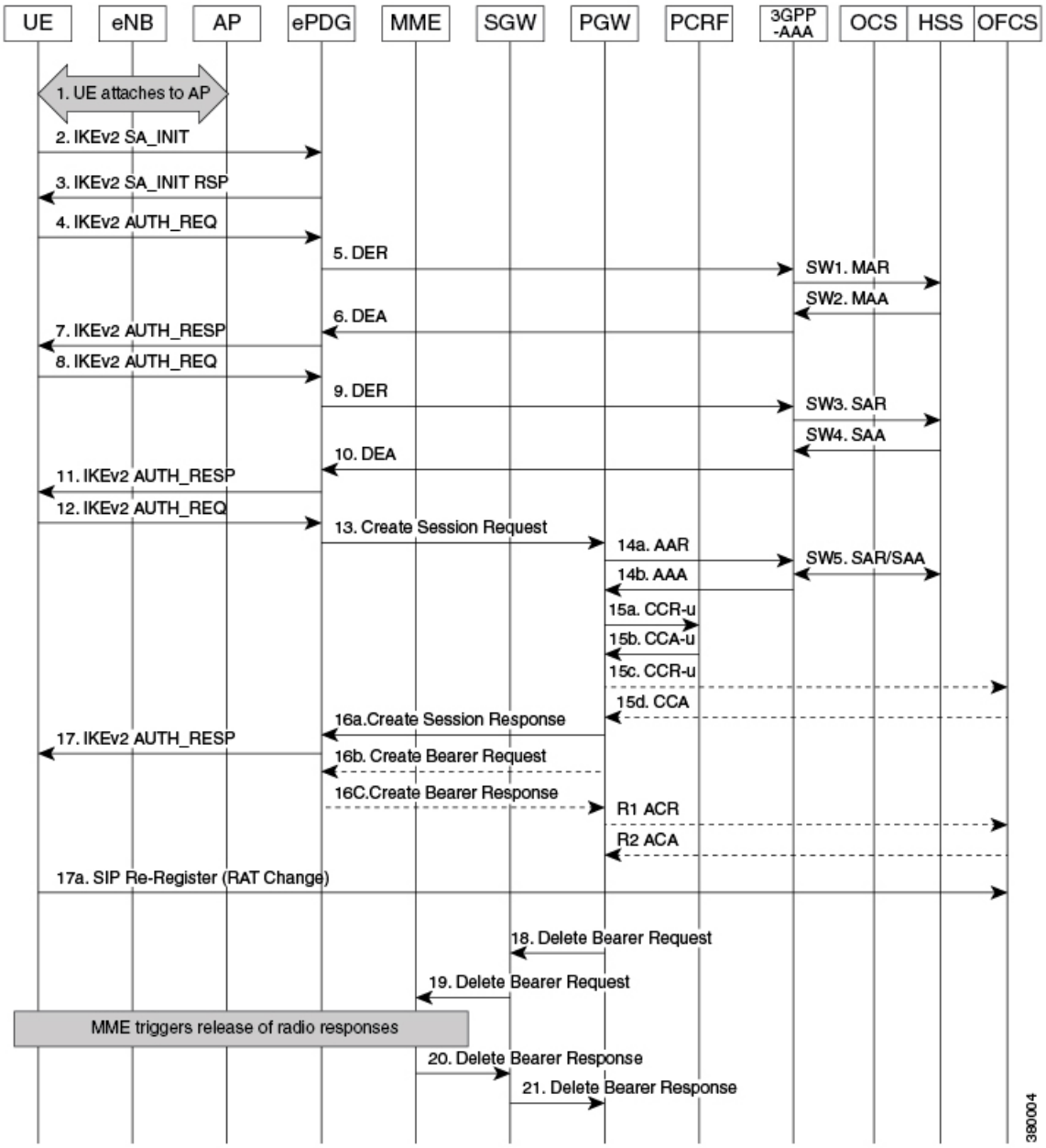


Table 20: LTE to WiFi Hand Off - With Dedicated Bearer 12

Step	Description
1.	The UE is mapped to the access point.
2.	UE -> ePDG: The UE sends IKE_SA_INIT Message.
3.	ePDG -> UE: The ePDG responds with IKE_SA_INIT_RSP Message.
4.	The UE sends the user identity (in the IDi payload) and the APN information (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in TS 23.003 containing the IMSI, as defined for EAP-AKA in RFC 4187. The UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message with the preserved IP address(es) from the LTE session so that ePDG knows its handoff case and communicates same IP address to P-GW. When the MAC ULI feature is enabled the root NAI used will be of the form "0<IMSI>AP_MAC_ADDR:nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org".
5.	The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN.
6.	The 3GPP AAA Server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server shall lookup the IMSI of the authenticated user based on the received user identity (root NAI) and include the EAP-AKA as requested authentication method in the request sent to the HSS. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access. The counter of IKE SAs for that APN is stepped up. If the maximum number of IKE SAs for that APN is exceeded, the 3GPP AAA Server shall send an indication to the ePDG that established the oldest active IKE SA (it could be the same ePDG or a different one) to delete the oldest established IKE SA. The 3GPP AAA Server shall update accordingly the information of IKE SAs active for the APN. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again.
7.	The ePDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations if any. The EAP message received from the 3GPP AAA Server (EAP-Request/AKA-Challenge) is included in order to start the EAP procedure over IKEv2.
8.	The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.
9.	The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server.
9a.	The AAA checks, if the authentication response is correct.

Step	Description
9b.	When all checks are successful, the 3GPP AAA Server sends the final Authentication and Authorization Answer (with a result code indicating success) including the relevant service authorization information, an EAP success and the key material to the ePDG. This key material shall consist of the MSK generated during the authentication process. When the SWm and SWd interfaces between ePDG and 3GPP AAA Server are implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key-AVP, as defined in RFC 4072.
10.	The MSK shall be used by the ePDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified for IKEv2 in RFC 4306. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 4306 [3], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.
11.	The EAP Success/Failure message is forwarded to the UE over IKEv2.
12.	UE -> ePDG: IKEv2 AUTH_REQUEST - The UE sends Auth_Request (IDi, [CERT] | [CERTREQ], IDr (CP), SA (CFQ_REQUEST (INTERNAL_IP4_ADDRESS, INTERNAL_IP4_NETMASK INTERNAL_IP6_ADDRESS, INTERNAL_IP6_SUBNET, INTERNAL_IP4_DNS, INTERNAL_IP6_DNS, TSi, TSr, P-CSCF) **Note** The INTERNAL_IP4_ADDRESS and/or INTERNAL_IP6_ADDRESS must be populated with the IP addresses previously assigned on LTE to indicate that this is a handover.
13.	ePDG -> P-GW: Create SessKPIsion Request - The ePDG sends Create Session Request (IMSI, Serving Network, RAT Type (WLAN), Indication Flags (handover=1, DAB=IPv4v6), Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, Bearer Contexts) to the P-GW. Selection Mode shall be set to "MS or network provided APN, subscribed verified".
16a.	P-GW -> ePDG: Create Session Response - The P-GW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, P-GW S2b Address C-plane, PAA, Bearer Contexts Created, APN-AMBR, Recovery, Additional Protocol Configuration Options (APCO). Private Extension) message
16b.	P-GW -> ePDG: Create Bearer Request - If there are PCC rules that require a dedicated bearer, the P-GW sends Create Bearer Request (LBI, Bearer Contexts (EPS Bearer ID, TFT, S2b-U PGW F-TEID, Bearer Level QoS)) to the ePDG. Note that Charging ID is not sent on S2b.
16c.	The ePDG sends Create Bearer Response (Cause, Bearer Context (EPS Bearer ID, Cause, S2b-U ePDG F-TEID, S2b-U PGW F-TEID), [Recovery]) message.
17.	ePDG -> UE: IKE_AUTH - The ePDG calculates the AUTH parameter, which authenticates the second IKE_SA_INIT message. The ePDG sends the assigned IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

Note The following two counters are available:

- tot--handoff-attempts: Total number of user equipment (UE) attempted LTE to WiFi Handoff. The counter gets incremented at the time of creating ePDG session post IKE_INIT completion, and if the handoff indicator is enabled based on the IKE_AUTH message received from UE.
- tot-success-handoff: Total number of successful LTE to WiFi handoff. UE requests IPv4 or IPv6 or both in CFG Req payload of first IKE_AUTH Req and AAA mandatorily provides PGW IP or FQDN.

Supported Standards

The ePDG service complies with the following standards:

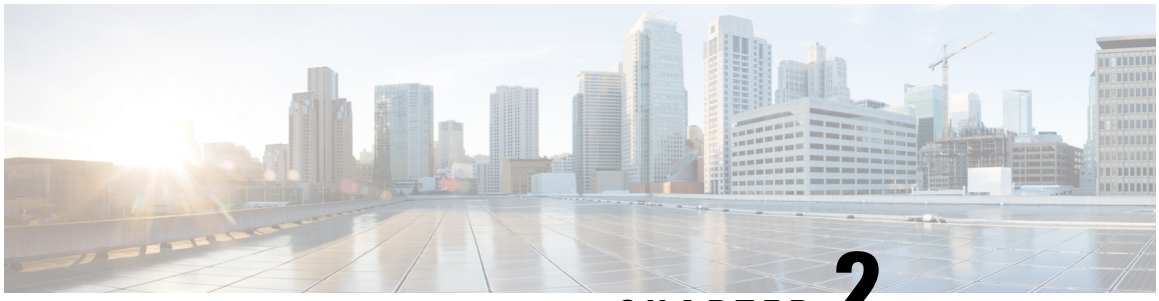
- 3GPP References, on page 90
- IETF References, on page 91

3GPP References

- 3GPP TS 23.234-b.0.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 11)".
- 3GPP TS 24.301-b.7.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)".
- 3GPP TS 23.402-b.7.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 9)".
- 3GPP TS 24.302-b.7.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 (Release 8)".
- 3GPP TS 29.273-b.6.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); 3GPP EPS AAA interfaces (Release 9)".
- 3GPP TS 29.274-b.7.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 11) (b.7.0 (June 2013))".
- 3GPP TS 29.275-a.2.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3 (Release 8)".
- 3GPP TS 29.303-b.2.0 Generation Partnership Project; Technical Specification Group Core Network and Terminals; Domain Name System Procedures; Stage 3(Release 11).
- 3GPP TS 33.234-b.4.0: "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3G Security; Wireless Local Area Network (WLAN) Interworking Security; (Release 6)".
- 3GPP TS 33.402-b.4.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses; (Release 8)."

IETF References

- RFC 2460 (December 1998): "Internet Protocol, Version 6 (IPv6) Specification".
- RFC 2461 (December 1998): "Neighbor Discovery for IP Version 6 (IPv6)".
- RFC 2473 (December 1998): "Generic Packet Tunneling in IPv6 Specification".
- RFC 3588 (September 2003): "Diameter Base Protocol".
- RFC 3602 (September 2003): The AES-CBC Cipher Algorithm and Its Use with IPsec".
- RFC 3715 (March 2004): "IPsec-Network Address Translation (NAT) Compatibility Requirements".
- RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".
- RFC 3775 (June 2004): "Mobility Support in IPv6".
- RFC 3948 (January 2005): "UDP Encapsulation of IPsec ESP Packets".
- RFC 4072 (August 2005): "Diameter Extensible Authentication Protocol (EAP) Application".
- RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".
- RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".
- RFC 4306 (December 2005): "Internet Key Exchange (IKEv2) Protocol".
- RFC 4739 (November 2006): "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".
- RFC 5213 (August 2008): "Proxy Mobile IPv6".
- RFC 5845 (June 2010): "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6".
- RFC 5846 (June 2010): "Binding Revocation for IPv6 Mobility".
- RFC 5996 (September 2010): "Internet Key Exchange Protocol Version 2 (IKEv2)".



CHAPTER 2

Configuring the Evolved Packet Data Gateway

This chapter provides configuration instructions for the ePDG (evolved Packet Data Gateway).

Important Information about the commands in this chapter can be found in the *eHRPD/LTE Command Line Interface Reference.*

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational.

The following section is included in this chapter:

Configuring the System to Perform as an Evolved Packet Data Gateway

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an ePDG in a test environment. For a configuration example without instructions, see "Sample Evolved Packet Data Gateway Configuration File".

Information provided in this section includes the following:

Required Information

The following sections describe the minimum amount of information required to configure and make the ePDG operational in the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

Required Local Context Configuration Information

Table 21: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name(s)	The name(s) of the management interface(s), which can be from 1 to 79 alpha and/or numeric characters. Multiple names are needed if multiple interfaces will be configured.
IP address(es) and subnet mask(s)	The IPv4 address(es) and subnet mask(s) assigned to the interface(s). Multiple addresses and subnet masks are needed if multiple interfaces will be configured.
Remote access type(s)	The type(s) of remote access that will be used to access the system, such as ftpd, sshd, and/or telnetd.
Security administrator name(s)	The name(s) of the security administrator(s) with full rights to the system.
Security administrator password(s)	Open or encrypted passwords can be used.
Gateway IP address(es)	Used when configuring static IP routes from the management interface(s) to a specific network.
Physical Ethernet port number	The physical Ethernet port to which the interface(s) will be bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connectors on the card. For example, port 24/1 identifies connector number 1 on the card in slot 24. A single physical port can facilitate multiple interfaces.

Required Information for ePDG Context and Service Configuration

Table 22: Required Information for ePDG Context and Service Configuration 0

Required Information	Description
ePDG Context Configuration	
ePDG context name	The name of the ePDG context, which can be from 1 to 79 alpha and/or numeric characters.
EAP profile name(s)	The name(s) of the EAP profile(s) to be used for UE authentication via the EAP authentication method.
IPSec transform set name(s)	The name(s) of the IPSec transform set(s) to be used by the ePDG service.
IKEv2 transform set name(s)	The name(s) of the IKEv2 transform set(s) to be used by the ePDG service.
Crypto template name(s)	The name(s) of the IKEv2 crypto template(s) to be used by the ePDG service.

Required Information	Description
Configuration for the SWu, SWm, and DNS Interfaces, and the SWu and SWm Loopback Interfaces	
SWu interface name	The name of the SWu interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface that carries the IPSec tunnels between the WLAN UEs and the ePDG.
SWm interface name	The name of the SWm interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface between the ePDG and the external 3GPP AAA server.
DNS interface name	The name of the DNS interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface between the ePDG and the external DNS.
SWu loopback interface name	The name of the SWu loopback interface, which can be from 1 to 79 alpha and/or numeric characters.
SWm loopback interface name	The name of the SWm loopback interface, which can be from 1 to 79 alpha and/or numeric characters.
IP addresses and subnet masks	The IP addresses assigned to the SWu (IPv4), SWm (either IPv4 or IPv6), and DNS interfaces (either IPv4 or IPv6), and to the SWu (IPv4) and SWm (either IPv4 or IPv6) loopback interfaces.
Physical Ethernet port numbers	The physical Ethernet ports to which the SWu, DNS, and SWm interfaces will be bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connectors on the card. For example, port 19/1 identifies connector number 1 on the card in slot 19. A single physical port can facilitate multiple interfaces.
AAA Group Configuration	
Diameter authentication dictionary	The name of the Diameter dictionary used for authentication.
Diameter endpoint name	The name of the Diameter endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server using the SWm interface.
ePDG Service Configuration	
ePDG service name	The name of the ePDG service, which can be from 1 to 63 alpha and/or numeric characters.
PLMN ID (Public Land Mobile Network Identifier)	The MCC (Mobile Country Code) and MNC (Mobile Network Code) for the ePDG.
Egress context name	The name of the Egress context, which can be from 1 to 79 alpha and/or numeric characters.
MAG service name	The name of the MAG (Mobile Access Gateway) service on the ePDG, which can be from 1 to 63 alpha and/or numeric characters.

Required Information	Description
EGTP service name	The name of the EGTP service associated with ePDG, which can be from 1 to 63 alpha and/or numeric characters.
ePDG FQDN	The ePDG FQDN (Fully Qualified Domain Name), used for longest suffix matching during P-GW dynamic allocation. The ePDG FQDN can be from 1 to 256 alpha and/or numeric characters.
Diameter endpoint name	The name of the Diameter endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server using the SWm interface.
Origin host	The name of the Diameter origin host, which can be from 1 to 255 alpha and/or numeric characters.
Origin host address	The IPv6 address of the Diameter origin host.
Peer name	The name of the Diameter endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server using the Swm interface.
Peer realm name	The name of the peer realm, which can be from 1 to 127 alpha and/or numeric characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Peer address	The IPv4 or IPv6 address of the Diameter endpoint.
DNS client name	The name of the DNS client on the ePDG, which can be from 1 to 63 alpha and/or numeric characters.
DNS address	The IPv4 or IPv6 address of the local DNS client.

Required Information for Egress Context and MAG Service Configuration

The following table lists the information that is required to configure the Egress context and MAG (Mobile Access Gateway) service on the ePDG.

Note ePDG can only be configured and associated either with MAG or EGTP and not both at a time.

Table 23: Required Information for Egress Context and MAG Service Configuration 1

Required Information	Description
Egress context name	The name of the Egress context, which can be from 1 to 79 alpha and/or numeric characters.
S2b Interface Configuration	

Required Information	Description
S2b interface name	The name of the S2b interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface that carries the PMIPv6 signaling between the MAG (Mobile Access Gateway) function on the ePDG and the LMA (Local Mobility Anchor) function on the P-GW.
MIPv6 address and subnet mask	The MIPv6 address and subnet mask assigned to the S2b interface.
S2b loopback interface name	The name of the S2b loopback interface, which can be from 1 to 79 alpha and/or numeric characters.
MIPv6 address and subnet mask	The MIPv6 address and subnet mask assigned to the S2b loopback interface.
Gateway IPv6 address	The gateway IP address for configuring the IPv6 route from the S2b interface to the P-GW.
MAG Service Configuration	
MAG service name	The name of the MAG (Mobile Access Gateway) service, which can be from 1 to 63 alpha and/or numeric characters.
Physical Ethernet port numbers	The physical Ethernet ports to which the SWu, DNS, SWm, and S2b interfaces will be bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connectors on the card. For example, port 24/1 identifies connector number 1 on the card in slot 24. A single physical port can facilitate multiple interfaces.

Required Information for Egress Context and EGTP Service Configuration

The following table lists the information that is required to configure the Egress context and EGTP (Evolved GPRS Tunneling Protocol) service on the ePDG.

Note ePDG can only be configured and associated either with MAG or EGTP and not both at a time.

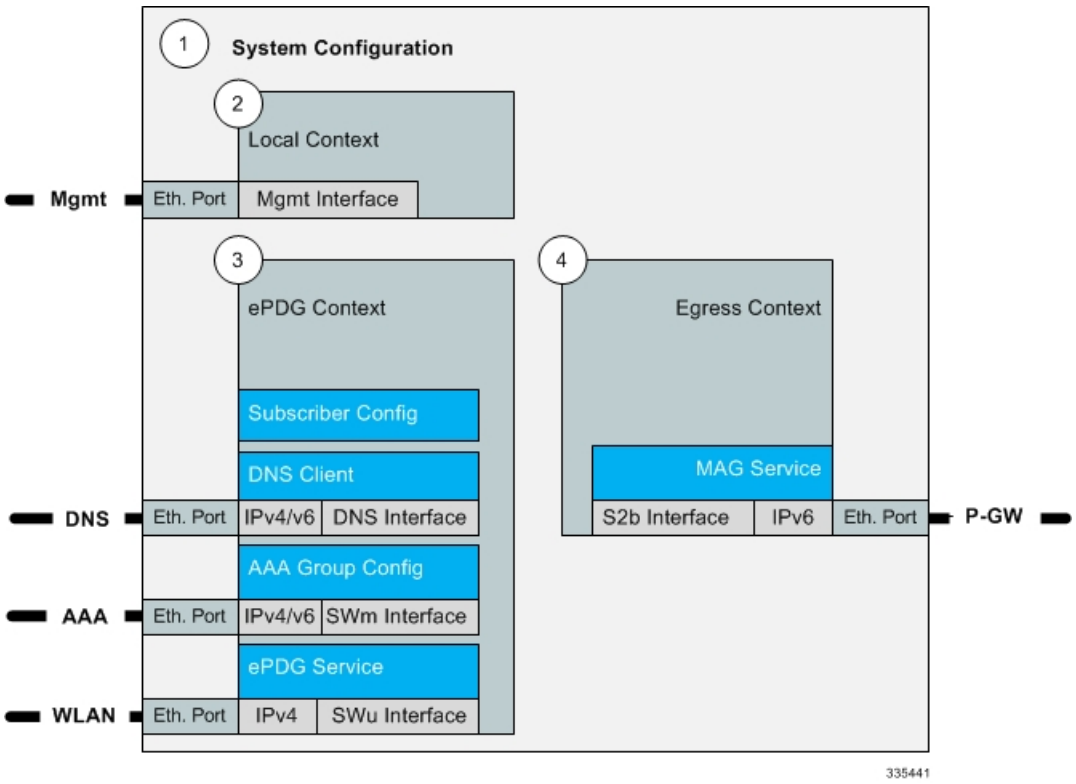
Table 24: Required Information for Egress Context and EGTP Service Configuration 2

Required Information	Description
Egress context name	The name of the Egress context, which can be from 1 to 79 alpha and/or numeric characters.
S2b Interface Configuration	
S2b interface name	The name of the S2b interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface that carries the GTPv2 Signaling and data messages between ePDG and PGW.
S2b loopback interface name	The name of the S2b loopback interface, which can be from 1 to 79 alpha and/or numeric characters.

Required Information	Description
Gateway IPv6 address	The gateway IP address for configuring from the S2b interface to the P-GW.
eGTP Service Configuration	
GTPU service name	Use GTPU service name to allow configuration of GTPU Service. Use the bind configuration to bind the s2b loopback address. This will be used for data plane of GTPv2.
egtp-service name	Use EGTP service name to allow configuration of eGTP service. Use the bind configuration to bind the s2b loopback address for gtpc and also use the association cli to associate the gtpu-service name.

Evolved Packet Data Gateway Configuration

The figure below shows the contexts in which ePDG configuration occurs. The steps that follow the figure explain the high-level ePDG configuration steps.



Step 1 Set system configuration parameters such as activating PSC2s, enabling Diameter Proxy mode, and enabling session recovery by following the configuration examples in the *System Administration Guide.*

Step 2 Set initial configuration parameters in the local context by following the configuration example in the section Initial Configuration, on page 99

Step 3 Configure the ePDG context, the EAP profile, the IPSec and IKEv2 transform sets, the crypto template, the SWu, SWm, and DNS interfaces, the SWu and SWm loopback interfaces, and the AAA group for Diameter authentication by following the configuration example in the section ePDG Context and Service Configuration, on page 100

Step 4 Configure the Egress context and MAG service or Egress context and EGTP by following the configuration example in the section Egress Context and MAG Service Configuration, on page 103 or Required Information for Egress Context and EGTP Service Configuration, on page 97

Step 5 Enable ePDG bulk statistics by following the configuration example in the section Bulk Statistics Configuration, on page 106

Step 6 Enable system logging activity by following the configuration example in the section Logging Configuration, on page 107

Step 7 Save the configuration file.

Initial Configuration

Set local system management parameters by following the configuration example in the section Modifying the Local Context, on page 99.

Modifying the Local Context

Use the following configuration example to create a management interface, configure remote access capability, and set the default subscriber in the local context:

```
configure
     context local
          interface <mgmt_interface_name>
               ip address <ip_address> <subnet_mask>
               exit
          server ftpd
          ssh key <data> length <octets>
          ssh key <data> length <octets>
          ssh key <data> length <octets>
          server sshd
               subsystem sftpd
               exit
          server telnetd
               exit
          subscriber default
               exit
          administrator <name> encrypted password <password> ftp
          aaa group default
             exit
          gttp group default
               exit
          ip route 0.0.0.0 0.0.0.0 <gateway_ip_addr> <mgmt_interface_name>
          exit
        port ethernet <slot_number/port_number>
          no shutdown
          bind interface <mgmt_interface_name> local
```

```
        exit
    end
```

The **server** command configures remote server access protocols for the current context. The system automatically creates a default subscriber, a default AAA group, and a default GTTP group whenever a context is created. The **ip route** command in this example creates a default route for the management interface.

ePDG Context and Service Configuration

Step 1 Create the context in which the ePDG service will reside by following the configuration example in the section Creating the ePDG Context, on page 100

Step 2 Create the ePDG service by following the configuration example in the section Creating the ePDG Service, on page 102

Creating the ePDG Context

Use the following configuration example to create the ePDG context, the EAP profile, the IPSec and IKEv2 transform sets, the crypto template, the SWu, SWm, and DNS interfaces, the SWm and IPSec loopback interfaces, and the AAA group for Diameter authentication:

```
configure
     context <epdg_context_name>
          eap-profile <eap_profile_name>
               mode authenticator-pass-through
               exit
          ipsec transform-set <ipsec_tset_name>
               hmac aes-xcbc-96
               exit
          ikev2-ikesa transform-set <ikev2_ikesa_tset_name>
               hmac aes-xcbc-96
               prf aes-scbc-128
               exit
          crypto template <crypto_template_name> ikev2-dynamic
               authentication remote eap-profile <eap_profile_name>
                    exit
               ikev2-ikesa retransmission-timeout <milliseconds>
               ikev2-ikesa transform-set list <ikev2_ikesa_tset_name>
               ikev2-ikesa rekey
               payload <payload_name> match childsa match any
               ipsec transform-set list <ipsec_tset_name>
                    lifetime <seconds>
                    rekey keepalive
                    exit
               ikev2-ikesa keepalive-user-activity
               ikev2-ikesa policy error-notification
 ikev2-ikesa policy use-rfc5996-notification
               exit
          ip routing maximum-paths <max_num>
          interface <swu_interface_name>
               ip address <ip_address> <subnet_mask>
```

```
            exit
        interface <swm_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        interface <epdg_dns_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        interface <swu_loopback_interface_name> loopback
            ip address <ip_address> <subnet_mask>
            exit
        interface <swm_ipsec_loopback_interface_name> loopback
            ip address <ip_address> <subnet_mask>
            exit
        subscriber default
            aaa group <group_name>
            ip context-name <epdg_context_name>
            exit
        aaa group default
            exit
        aaa group <group_name>
            diameter authentication dictionary <aaa_custom_dictionary>
            diameter authentication endpoint <endpoint_name>
            diameter authentication max-retries <max_retries>
            diameter authentication max-transmissions <max_transmissions>
           diameter authentication request-timeout <request_timeout_duration>

            diameter authentication failure-handling eap-request
request-timeout action terminate
            diameter authentication failure-handling eap-request
result-code <start_result_code_1> to <end_result_code_1> action retry-and-terminate

            diameter authentication failure-handling eap-request
result-code <start_result_code_2> to <end_result_code_2> action terminate
            diameter authentication server <host_name> priority <priority>
            exit
        gttp group default
        exit
    end
```

In this example, the EAP method is used for UE authentication. The **eap-profile** command creates the EAP profile to be used in the crypto template for the ePDG service. The **mode authenticator-pass-through** command specifies that the ePDG functions as an authenticator passthrough device, enabling an external EAP server to perform UE authentication.

The **crypto template** command and associated commands are used to define the cryptographic policy for the ePDG. You must create one crypto template per ePDG service. The **ikev2-dynamic** keyword in the **crypto template** command specifies that IKEv2 protocol is used. The **authentication remote** command specifies the EAP profile to use for authenticating the remote peer.

The **rekey keepalive** command enables Child SA (Security Association) rekeying so that a session will be rekeyed even when there has been no data exchanged since the last rekeying operation. The **ikev2-ikesa keepalive-user-activity** command resets the user inactivity timer when keepalive messages are received from the peer. The **ikev2-ikesa policy error-notification** command enables the ePDG to generate Error Notify

messages for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT exchange.

The **ip routing maximum-paths** command enables ECMP (Equal Cost Multiple Path) routing support and specifies the maximum number of ECMP paths that can be submitted by a routing protocol in the current context. The **interface** command creates each of the logical interfaces, and the associated **ip address** command specifies the IP address and subnet mask of each interface.

The **aaa group** command configures the AAA server group in the ePDG context and the **diameter authentication** commands specify the associated Diameter authentication settings.

The **ikev2-ikesa policy use-rfc5996-notification** command enables processing for new notification payloads added in RFC 5996, and is disabled by default.

Creating the ePDG Service

Use the following configuration example to do the following:

- Create the ePDG service.
- Specify the context in which the MAG/EGTP service will reside.
- Specify the ePDG FQDN (Fully Qualified Domain Name) used for longest suffix matching during P-GW dynamic allocation.
- Bind the crypto template to the ePDG service.
- Specify the Diameter origin endpoint and associated settings.
- Specify the name of the DNS client for DNS queries and bind the IP address.

Important When GTPv2 is used instead of mobile-access-gateway configuration, ePDG shall use associate egtp-service *egtp_service_name*.

```
configure
     context <epdg_context_name>
          epdg-service <epdg_service_name>
               plmn id mcc <code> mnc <code>
```

Note If egtp service is used, we should have **associate egtp-service** <*egtp service name*> instead of **mobile-access-gateway**

```
               mobile-access-gateway context <egress_context_name> mag-service
<mag_service_name>
               setup-timeout <seconds>
               fqdn <domain_name>
               bind address <ip_address> crypto-template <crypto_template_name>
               pgw-selection agent-info error-terminate
               dns-pgw selection topology weight
               exit
          ip route <ip_address/subnet mask> <ip_address/subnet mask> <gateway_ip_address>
 <mgmt_interface_name>
          ip domain-lookup
          ip name-servers <ip_address>
          diameter endpoint <endpoint_name>
```

```
        use-proxy
        origin host <host_name> address <ip_address> port <port_number>
        response-timeout <seconds>
        connection timeout <seconds>
        cea-timeout <seconds>
        dpa-timeout <seconds>
        connection retry-timeout <seconds>
        peer <peer_name> realm <realm_name> address <ip_address>
        route-entry peer <peer_id> weight <priority>
        exit
    dns-client <dns_client_name>
        bind address <ip_address>
        exit
    end
```

The ePDG context defaults to a MAG service configured in the same context unless the **mobile-access-gateway** command is used to specify the context where the MAG service will reside as shown above. The **fqdn** command configures the ePDG FQDN (Fully Qualified Domain Name) for longest suffix match during P-GW dynamic allocation. The IP address that you to the ePDG service above is used as the connection point for establishing the IKEv2 sessions between the WLAN UEs and the ePDG. The **pgw-selection agent-info error-terminate** command specifies the action to be taken during P-GW selection when the MIP6-agent-info parameter is expected but not received from the AAA server/HSS, which is to terminate P-GW selection and reject the call. The **dns-pgw selection topology weight** command enables P-GW load balancing based on both topology, in which the nearest P-GW to the subscriber is selected first, and weight, in which the P-GW is select based on a weighted average.

The **ip route** command in this example creates a route for the SWu interface between the WLAN UEs and the ePDG and specifies the destination IP addresses that will use this route. The **ip domain-lookup** command enables domain name lookup via DNS for the current context. The **ip name-servers** command specifies the IP address of the DNS that the ePDG context will use for logical host name resolution. The **diameter endpoint** command specifies the Diameter origin endpoint.

The **origin host** command specifies the origin host for the Diameter endpoint. The **peer** command specifies a peer address for the Diameter endpoint. The **route-entry** command creates an entry in the route table for the Diameter peer.

The **dns-client** command specifies the DNS client used during P-GW FQDN discovery.

Egress Context and MAG Service Configuration

Create the Egress context and the MAG (Mobile Access Gateway) service by following the configuration example in the section Configuring the Egress Context and MAG Service, on page 103

Configuring the Egress Context and MAG Service

Use the following configuration example to configure the Egress context, the MAG (Mobile Access Gateway) service, the S2b interface and S2b loopback interface to the P-GW, and bind all of the logical interfaces to the physical Ethernet ports.

```
configure
    context <egress_context_name>
        interface <s2b_interface_name>
            ipv6 address <ipv6_address>
```

```
            exit
        interface <s2b_loopback_interface_name>
            ipv6 address <ipv6_address>
            exit
        subscriber default
            exit
        aaa group default
            exit
        gtpp group default
            exit
        mag-service <mag_service_name>
            reg-lifetime <seconds>
            bind address <ipv6_address>
            exit
       ipv6 route <ipv6_address/prefix_length> next-hop <ipv6_address> interface
<s2b_interface_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <swu_interface_name> <epdg_context_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <epdg_dns_interface_name> <epdg_context_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <swm_interface_name> <epdg_context_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <s2b_interface_name> <egress_context_name>
        exit
    end
```

The **mag-service** command creates the MAG (Mobile Access Gateway) service that communicates with the LMA (Local Mobility Anchor) service on the P-GW to provide network-based mobility management. The **ipv6 route** command configures a static IPv6 route to the next-hop router. In this configuration, it configures a static route from the ePDG to the P-GW over the S2b interface. The **bind interface** command binds each logical interface to a physical Ethernet port.

Egress Context and EGTP Service Configuration

Create the Egress context and the EGTP (Evolved GPRS Tunnel Protocal) service by following the configuration example in the section Configuring the Egress Context and EGTP Service, on page 105

Configuring the Egress Context and EGTP Service

Use the following configuration example to configure thegress context, the EGTP (Evolved GPRS Tunnel Protocal) service, the S2b interface and S2b loopback interface to the P-GW, and bind all of the logical interfaces to the physical Ethernet ports.

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

```
configure
     context <egress_context_name>
          interface <s2b_interface_name>
               ipv4/ipv6 address <ipv6_address>
               exit
          interface <s2b_loopback_interface_name>
               ipv4/ipv6 address <ipv6_address>
               exit
          subscriber default
               exit
          aaa group default
               exit
          gtpp group default
               exit
          gtpu-service <gtpu-service-name>
               reg-lifetime <seconds>
               bind ipv4/ipv6-address <s2bloopbackipv4/ipv6_address>
               exit
          egtp-service egtp-epdg-egress
               interface-type interface-epdg-egress
               associate gtpu-service gtpu-epdg-egress
               exit
        ipv4/ipv6 route <ipv4/ipv6_address/prefix_length> next-hop <ip4/ipv6_address>
interface <s2b_interface_name>
          exit
     port ethernet <slot_number/port_number>
          no shutdown
          vlan <tag>
          bind interface <swu_interface_name> <epdg_context_name>
          exit
     port ethernet <slot_number/port_number>
          no shutdown
          vlan <tag>
          bind interface <epdg_dns_interface_name> <epdg_context_name>
          exit
     port ethernet <slot_number/port_number>
          no shutdown
          vlan <tag>
          bind interface <swm_interface_name> <epdg_context_name>
          exit
```

```
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <s2b_interface_name> <egress_context_name>
        exit
    end
```

The **egtp-service** command creates the eGTP (evolved GPRS Tunneling Protocol) service that communicates with the LMA (Local Mobility Anchor) service on the P-GW to provide network-based mobility management. The **ipv6 route** command configures a static IPv6 route to the next-hop router. In this configuration, it configures a static route from the ePDG to the P-GW over the S2b interface. The **bind interface** command binds each logical interface to a physical Ethernet port.

Bulk Statistics Configuration

Use the following configuration example to enable ePDG bulk statistics:

```
configure
    bulkstats collection
    bulkstats mode
        sample-interval <time_interval>
        transfer-interval <xmit_time_interval>
        file <number>
            receiver <ip_address> primary mechanism ftp login <username>
password <pwd>
            receiver <ip_address> secondary mechanism ftp login <username>
password <pwd>
            epdg schema <file_name> format " txbytes : txbytes txpkts :
txpkts rxbytes : rxbytes rxpkts : rxpkts sess-txbytes : sess-txbytes
sess-rxbytes : sess-rxbytes sess-txpackets : sess-txpackets sess-rxpackets
 : sess-rxpackets eap-rxttlsrvrpassthru : eap-rxttlsrvrpassthru
eap-rxsuccsrvrpassthru : eap-rxsuccsrvrpassthru num-gtp-bearermodified :
 num-gtp-bearermodified num-gtp-db-active : num-gtp-db-active
num-gtp-db-released : num-gtp-db-released curses-gtp-ipv4 : curses-gtp-ipv4
 curses-gtp-ipv6 : curses-gtp-ipv6 curses-gtp-ipv4v6 : curses-gtp-ipv4v6
 "
            end
```

The **bulkstats collection** command in this example enables bulk statistics, and the system begins collecting pre-defined bulk statistical information.

The **bulkstats mode** command enters Bulk Statistics Configuration Mode, where you define the statistics to collect.

The **sample-interval** command specifies the time interval, in minutes, to collect the defined statistics. The <*time-interval*> can be in the range of 1 to 1440 minutes. The default value is 15 minutes.

The **transfer-interval** command specifies the time interval, in minutes, to transfer the collected statistics to the receiver (the collection server). The <*xmit_time_interval*> can be in the range of 1 to 999999 minutes. The default value is 480 minutes.

The **file** command specifies a file in which to collect the bulk statistics. A bulk statistics file is used to group bulk statistics schema, delivery options, and receiver configuration. The <*number*> can be in the range of 1 to 4.

The **receiver** command in this example specifies a primary and secondary collection server, the transfer mechanism (in this example, ftp), and a login name and password.

The **epdg schema** command specifies that the epdg schema is used to gather statistics. The <*file_name*> is an arbitrary name (in the range of 1 to 31 characters) to use as a label for the collected statistics defined by the **format** option. The **format** option defines within quotation marks the list of variables in the epdg schema to collect. The format string can be in the range of 1 to 3599.

For descriptions of the epdg schema variables, see "ePDG Schema Statistics" in the *Statistics and Counters Reference.* For more information on configuring bulk statistics, see the *System Administration Guide.*

Logging Configuration

Use the following configuration example to enable logging on the ePDG:

```
configure
     logging filter active facility sessmgr level <critical/error>
     logging filter active facility ipsec level <critical/error>
     logging filter active facility ikev2 level <critical/error>
     logging filter active facility epdg level <critical/error>
     logging filter active facility aaamgr level<critical/error>
     logging filter active facility diameter level<critical/error>
     logging filter active facility egtpc level<critical/error>
     logging filter active facility egtpmgr level<critical/error>
     logging filter active facility gtpumgr level<critical/error>
     logging filter active facility diameter-auth level<critical/error>
     logging active
     end
```

Non UICC device support for certificate and multi authentication configuration

List of authentication methods are defined and associated in Crypto Template. The basic sample configuration required for OCSP and Certificate based authentication is as follows. For backward compatibility, the configuration for auth method inside Crypto Template will be working.

The following are the configuration considerations:

1. At max three sets of authentication methods in list can be associated.
2. Each set has only one local and one remote authentication method configuration.
3. The existing configuration inside the Crypto Template takes precedence over the new auth-method-set defined in case same auth method is configured at both places.

```
configure
```

CA Certificate for device certificate authentication:

```
ca-certificate name <ca-name> pem url file: <ca certificate path>
```

ePDG Certificate:

```
certificate name <epdg-name> pem url file: <epdg certificate path> private-key
pem url file:<epdg private key path>
       eap-profile <profile name>
          mode authenticator-pass-through
       exit
```

```
ikev2-ikesa auth-method-set <list-name-1>
  authentication remote certificate
  authentication local certificate
exit
  ikev2-ikesa auth-method-set <list-name-2>
    authentication eap-profile eap1
exit
     crypto template boston ikev2-subscriber
ikev2-ikesa auth-method-set list <list-name-2> <list-name-2>
  certificate <epdg-name>
  ca-certificate list ca-cert-name <ca-name>
exit
```

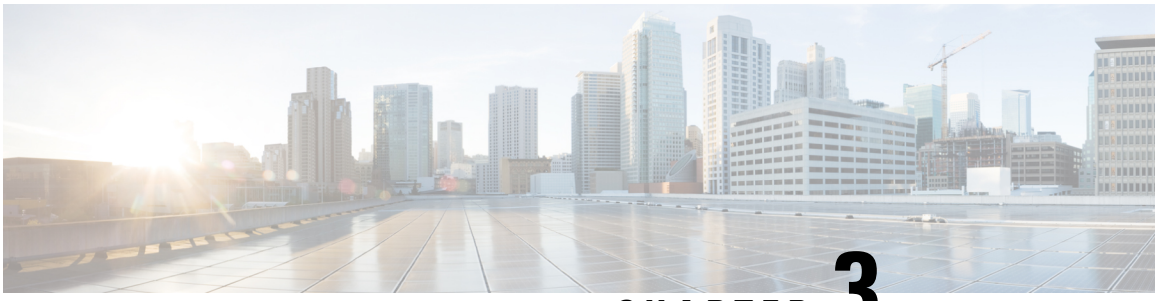
Saving the Configuration

Save the ePDG configuration file to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**.

For additional information on how to verify and save configuration files, see the *System Administration Guide* and the *eHRPD/LTE Command Line Interface Reference.*

Verifying the Configuration

For additional information on how to verify and save configuration files, see the *System Administration Guide* and the *eHRPD/LTE Command Line Interface Reference.*



CHAPTER 3

Monitoring the Evolved Packet Data Gateway

This chapter provides information for monitoring the status and performance of the ePDG (evolved Packet Data Gateway) using the **show** commands found in the CLI (Command Line Interface). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of **show** commands listed in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** commands and keywords, refer to the *eHRPD/LTE Command Line Interface Reference.*

The system also supports the sending of SNMP (Simple Network Management Protocol) traps that indicate status and alarm conditions. See the *SNMP MIB Reference* for a detailed listing of these traps.

Monitoring ePDG Status and Performance

The following table contains the CLI commands used to monitor the status of the ePDG features and functions. Output descriptions for most of the commands are located in the *Statistics and Counters Reference.*

Table 25: ePDG Status and Performance Monitoring Commands

To do this:	Enter this command:
View ePDG Service Information and Statistics	
View ePDG service information and statistics.	**show epdg-service { all [counters] | name** *service_name* **dns-stats] | session | statistics [dns-stats] }**
View ePDG service session information.	**show epdg-service session [all | callid** *call_id* **| counters | | callid** *call_id* **| ip-address** *ip-address* **| peer-address** *ip_a* **username** *name* **] | ip-address** *ip_address* **| peer-address** *ip* **| summary [all | callid** *call_id* **| ip-address** *ip_address* **| peer-address** *ip_address* **| username** *name* **] | username** *n*
View additional session statistics.	**show session [disconnect-reasons | duration | progress | se | subsystem]**
View ePDG bulk statistics.	**show bulkstats variables epdg**

To do this:	Enter this command:
View bulk statistics for the system.	**show bulkstats data**
View IPSec and IKEv2 Information	
View IPSec security associations.	**show crypto ipsec security-associations [summary | tag** *crypto_map_name* **]**
View IPSec transform sets.	**show crypto ipsec transform-set**
View IKEv2 security associations.	**show crypto ikev2-ikesa security-associations [peer** *ipv4/ipv6_address* **| summary | tag** *crypto_map_name* **]**
View IKEv2 transform sets.	**show crypto ikev2-ikesa transform-set**
View IKEv2 statistics.	**show crypto statistics [ikev2]**
View crypto manager statistics.	**show crypto managers [crypto-map** *crypto_map_name* **| inst** *instance_number* **| summary]**
View AES New Instructions (NI) Information **Important** The AES-NI Transform Encryption is supported only on the Ultra Services Platform-based Ultra Gateway Platf (UGP) virtual network function (VNF).	
View the crypto accelerator in the output of this command will indicate if AES-NI acceleration is available for ePDG.	**show card hardware**
View information on AES-NI capabilities, crypto processing threads (shared/dedicated), and statistics on processing of packets per second and IFTASK utilization per thread.	**show crypto process**
View information on Cipher and HMAC per algorithm.	**show crypto process performance slot** *slot_number*
View Diameter AAA Server Information	
View Diameter AAA server statistics.	**show diameter aaa-statistics all**
View Diameter message queue counters.	**show diameter message-queue counters { inbound | outbou**
View Diameter statistics.	**show diameter statistics**
View Congestion Control Information	
View congestion control statistics.	**show congestion-control statistics ipsecmgr**
View Subscriber Information	
View Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in the context where the subscriber resides).	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings.	**show subscribers aaa-configuration username** *subscriber_r*

To do this:	Enter this command:
View subscriber information based on IPv6 address.	**show subscribers ipv6-address** *ipv6_address*
View subscriber information based on IPv6 address prefix.	**show subscribers ipv6-prefix** *prefix*
View subscriber information based on caller ID.	**show subscribers callid** *call_id*
View subscriber information based on username.	**show subscribers username** *name*
View information for troubleshooting subscriber sessions.	**show subscribers debug-info**
View a summary of subscriber information.	**show subscribers summary**
View Subscribers Currently Accessing the System	
View a list of subscribers currently accessing the system.	**show subscribers all**
View a list of ePDG subscribers currently accessing the system.	**show subscribers epdg-only** [[**all**] | [*call_id*] | [**card-num** *card_num*] | [**configured-idle-timeout** { **0..4294967295** | *idle_timeout* | **>** *idle_timeout* | **greater-than** *idle_timeout* | **less-than** *idle_timeout* }] | [**connected-time** { **0..4294967295** | **<** *connect* | **>** *connected_time* | **greater-than** *connected_ti* **less-than** *connected_time* }] | [**counters**] **data-rate**] | [**full**] | [**gtp-version** *vers* [**gtpu-bind-address** *ip_address*] | [**gtpu-s** *service_name*] | [**idle-time** { **0..429496729** *idle_time* | **>** *idle_time* | **greater-than** *idle_ti* **less-than** *idle_time* }] | [**ip-address** { **<** *ipv4_address* | **>** *ipv4_address* | **IPv4** | **greater** *ipv4_address* | **less-than** *ipv4_address* }] | [**ipv6-prefix** *ipv6_address/len_format*] | [**long-duration-time-left** { **0..4294967295** *long_dur_time* | **>** *long_dur_time* | **greater-than** *long_dur_time* | **less-than** *long_dur_time* }] | **network-type** { **gre** | **ipip** | **ipsec** | **ipv4** | **ipv4-pmipv**6 | **ipv4v6** | **ipv4v6-pmipv6** | **ip** **ipv6-pmipv6** | **l2tp** | **mobile-ip** | **proxy-mob** }] | [**qci** *qci*] | [**rx-data** { **0..18446744073709551615** | **<** *rx_bytes* | **>** *rx* | **greater-than** *rx_bytes* | **less-than** *rx_bytes* [**session-time-left** { **0..4294967295** | **<** *sess_time_left* | **>** *sess_time_left* | **greater-th** *sess_time_left* | **less-than** *sess_time_left* }] **smgr-instance** *smgr_instance*] | [**summary**]] | [**tx-data** { **0..18446744073709551615** *tx_bytes* | **>** *tx_bytes* | **greater-than** *tx_bytes* **less-than** *tx_bytes* }] | [**username**] | [**|** *grep_options* **| more }**]]

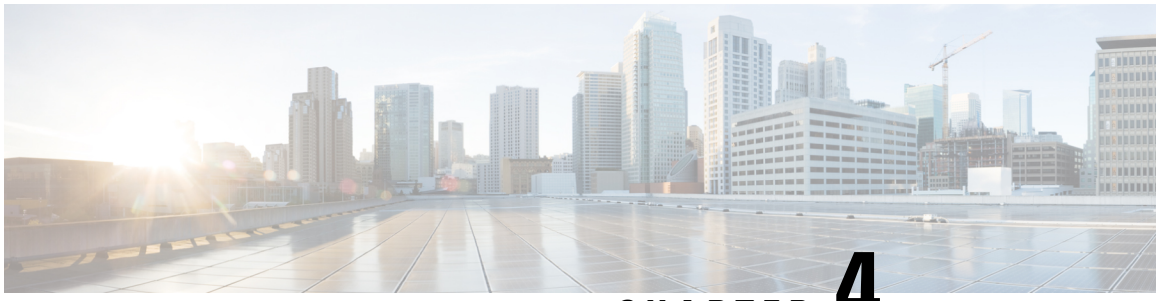
To do this:	Enter this command:
View a list of ePDG subscribers currently accessing the system per ePDG service.	**show subscribers epdg-service** *service_name* [**all**] | [**callid** *call_id*] | [**card-num** *card_nu* [**configured-idle-timeout** { **0..4294967295** *idle_timeout* | **>** *idle_timeout* | **greater-than** *idle_timeout* | **less-than** *idle_timeout* }] | [**connected-time** { **0..4294967295** | **<** *connected_* | **>** *connected_time* | **greater-than** *connected_time* **less-than** *connected_time* }] | [**counters**] | [**data-rate**] | [**full**] | [**gtp-version** *version* [**gtpu-bind-address** *ip_address*] | [**gtpu-ser** *service_name*] | [**idle-time** { **0..4294967295** *idle_time* | **>** *idle_time* | **greater-than** *idle_time* **less-than** *idle_time* }] | [**ip-address** { **<** *ipv4_address* | **>** *ipv4_address* | **IPv4** | **greater-t** *ipv4_address* | **less-than** *ipv4_address* }] | [**ipv6-prefix** *ipv6_address/len_format*] | [**long-duration-time-left** { **0..4294967295** | **<** *long_dur_time* | **>** *long_dur_time* | **greater-than** *long_dur_time* | **less-than** *long_dur_time* }] | [**network-type** { **gre** | **ipip** | **ipsec** | **ipv4** | **ipv4-pmipv**6 | **ipv4v6** | **ipv4v6-pmipv6** | **ipv6** **ipv6-pmipv6** | **l2tp** | **mobile-ip** | **proxy-mobil** }] | [**qci** *qci*] | [**rx-data** { **0..18446744073709551615** | **<** *rx_bytes* | **>** *rx_by* | **greater-than** *rx_bytes* | **less-than** *rx_bytes* } [**session-time-left** { **0..4294967295** | **<** *sess_time_left* | **>** *sess_time_left* | **greater-than** *sess_time_left* | **less-than** *sess_time_left* }] | [**smgr-instance** *smgr_instance*] | [**summary**] | [ ] | [**tx-data** { **0..18446744073709551615** | **<** *tx_bytes* | **>** *tx_bytes* | **greater-than** *tx_bytes* | **less-than** *tx_bytes* }] | [**username**] | [**| { g** *grep_options* **| more }**]]
View the P-CSCF addresses received from the P-GW.	**show subscribers full username** *subscriber_name*
View statistics for subscribers using a MAG service on the system.	**show subscribers mag-only [all | full | summary]**
View statistics for subscribers using a MAG service per MAG service.	**show subscribers mag-service** *service_name*
View Session Subsystem and Task Information	
View Session Subsystem Statistics **Important** Refer to the *System Administration Guide* for additional information on the Session subsystem and its vario manager tasks.	
View AAA Manager statistics.	**show session subsystem facility aaamgr all**

To do this:	Enter this command:
View AAA Proxy statistics.	**show session subsystem facility aaaproxy all**
View Session Manager statistics.	**show session subsystem facility sessmgr all**
View MAG Manager statistics.	**show session subsystem facility magmgr all**
View session progress information for the ePDG service.	**show session progress epdg-service** *service_name*
View session duration information for the ePDG service.	**show session duration epdg-service** *service_name*
View Task Statistics	
View resource allocation and usage information for Session Manager.	**show task resources facility sessmgr all**
View resource allocation and usage information for IPSec Manager.	**show task resources facility ipsecmgr all**
View Session Resource Status	
View session resource status.	**show resources session**
View Session Recovery Status	
View session recovery status.	**show session recovery status [verbose]**
View Session Disconnect Reasons	
View session disconnect reasons.	**show session disconnect-reasons**
View GTPU Tunnels Information	
View GTPU tunnels information	**show gtpu statistics**
View GTP Session Information Like Control Plane TEIDs	
View GTP session information like control plane TEIDs	**show egtp sessions**
View Subscriber TFT	
View subscriber TFT	**show subscriber tft**
View GTP Messages Information	
View GTP messages information	**show egtpc statistics**
Chassis ICSR Status and monitoring	
View SRP Information	**show srp info**
View SRP checkpoint Statistics	**show srp checkpoint statistics**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping.

Statistics and counters can be cleared using the CLI **clear** command. You can also use specific command options such as **clear epdg-service statistics dns-stats**. Refer to the *eHRPD/LTE Command Line Interface Reference* for detailed information on using this command.



CHAPTER 4

AAA based PGW Selection for ePDG Initial Attach

This chapter describes configuring AAA provided PGW-ID as top priority for PGW selection for initial attach using the CLI **prefer aaa-pgw-id** .

AAA Based PGW Selection

Feature Description

ePDG allows to configure AAA provided PGW-ID as top priority for PGW selection for initial attach using the “prefer aaa-pgw-id” CLI under pgw-selection of epdg-service. By default this feature is disabled.

ePDG support PGW selection based on the configuration for the following options for the initial attach calls regardless of allocation type static or dynamic.

- AAA provided PGW ID (IP address as well as FQDN) when alloc type is dynamic or static
- APN-FQDN based PGW selection
- Local IP/FQDN based PGW selection

Following fall back combinations to be supported

1. AAA ->DNS
2. AAA ->Local
3. AAA->DNS->Local
4. AAA->Local->DNS

Note AAA means PGW-ID provided from AAA server is considered for PGW selection. DNS means APN-FQDN is considered for PGW selection.

Note In case of PGW FQDN configured locally, then ePDG will not consider local configuration regarding fallback and will consider DNS in case first selection will fail.

There is no change for PGW selection in handover scenario. ePDG is considering only PGW-ID (IP address/FQDN) for handover.

Configuring AAA Based PGW Selection

Configuring AAA Based PGW Selection

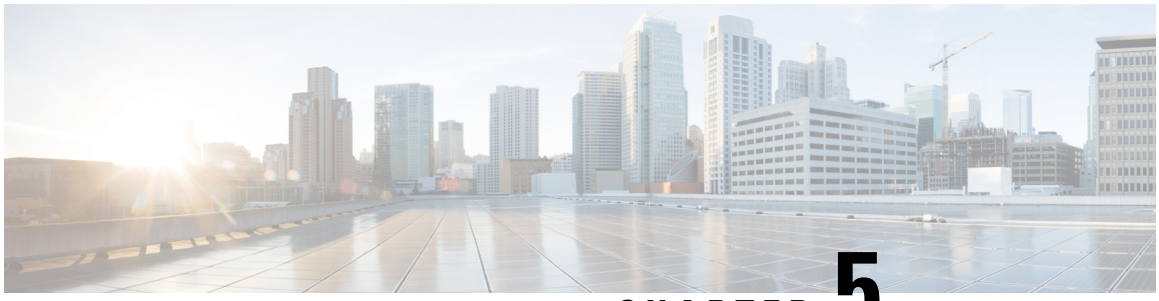
Syntax

```
configure
    eped service
        [ no ] pgw-selection { agent-info error-terminate  |
local-configuration-preferred | prefer aaa-pgw-id }
    end
```

show epdg-service all

The following show output variables are introduced for **show epdg-service all** command.

- AAA-PGW-ID(IP Address/FQDN)
- Local(IP address)
- DNS(APN-FQDN)



CHAPTER 5

Capability to Record and Produce Call Transactions

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Added RTT Record Schema table.	21.26
ePDG supports capability to record and produce call transactions.	21.23
First Introduced.	Release 20

Feature Description

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

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

How it Works

This section describes the RTT procedures and schema.

RTT Procedures

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

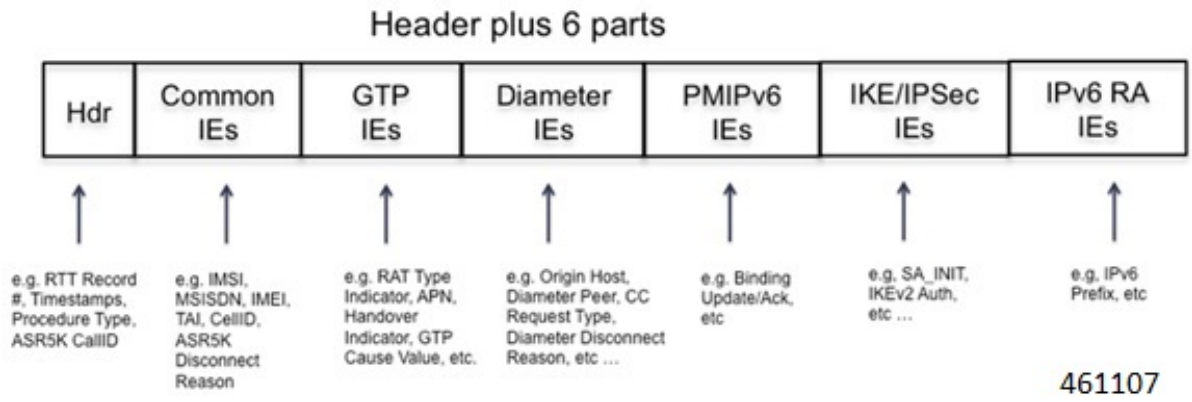
Procedure Number	Procedure Name	Applicability
1	S5/S8/S2b GTP Create Session	P-GW, ePDG, SaMOG
2	S5/S8/S2b GTP Create Bearer	P-GW, ePDG, SaMOG
3	S5/S8/S2b GTP Delete Session	P-GW, ePDG, SaMOG
4	S5/S8/S2b GTP Delete Bearer	P-GW, ePDG, SaMOG
5	GTP Modify Bearer	P-GW
6	S5/S8/S2b GTP Update Bearer	P-GW, ePDG, SaMOG
7	S6b/SWm – Diameter AAR/ AAA	P-GW, ePDG, SaMOG
8	S6b/SWm – Diameter RAR/RAA	P-GW, ePDG, SaMOG
9	S6b/SWm – Diameter Session Termination	P-GW, ePDG, SaMOG
10	S6b – Abort Session	P-GW, ePDG, SaMOG
11	Diameter Gx – CCR-I/CCA-I	P-GW
12	Diameter Gx – CCR-U/CCA-U	P-GW

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

RTT Record Schema

The following figure details the new RTT schema.

Figure 22: RTT Record Schema

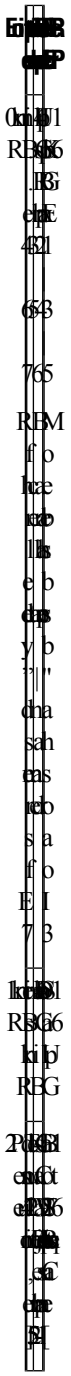


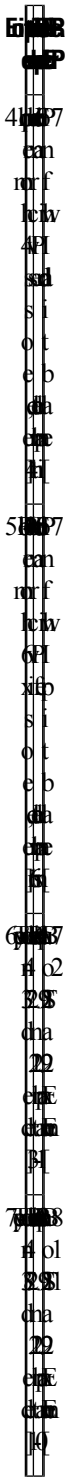
RTT schema has a Header and the following six blocks of Information Elements (IEs). There are totally 170 IEs that are grouped in 6 blocks. Contact your Cisco account representative for the complete list of RTT Record Schema IEs.

- Common IEs
- GPRS Tunneling Protocol (GTP) IEs. These IEs are existing and are re-used.
- Diameter IEs (new IEs)
- Proxy Mobile IPv6 IEs
- Internet Key Exchange (IKE)/ Internet Protocol Security (IPsec) IEs
- Internet Protocol v6 Router Advertisement (IPv6 RA IEs

Note IKE/IPSec and IPv6 RA IEs are new and they are contained inside new blocks. Diameter IEs are new and are appended to the existing Diameter IE blocks.

The RTT Record schemas are listed in the following table:





Configuring RTT for ePDG

This section provides RTT configuration information for ePDG.

Enabling RTT to Record and Produce Call Transactions

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

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

NOTES:

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

Configuring RTT

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

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

NOTES:

- **transfer-mode**: Enables the transfer mode in RTT.
- **push primary url**: Specifies the external server location where the records are transferred from ePDG.
- **file name**: Specifies the RTT file name where the records are stored.
- **rotation volume**: The volume based on which the RTT file is generated.

- **rotation time**: The time based on which the RTT file is generated.

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

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

Monitoring and Troubleshooting

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

Show Commands and Output

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

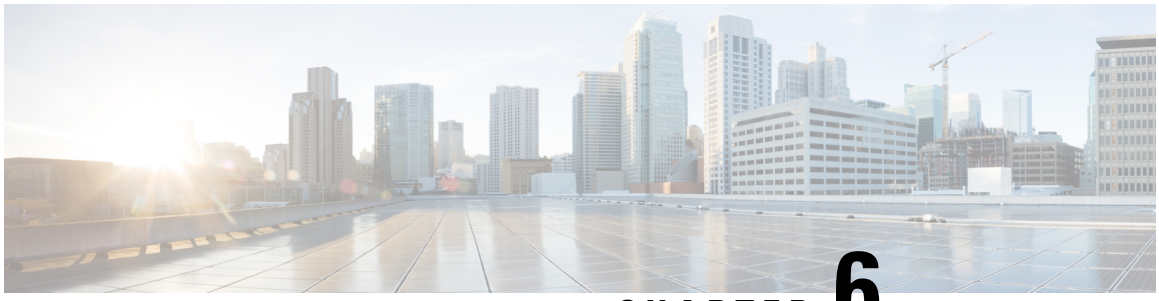
show Event-Record Statistics ePDG

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

Table 26: show event-record statistics ePDG Command Output Descriptions

Field	Description
Total Number of Event Records	The total number of event records (GTPv2 + Diameter + IKE + RA).
GTPv2 Event Records	The total number of GTPv2 records
CSR	The total number of CSR (Create Session Request) events.
CBR	The total number of CBR (Create Bearer Request) events.
DSR	The total number of DSR (Delete Session Request) events.
DBR	The total number of DBR (Delete Bearer Request) events.
UBR	The total number of UBR (Update Bearer Request) events.

Field	Description
IKEv2 Event Records	The total number of IKE events.
IKE_SA_INIT	The total number of IKE_SA_INIT events.
IKE_AUTH	The total number of IKE_AUTH events.
IKE_INFORMATION	The total number of IKE_INFORMATION events.
CREATE_CHILD_SA	The total number of CREATE_CHILD_SA events.
IPV6 RA Event Records	The total number of IPV6 RA event records.
RA Prefix	The total number of RA prefix events.
Diameter Event Records	The total number of Diameter event records.
SWm Procedures	The total number of SWm interface specific events.
AAR	The total number AAR (AA-Request) events.
RAR	The total number of RAR (Re-Auth-Request) events
ASR	The total number of ASR (Abort Session Request) events
STR	The total number of STR (Session Termination Request) events.
DER	The total number of DER (DE-Request) events.



CHAPTER 6

Custom S2B to SWu error code mapping

ePDG does supports mapping of S2B to SWu error codes so that device can identify whether it is temporary failure or permanent and can accordingly try connecting to the ePDG.

Description

The communication service providers (CSP) would like the ability to take different actions depending on the severity of the error received from the PGW (S2B interface). If there is a temporary congestion in the network, a retry is appropriate.

The ePDG needs mapping of S2B to SWu error codes for communicating different error codes to device, enabling device to identify whether its temporary failure or permanent and can accordingly try connecting to the ePDG.

The ePDG continues to release the call while notifying the UE about the S2B error, however the UE based on error code shall take decision when to try connecting again.

For the mapping ePDG uses Notify Error Message type between 31 to 8191 from the range reserved for IANA or from the private range 8192 to 16383.

Custom S2B to SWu error code mapping Configuration

Performance Indicator Changes

As part of " allow custom s2b-swu-error-mapping " feature below show commands output are introduced:

show epdg-service name

Service Name

- Custom S2b-SWu Error Mapping

show epdg-service statistics

GTP related reasons

- S2B Access Denied

- S2B Network Failure
- S2B Message Failure
- S2B RAT Disallowed

show session disconnect-reasons

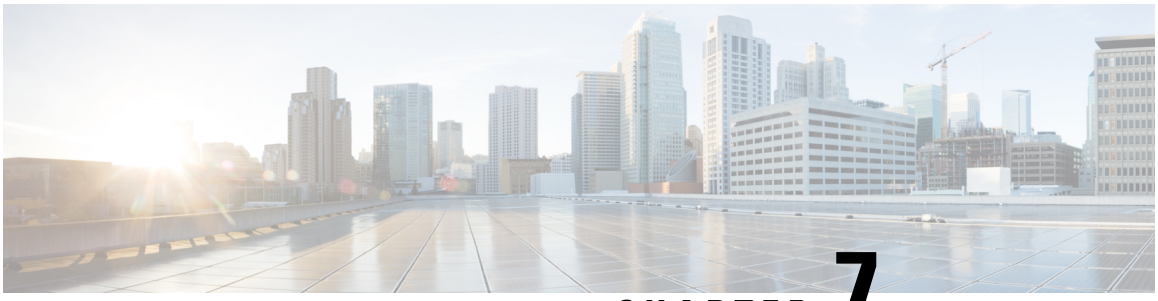
Session Disconnect Statistics

- ePDG-s2b-access-denied
- ePDG-s2b-network-failure
- ePDG-s2b-msg-failure
- ePDG-s2b-rat-disallowed

ePDG allow custom s2b-swu-error-mapping Support Bulkstats

Below Bulkstats are introduced in ePDG Schema to support s2b-swu-error-mapping Support feature:

- sess-disconnect-s2b-access-denied
- sess-disconnect-s2b-network-failure
- sess-disconnect-s2b-message-failure
- sess-disconnect-s2b-rat-disallowed



CHAPTER 7

EAP-PEAP/MSCHAPv2 Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	ASR 5500
Feature Default	Enabled - Always On
Related Changes in This Release	Not applicable
Related Documentation	*ePDG Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.3

Feature Changes

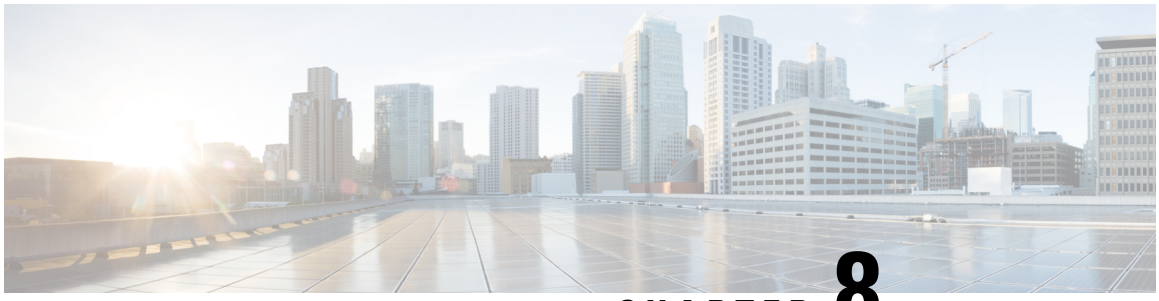
ePDG acts as Pass Through Node for Protected Extensible Authentication Protocol (PEAP). New counters have been added for EAP-PEAP/MSCHAPv2 authentication method.

Performance Indicator Changes

System Schema

The following new bulk statistics are added in the System schema to support EAP-PEAP/MSCHAPv2:

- ikev2-current-eap-peap-auth-method - Total number of current security associations with eap-peap auth method.
- ikev2-attempt-eap-peap-auth-method - Total number of security associations attempts with eap-peap auth method.
- ikev2-success-eap-peap-auth-method - Total number of successful security associations with eap-peap auth method.
- ikev2-failure-eap-peap-auth-method - Total number of security associations failures with eap-peap auth method.



CHAPTER 8

ePDG Auth Bulkstats for Non-UICC/UICC

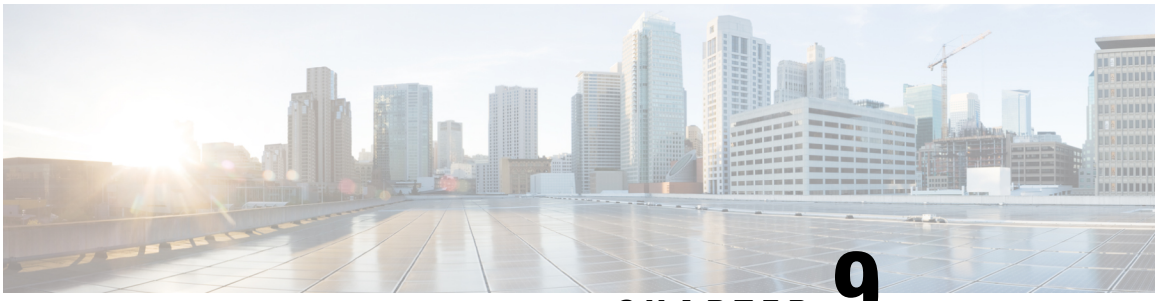
This chapter provides bulkstats related to non-UICC and UICC ePDG authentication.

Auth Bulkstats for Non-UICC/UICC

The following bulk statistics are added under System Schema as part of Non-UICC/UICC device support.

- ikev2-current-eap-aka-auth-method
- ikev2-attempt-eap-aka-auth-method
- ikev2-success-eap-aka-auth-method
- ikev2-failure-eap-aka-auth-method
- ikev2-current-eap-sim-auth-method
- ikev2-attempt-eap-sim-auth-method
- ikev2-success-eap-sim-auth-method
- ikev2-failure-eap-sim-auth-method
- ikev2-current-local-cert-auth-method
- ikev2-attempt-local-cert-auth-method
- ikev2-success-local-cert-auth-method
- ikev2-failure-local-cert-auth-method
- ikev2-current-remote-cert-auth-method
- ikev2-attempt-remote-cert-auth-method
- ikev2-success-remote-cert-auth-method
- ikev2-failure-remote-cert-auth-method
- ikev2-current-eap-tls-auth-method
- ikev2-attempt-eap-tls-auth-method

- ikev2-success-eap-tls-auth-method
- ikev2-failure-eap-tls-auth-method
- ikev2-current-eap-ttls-auth-method
- ikev2-attempt-eap-ttls-auth-method
- ikev2-success-eap-ttls-auth-method
- ikev2-failure-eap-ttls-auth-method
- ikev2-current-eap-mschapv2-auth-method
- ikev2-attempt-eap-mschapv2-auth-method
- ikev2-success-eap-mschapv2-auth-method
- ikev2-failure-eap-mschapv2-auth-method



CHAPTER 9

ePDG DDoS Attack Mitigation

This chapter describes the ePDG DDoS Attack Mitigation feature.

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

Revision History

Revision Details	**Release**
First introduced.	21.4

Feature Description

ePDG is a network element in EPC Core in the service provider LTE networks that terminates untrusted Wi-Fi. ePDG is reachable via public IP address from UE on UDP port 500/4500. ePDG services UEs from un-secure network making it vulnerable to a host of DDoS attacks. This feature mitigates various types of DDoS attacks.

This section describes high level events/alerts which ePDG mitigates:

UDP/IKE_INIT Decode failure

Attacker can send flood of UDP or IKE_INIT traffic on port 500/4500 from spoofed IP address(es) or compromised hosts (Botnet kind of attacks) from multiple hosts, which in turn will utilize system's CPU and memory, denying services to legitimate users.

No Response for INIT Cookie Challenge or No IKE_AUTH

Attacker can just chose to send valid IKE_INIT requests without sending IKE_AUTH requests for them. If DoS cookie is enabled in the system, and once the half open session hits the threshold. The ePDG will send cookie challenge to peer in order to check if peer is legitimate, but peer is just sending INITs and will not respond to cookie challenge.

All packets till Auth complete

ePDG can face variation of attacks after IKE_INIT transaction is done. Integrity Checksum failure of IKE_AUTH req, Decode Failure after decryption, high rate of junk packets (especially Auth Reqs), or authentication failure if all the subsequent packets are decrypted and decoded successfully.

Attack after Auth Complete

These attacks are result of installing malware, or hacking legitimate user's device. The attacks can be Integrity Check Value (ICV) failure or high data rate of control traffic. ICV failure will utilize CPU resources and high data rate can exhaust the system limit and denying services to legitimate user. High control traffic can include DPD, ike-sa rekey, ipsec-sa rekey, create-child sa req, delete-req etc.

Relationships to Other Features

SR/ICSR Recovery

- SR/Unplanned card migration, monitoring will start from first packet onwards and all data collected before SR/Card migration will be lost. Alarm raised earlier will not be cleared.
- Blockedlisting of IP address for multiple services of the same IP type is not supported.
- The Blockedlist IP address configuration is not supported at the boot time. It must be configured once the system is up and running.

How It Works

The ePDG threat detection and mitigation mechanism is implemented to mitigate multiple types of attacks. The following methods describe how to detect a threat from source IP.

UDP Flood / INIT Decode Failure Flood

- A context level failure threshold with upper and lower limit with interval in seconds is configured.
- If the higher threshold is met within the interval, then monitoring will start for each IP address with UDP/INIT packet drops. It will also raise an alarm/SNMP. The alarm will be cleared once the lower threshold is met in any subsequent duration. After the lower threshold is met, IP Address level monitoring will also be stopped.
- Once the upper threshold is met, an alarm/SNMP will be raised with relevant information. The alarm will be cleared for an IP once the lower threshold is met in any subsequent interval.
- Alarm is cleared in next interval once the operator configures the IP address to drop the packets at ipsec demux.

IKE_INIT Flood (no cookie response or no first IKE_AUTH):

- As the attacker can use multiple IP addresses, monitoring INIT storm per source IP address is required.
- A configurable threshold (upper and lower) count per source IP (and/or port) will be used to mark it suspicious and alarm will be raised so that operator can block the IP address.
- Not more than eight IKE_INIT packets should be forwarded to IPSec manager from a single source IP/Port/SPI-I and not more than 8 IKE_INIT with unique SPI_i should be forwarded to IPSec manager from a single Source IP/Port.

Note IPSec cookie configuration and Half-open SA lifetime reduction timeout configuration to mitigate IKE-INIT flood attack are already in place. This new implementation will be an additional way to mitigate the attack.

IKE_AUTH Flood (IKE_AUTH hmac failed or Decode Failed):

- After INIT Request/Response transaction is completed, attacker or device software issue can send flood of Junk IKE_AUTH. Due to which HMAC or decode will fail after decryption, and IMSI will not be available for the scenario.
- For this scenario, process only configured number of HMAC/Decode failures per IKESA. Then delete the session and raise an alarm.

IKE_AUTH Flood (All packets till Auth Complete, after IMSI is available):

- After INIT is completed, attacker can send IKE_AUTH packets on same SPI_i and SPI_r launch high rate of control traffic.
- This can either fail at decryption stage/decode phase
- IPSec manager needs to monitored:

- **Decryption decode fail count**: If threshold crosses the decryption failure, drop the ongoing session and raise an alarm.
- **Decode fail count**: This count only decodes after decryption. This will be counted towards Max IKE request allowed per interval
- **Max IKE request count**: If this request count crosses the threshold, drop ongoing session and raise an alarm

Attack after Auth Complete:

Monitoring Source IP/IMSI SNMP alarm is raised due to block/unblock of IP/IMSI, It will inform all IPSec managers so that once IMSI is available (after authentication) the session can be rejected with appropriate failure notify message.

- Alarm is raised after configured HMAC failure control threshold (upper/lower) fails
- **Control**

Note As part of ePDG DDoS Attack Mitigation Rekey Rate and Half Open Timer along with few other features are implemented. For more details, refer *IKEv2 Protection Against Distributed Denial of Service* of *IPSec Admin Guide*.

- Monitoring is with respect to decryption failure and maximum IKE request allowed per interval
- An alarm is raised once allowed maximum IKE_AUTH phase attempts per interval fails
- Number of IKE/IPSec Rekey per second is limited, notify failure is sent once limit is reached.

Configuring DDoS Attack Mitigation

This section describes the configuration of ePDG DDoS Attack Mitigation.

Configuring IKEv2 Request Rate

Use the following configuration to configure IKEv2 request rate in an interval.

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
     ikev2-ikesa ddos ikev2-req-rate ikev2_req_rate_count [ interval interval
]
      { no | default } ikev2-ikesa ddos ikev2-req-rate
      end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association parameters.
- **ddos**: Configures the IKEv2 DDos mitigation parameters.

- **ikev2-req-rate** *ikev2_req_rate_count*: Configures the maximum number of IKEv2 requests allowed per configured interval. *ikev2_req_rate_count* must be an integer from 1 to 3000.

  Default: 10

- **interval** *interval* : Configures the interval for monitoring IKEv2 requests. *interval* must be an integer from 1 to 300.

  Default: 1 second

- **no**: Disables the IKEv2 request count.
- **default**: Sets the default value of the IKEv2 request count.

Configuring INIT Floods

Use the below configuration to configure init flood:

```
configure
   context context_name
      ikev2-ikesa ddos init-flood { source-based | system-based } [
threshold-upper threshold_upper_value  [ threshold-lower threshold_lower_value [
poll-timer-duration poll_timer_duration_value ] ] ]
     { default | no } ikev2-ikesa ddos init-flood { source-based |
system-based }
     end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association Parameters.
- **ddos**: Configures the IKEv2 DDos mitigation parameters.
- **init-flood**: Specifies the IKEv2 DDoS mitigation parameters for INIT Floods.
- **source-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at source IP address level.

  threshold-upper *threshold_upper_value*: Configures upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 100 to 4294967295. Default: 10000.

  threshold-lower *threshold_lower_value*: Configures lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 50 to 4294967294. Default: 5000.

  poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS INIT Floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 30 to 3600. Default: 60 seconds.

- **system-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at system level.

  threshold-upper *threshold_upper_value*: Configures the upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 1000 to 4294967295. Default: 100000.

threshold-lower *threshold_lower_value*: Configures the lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 500 to 4294967294. Default: 50000.

poll-timer-duration *poll_timer_duration_value*: Configures the IKEv2 DDoS INIT floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 60 to 3600. Default: 60 seconds.

- **no**: Removes IKEv2 DDoS mitigation parameters for INIT Floods.
- **default**: Sets the default values for IKEv2 DDoS mitigation parameters for INIT Floods.

Configuring Source Identifiers to Blockedlist

Use the following configuration to configure source identifiers to blacklist :

```
configure
   context context_name
      [ no ] ikev2-ikesa ddos blacklist ip-address ipv4_address | ipv6_address
      end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association parameters.
- **ddos**: Configures IKEv2 DDoS mitigation Parameters.
- **blacklist**: Configures the source identifiers to blacklist.
- **ip-address** *ipv4_address* | *ipv6_address*: Configures the source IPv4 or IPv6 address to be blacklisted.
- **no**: Removes the DDoS blacklist configuration.

Configuring UDP Errors

Use the below configuration to configure UDP errors:

```
configure
   context context_name
      ikev2-ikesa ddos udp-error { source-based | system-based } [
threshold-upper threshold_upper_value [ threshold-lower threshold_lower_value [
poll-timer-duration poll_timer_duration_value ] ] ]
      { default | no } ikev2-ikesa ddos udp-error { source-based |
system-based }
      end
```

Notes:

- **ikev2-ikesa**: Configures IKEv2 IKE Security Association Parameters.
- **udp-error**: Specifies IKEv2 DDoS mitigation parameters for UDP errors.
- **source-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for UDP errors applicable at source IP address level.

threshold-upper *threshold_upper_value*: Configures the upper threshold value for error, after which alarm will be raised. *threshold_upper_value* must be an integer from 100 to 4294967295. Default: 10000.

threshold-lower *threshold_lower_value*: Configures the lower threshold value for error, after which alarm will be cleared. *threshold_lower_value* must be an integer from 50 to 4294967294. Default: 5000.

poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS UDP errors timer duration in seconds. *poll_timer_duration_value* must be an integer from 30 to 3600. Default: 60 seconds.

- **system-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for UDP errors applicable at system level.

  threshold-upper *threshold_upper_value*: Configures upper threshold value for error, after which alarm will be raised. *threshold_upper_value* must be an integer from 1000 to 4294967295. Default: 100000.

  threshold-lower *threshold_lower_value*: Configures lower threshold value for error, after which alarm will be cleared. *threshold_lower_value* must be an integer from 500 to 4294967294. Default: 50000.

  poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS UDP errors timer duration in seconds. *poll_timer_duration_value* must be an integer from 60 to 3600. Default: 60 seconds.

- **no**: Removes IKEv2 DDoS mitigation parameters for UDP errors.
- **default**: Sets the default values for IKEv2 DDoS mitigation parameters for UDP errors.

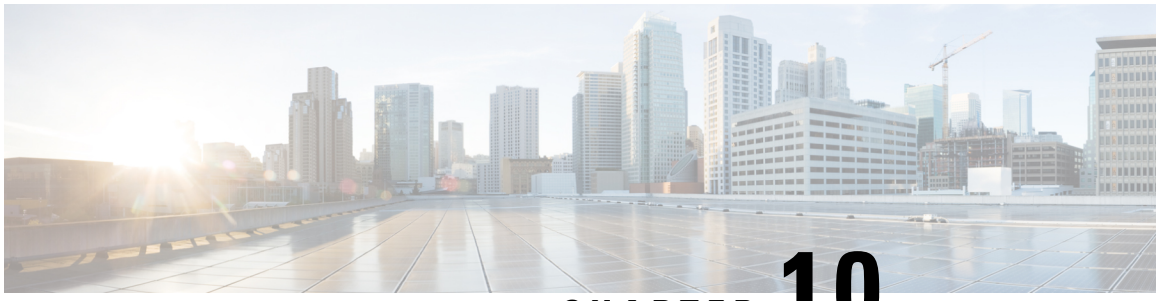
Monitoring and Troubleshooting

This section provides information on alarms and thresholds for the DDoS Attack Mitigation feature.

Alarms and Thresholds

The following alarms are added in support of this feature:

- IKEv2DDOSAttackUDPFail
- IKEv2DDOSAttackUDPFailClear
- IKEv2DDOSAttackUDPPeerFail
- IKEv2DDOSAttackUDPPeerFailClear
- IKEv2DDOSAttackINITFlood
- IKEv2DDOSAttackINITFloodClear
- IKEv2DDOSAttackINITPeerFlood
- IKEv2DDOSAttackINITPeerFloodClear
- IKEv2ReqRateThreshold
- IKEv2ClearReqRateThreshold



CHAPTER 10

ePDG IMSI Privacy Support

This chapter describes the ePDG IMSI Privacy Support feature.

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

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

The IMSI Privacy feature protects the exposure of IMSI to the untrusted ePDG and shares it only after it has authenticated the ePDG.

How it Works

1. ePDG decodes and processes the string anonymous or any configured value received in IDi payload in IKE_AUTH request.
2. ePDG then responds with IKE AUTH response which includes the ePDG server certificate along with the authentication payload.
3. The client can be configured to send a CERTREQ in the IKE AUTH request if required. In addition to the ePDG server certificate, the IKEv2 server initiates an EAP Identity request towards the IKEv2 client.
4. The IKEv2 client authenticates the server using the certificate and provides the IMSI in the EAP Identity response.
5. The same EAP Payload (EAP response) will be forwarded to AAA with the first Diameter EAP Request. Rest of the call flow for ePDG remains the same.

Configuring IMSI Privacy Support

This section describes the configuration of IMSI Privacy.

Configuring IDI

Use the following configuration to match IDI from peer which enables the ePDG to request the real identity using EAP-Identity Request.

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
      ikev2-ikesa idi peer_idi_value request-eap-identity
      no ikev2-ikesa idi peer_idi_value
      end
```

Notes:

- **crypto template** *template_name*: Configures the context level name to be used to identify the Crypto Template. *template_name* is string of size 1 to 104.
- **ikev2-dynamic**: Configures the parameters for IKEv2 Security Associations derived from this Crypto Template.
- **idi** *peer_idi_value*: Specifies the IDI related configuration. *peer_idi_value* is a string of size 1 to 127.
- **request-eap-identity**: Requests EAP-Identity from peer.

- **no**: Disables the peer IDI value.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot the IMSI Privacy feature.

Show Commands and Outputs

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

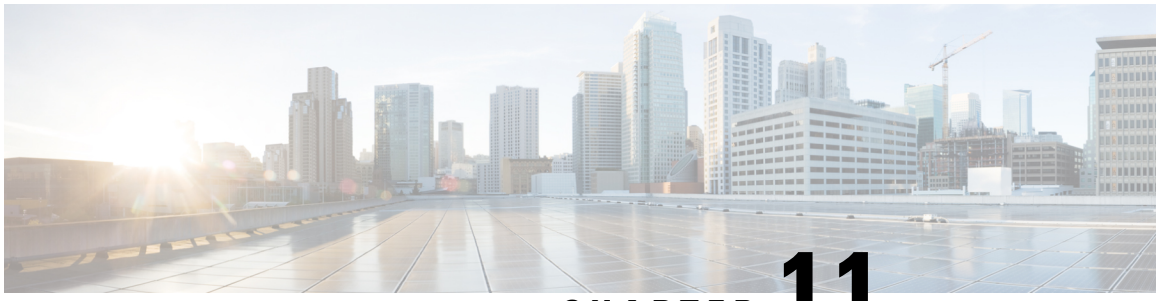
show crypto statistics ikev2

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

- EAP-Identity Req Sent

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

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



CHAPTER 11

ePDG International Roaming - Redirection Based on Outer IP

RFC 5685 defines an IKEv2 extension i.e IKEv2 Redirect that allows an ePDG to redirect current ongoing Ikev2 exchange to some other ePDG.

Feature Description

Only one or some explicit ePDG will be handling International Roaming users, not all. When UE attaches to WIFI, public DNS server can be initially route to any ePDG randomly. If initial ePDG finds out that it is an international user, it will route it using IKEv2 redirect mechanism to corresponding ePDG which handles International Roaming Users.

Note Basic Ikev2-Redirect support on ePDG is already present, this feature will use existing Staros Ikev2 redirect framework to redirect all International Roaming users to specific ePDG.

Assumptions and Limitations:

- Zone matching done by matching zone configured with MIP6 AVP removing configured/default strip levels as per requirement
- Initial ePDG will expect that AAA responce with PGW FQDN in DEA message for all International Roaming users to be redirected to specific configured ePDG
- International roaming user will be redirected to proper ePDG, PGW FQDN comes from AAA and matching zone configured under gateway-selection-profile

Configuring ePDG International Roaming Redirection Based on Outer IP

Use the following configuration to ePDG International Roaming Redirection Based on Outer IP.

Below are the newly introduced commands for the ePDG International Roaming Redirection Based on Outer IP

gateway selection profile

```
config
        gateway-selection-profile  profile_name
          end
```

description

```
config
    context context_name
        gateway-selection-profile  profile_name
            description   descriptive_string
          end
```

zone

```
config
    context context_name
        gateway-selection-profile  profile_name
            zone   zone_fqdn  action { ignore | mandatory }
          end
```

associate gateway-selection-profile

```
config
        gateway-selection-profile  profile_name
            associate gateway-selection-profile  profile_name
          end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature to support ePDG International Roaming-Redirection based on outer IP.

show apn-profile full all

- Associated Gateway Selection Profile

show gateway-selection-profile all

- epdg_gwsel_profile1

show gateway-selection-profile full all

- Gateway Selection Profile Name

- Details of zones configured
- zone <yyyy> action ignore
- zone <zzzz> action mandate
- Total 2 zones configured

show epdg statistics

- Zone Action Ignore Configured:

  Zone Matching stats:

- Mandatory:

  Session Disconnect reason:

- Roaming Mandatory:

show sessctrl config-reconciliation statistics

Task	Config-type
Sessmgr	gw-selection profile

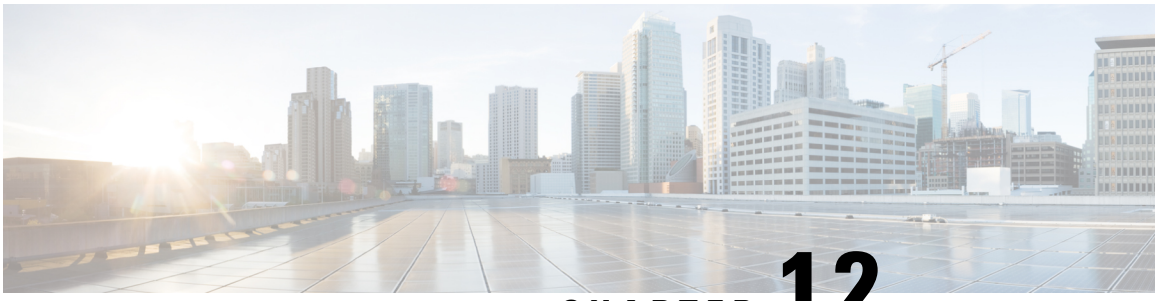
show session disconnect-reasons

Disconnect Reason	Num Disc	Percentage
ePDG-roaming-mandatory		

Bulkstats

Below are the new bulkstats introduced in ePDG Schema as part of ePDG International Roaming-Redirection based on outer IP.

- sess-disconnect-roaming-mandatory
- alt-epdg-selection-mandatory
- redirect-zone-action-ignored



CHAPTER 12

ePDG Interworking with SMF+P-GW-IWK Support

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release

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

Feature Description

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

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

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

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

License Requirements

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

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

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

Standards Compliance

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

3GPP References

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

How it Works

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

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

Call Flow

Figure 23: ePDG Setup Procedure Call Flow

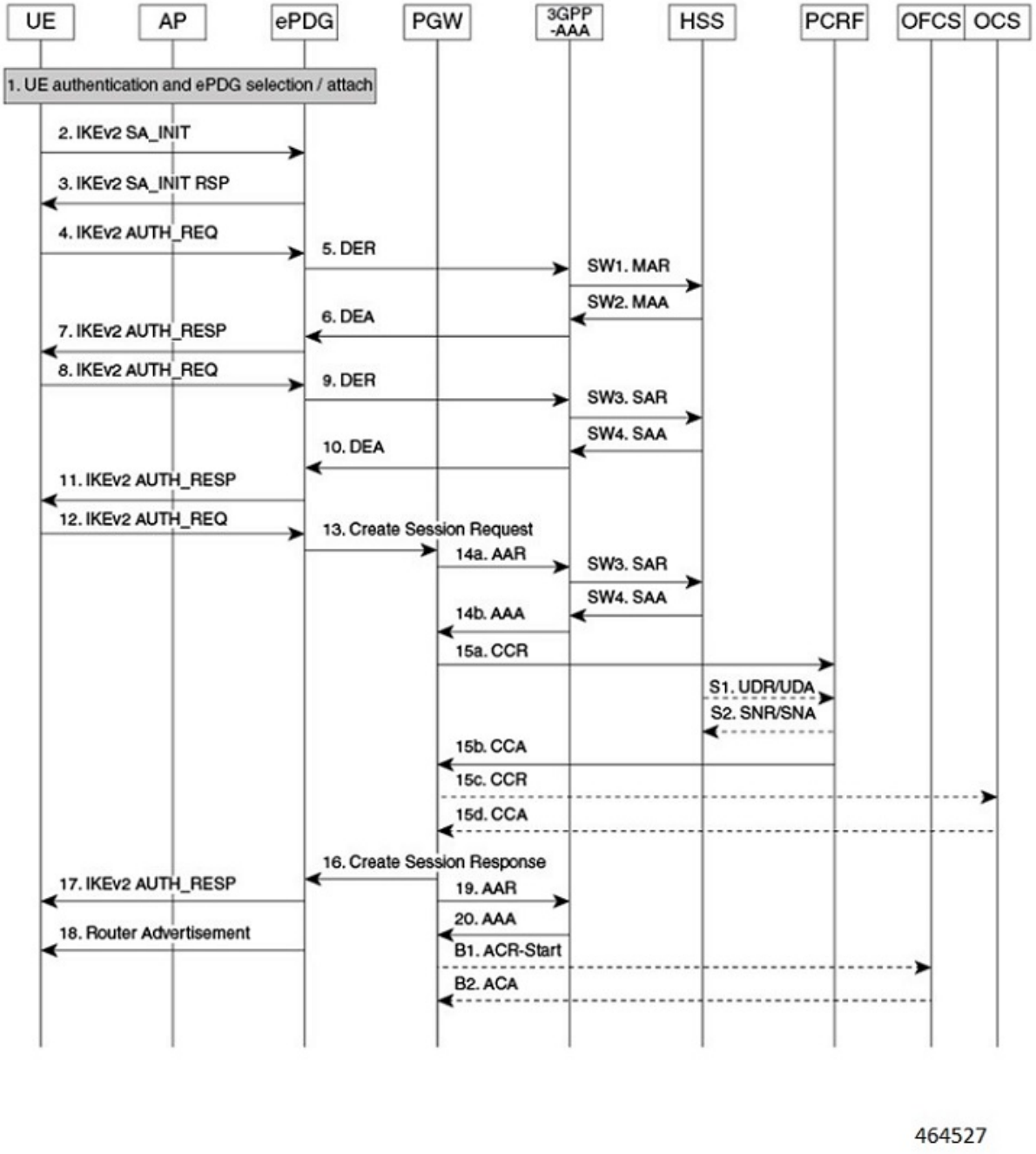


Table 27: ePDG Setup Procedure Call Flow Description

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

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

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

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

Information Element and AVP Support

This feature supports the following IE and AVPs:

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

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

PDU Session ID

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

S-NSSAI

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

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

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

Core-Network-Restrictions

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

The following table explains the bits:

Table 28: Meaning of Bits

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

Interworking-5GS-Indicator

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

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

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

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

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

5GSIWKI Indicator Flag

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

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

5GCNRS Flag

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

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

5GCNRI Flag

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

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

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

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

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

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

Figure 24: P-GW or SMF+PGW-IWK Decision Matrix Table

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

464608

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

NOTE 1:

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

NOTE 2:

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

NOTE 3:

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

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

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

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

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

Fallback Mechanism for Selecting Combined SMF+PGW-IWK

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

Table 29: Fallback Mechanism

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

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

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

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

Limitations

This feature has the following limitations:

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

Configuring ePDG to Enable 5G Interworking

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

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

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

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

NOTES:

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

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

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

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

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

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

```
configure
    context context_name
```

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

NOTES:

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

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

Configuring ePDG to Consider Interworking-5GS-Indicator

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

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

NOTES:

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

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

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

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

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

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

NOTES:

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

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

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

Configuring ePDG in the Local SMF+PGW-IWK Node

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

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

NOTES:

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

Configuring ePDG 5G Interworking Bulk Statistics

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

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

NOTES:

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

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show epdg-service statistics interworking-5g

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

Table 30: show epdg-service statistics interworking-5g Command Output Descriptions

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

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

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

show configuration

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

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

The following is a sample output:

```
config
cli hidden
tech-support test-commands encrypted password ***
....
.....
epdg-service epdg1
plmn id mcc 242 mnc 002
associate egtp-service egtp-epdg-egress-v4
ebi range start 10 end 13
pgw-selection agent-info error-terminate
dns-pgw selection topology weight
associate qci-qos-mapping epdg_mapping
```

```
associate subscriber-map map1
associate lte-emergency-profile emergency
username check-mac-address failure-handling continue
reporting-action event-record
max-sessions 100000
bind address 111.111.11.2 crypto-template boston
interworking-5g
pgw-selection select pgw 4gonly-ue
pgw-selection select pgw no-5gs-interworking
pgw-selection select pgw smf-not-configured
#exit
```

show epdg-service name

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

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

The following is a sample output:

```
Service name: epdg1
Context: pdif
Bind: Done
Max Sessions : 100000
IP address: 111.111.11.2 UDP Port : 500
Crypto-template: boston
Reporting Action:
Event Record: Enabled
Service State: Started Service Id: 6
EGTP service : egtp-epdg-egress-v4
MAG service : n/a
MAG context : n/a
PLMN Id: MCC:242 , MNC:002
Setup Timeout (sec) : 60
dns-pgw context: pdif
dns-pgw selection : weight,topology
fqdn: n/a
pgw-selection agent-info error-handling: terminate
pgw-selection select PGW: 4G Only UE, No 5GS Interworking, SMF Not Configured
Custom SWm-SWu Error Mapping: Disabled
Custom S2b-SWu Error Mapping: Disabled
3GPP SWu Private Notify Error Types: Disabled
Preferred PGW selection mechanism: AAA/DNS
vendor-specific-attr dns-server-req: APCO
vendor-specific-attr pcscf-server-req: Private Extension
Username MAC Address Stripping : Disabled
QCI QOS Mapping Table : epdg_mapping
Username MAC Address Validate : Enabled Failure-handling : Continue
Newcall Policy : None
Duplicate precedence in TFT - Allowed
IP Fragment-Chain Timeout : 5 sec and Max OOO Fragment : 45
```

```
EBI :
Allowed Range 10 to 13
Username MAC Address Delimiter - colon-or-NAI-Label
Subscriber Map : map1
AAA Send Framed-MTU Size : Disabled
Data Buffering : Enabled
PDN-type IPv6 Path-MTU : Enabled
GTPC Overload Control Profile : None
GTPC Load Control Profile: None
LTE Emergency Profile: emergency
Timeout Idle : Disabled
Suppress International Roamer Handover : Disabled
5G Interworking : Enabled
```

Bulk Statistics

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

show bulkstats variables epdg-interworking-5g

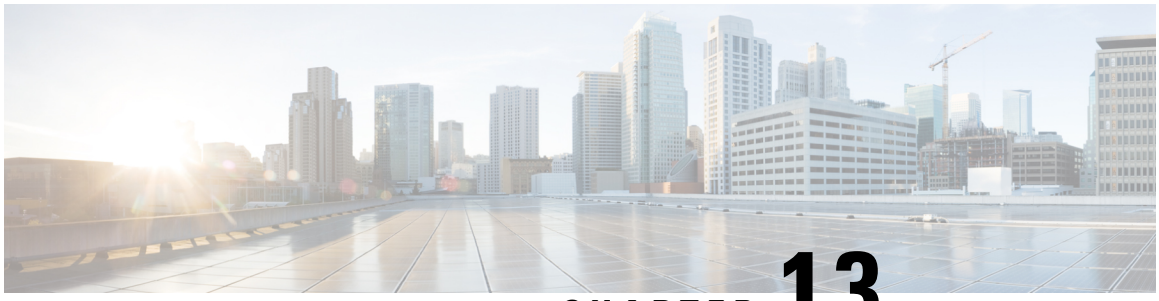
Use this command to display the list of bulk statistics variables supported by **epdg-interworking-5g schema**.

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

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

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

iwk5g-dns-no-matching-smf-service	The number of times that the DNS server responded with no SMFs in the resource records, when SMF is the preferred gateway for the session.
iwk5g-dns-pgw-list-exhausted	The number of times that P-GW provided by DNS response failed to connect, when P-GW is the preferred gateway for the session.
iwk5g-dns-smf-list-exhausted	The number of times that SMF provided by DNS response failed to connect, when SMF is the preferred gateway for the session.



CHAPTER 13

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.

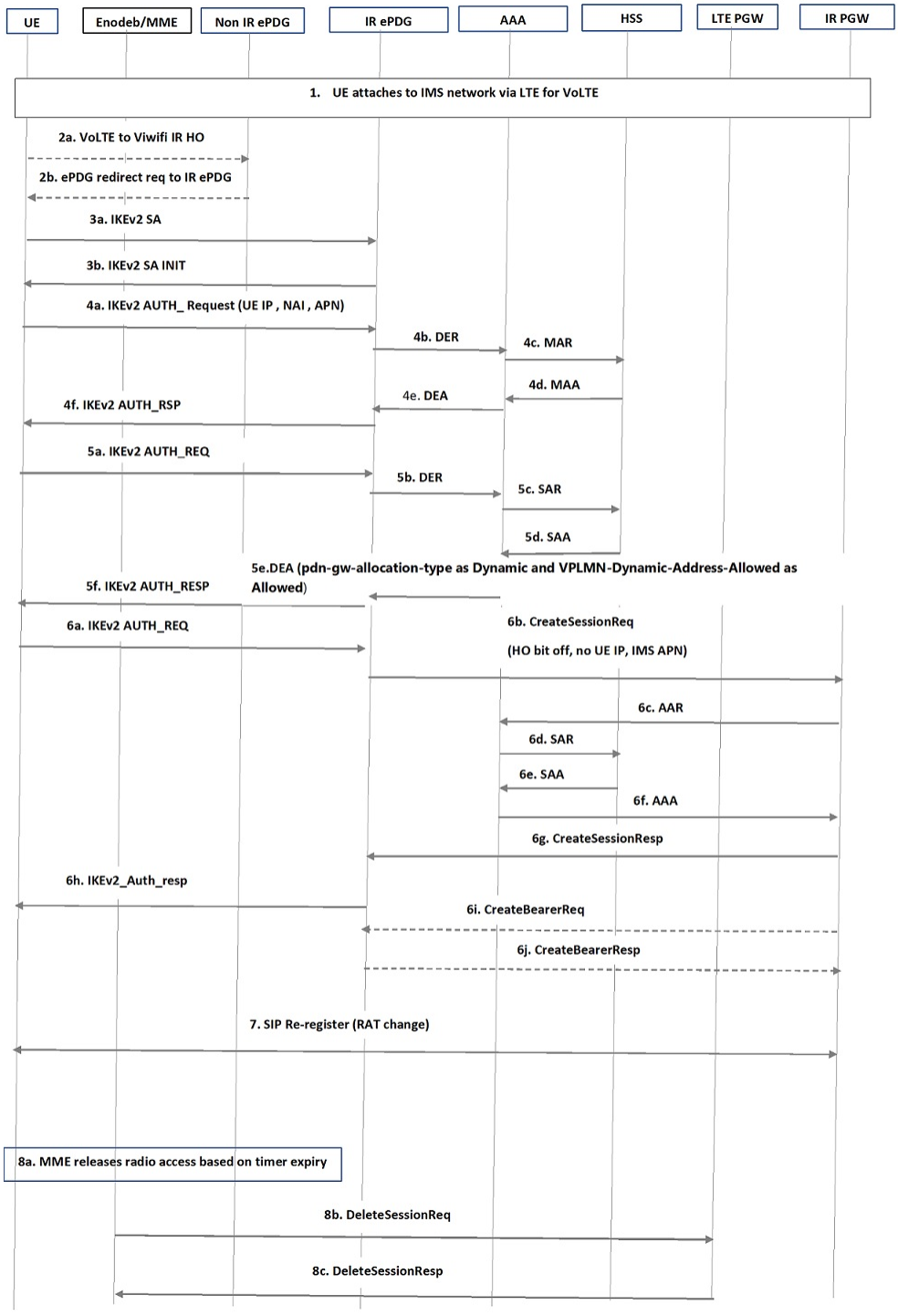
Enabling the CLI in normal ePDG impacts the normal ePDG HO call flows. The following warning message is displayed on enabling the feature:

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 25: 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*

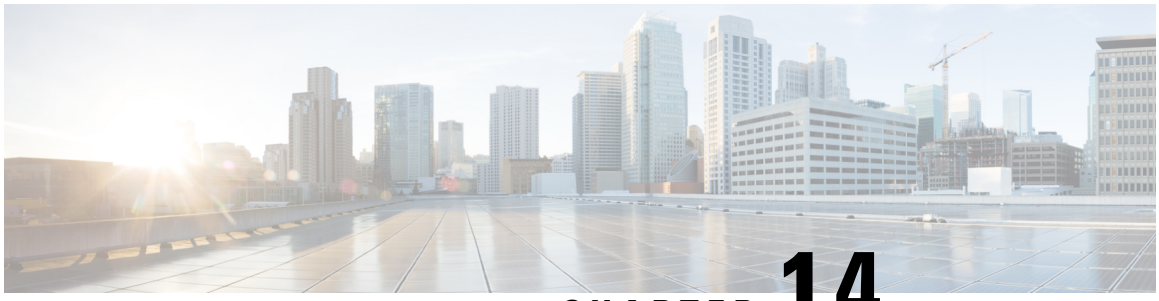
The output of this command includes the following fields to check whether IR suppress handover is enabled or disabled.

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 14

ePDG MOBIKE Support

Feature Summary and Revision History

Summary Data

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

Revision History

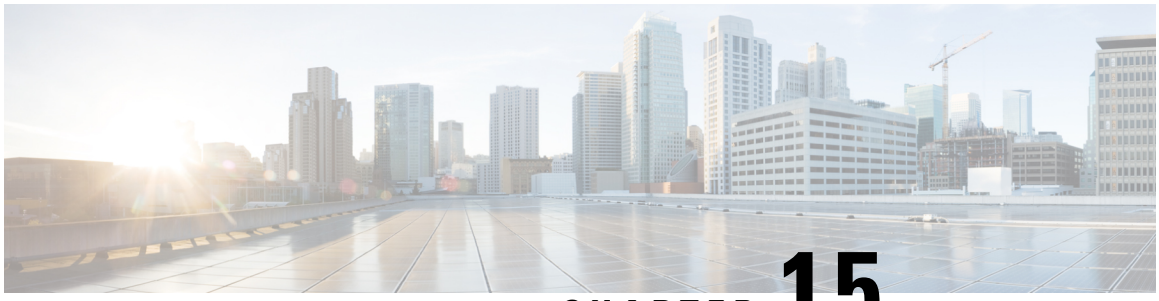
Important Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
First introduced.	21.3

Feature Changes

The IKEv2 Mobility and Multi-homing protocol (MOBIKE) is supported on ePDG/IPSec as defined in RFC 4555. MOBIKE allows the IP addresses associated with IKEv2 and tunnel mode IPSec Security Associations (SA) to change. This enables peer hosts to change its point of network attachment and use different interfaces without removing the existing IPSec tunnel.

MOBIKE feature is supported only on ASR 5500 and Ultra Services platforms.



CHAPTER 15

ePDG Modify Bearer Command Support

The Modify Bearer Command (MBC) is sent on the S2b interface by ePDG to PGW as part of the HSS Initiated Subscribed QoS Modification procedure. ePDG receives the modified QoS from 3gpp-AAA in Authorization-Authentication-Answer (AAA) message during AAA/ePDG initiated re-authorization procedure. If QCI and/or ARP and/or subscribed APN-AMBR changes, MBC is triggered. Please note that it is sent only for default bearer. Upon receiving it, PGW will send Update Bearer Request. Handling of update bearer request on ePDG will not be changed. If QoS modification fails on PGW, it will send Modify Bearer Failure Indication to ePDG. The ePDG will not take any action on it. ePDG will generate LI event regarding failure indication.

Description

Modify Bearer Command (MBC) to PGW

1. MBC is sent on S2b interface by the ePDG to the PGW as part of the HSS Initiated Subscribed QoS Modification procedure.
2. It is done as part of 3GPP-AAA or ePDG initiated Re-authorization procedure.
3. In Authorization Authenticate Answer message, if result is DIAMETER_SUCCESS, AAA sends APN-Configuration AVP which will contain AMBR and EPS-Subscribed-QoS Profile.
4. If ambr or QoS value is changed, then MBC is sent to PGW, to start Update Bearer Request procedure.

Modify Bearer Failure Indication from PGW (MBC) to PGW

1. MBC is sent on S2b interface by the ePDG to the PGW as part of the HSS Initiated Subscribed QoS Modification procedure.
2. It is done as part of 3GPP-AAA or ePDG initiated Re-authorization procedure.
3. In Authorization Authenticate Answer message, if result is DIAMETER_SUCCESS, AAA sends APN-Configuration AVP which will contain AMBR and EPS-Subscribed-QoS Profile.
4. If ambr or QoS value is changed, then MBC is sent to PGW, to start Update Bearer Request procedure.
5. If PGW is not able to update AMBR or QoS (may be due to PCC infra), then it will send Modify Bearer Failure Indication to ePDG.

6. There is no action defined if ePDG receives Modify Bearer Failure Indication.

Scope and Assumptions

- MBC is sent only for default bearer update for apn-ambr or qci or arp update.
- This feature is enabled by default.
- There is no failure handling needed for Modify Bearer Failure Indication received if PGW is not able to update QoS profile.
- There is no change required to current implementation of Update Bearer Request and Update Bearer Response procedure handling on ePDG.
- There is no change required to current implementation of RAR/RAA and AAR/AAA message handling on ePDG.
- No SR / ICSR changes is required, as the final outcome for this feature is Update Beare Req/Rsp, which is already supported.

ePDG Modify Bearer Command Support Configuration

As part of ePDG Modify Bearer Command Support feature below show commands output used: **show egtpc statistics interfae epdg-egress**

Modify Barer Command

- Total TX
- Total RX
- Initial TX
- Initial RX
- Retrans TX
- Retrans RX
- Discarded
- No Rsp RX

Modify Bearer Failure Indication:

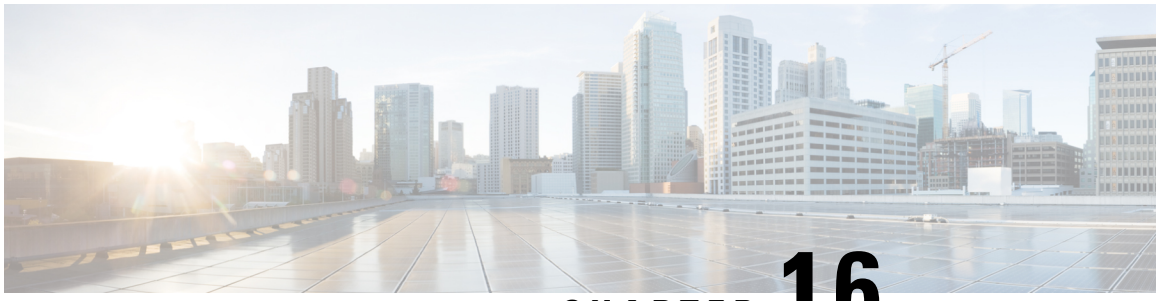
- Total TX
- Total RX
- Initial TX
- Initial RX
- Retrans TX
- Discarded

As part of ePDG Modify Bearer Command Support feature below stat is added in ePDG and ePDG APN Schema:

- sess-disconnect-s2b-context-not-found

As part of ePDG Modify Bearer Command Support feature below disconnect reason is added:

- Gtpv2-context-not-found(627)



CHAPTER 16

ePDG P-CSCF Restoration Support

Feature Information

Summary Data

Status:	New Feature
Introduced-In Release:	21.2
Modified-In Release(s):	ePDG
Applicable Product(s):	Cisco ASR 5500, VPC-SI, VPC-DI, UGP
Customer Specific:	No
Default Setting:	Disabled
CDETS ID(s)	CSCvc97504
Related Changes in this Release:	NA
Related Documentation:	ePDG Admin Guide, CLI Ref Guide and RCR

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

ePDG supports P-CSCF restoration on ePDG(Swu and S2b interface). P-CSCF restoration procedures designed to minimize the time a UE is unreachable for terminating calls after a P-CSCF failure.

P-CSCF restoration generally consists one of the below two ways:

1. Basic mechanism that makes use of a path through HSS/PCRF and PGW to request the release of the IMS PDN connection to the corresponding UE
2. An optional extension that avoids the IMS PDN deactivation and re-activation.

Key functionality of P-CSCF Restoration Support on ePDG:

- Processing of P-CSCF_RESELECTION_SUPPORT Notify payload in IKE-AUTH which when present indicates that the UE supports the P-CSCF restoration extension for untrusted WLAN
- Forwarding of UE capability (i.e. UE support of the P-CSCF restoration extension) in the APCO information element to the PGW over the S2b interface at the IMS PDN connection establishment (or handover) over S2b
- Handling of the updated addresses list of available P-CSCFs towards the UE sent by PGW, using the APCO IE in Update Bearer Req and sending Update Bearer Resp after procedure completion
- Forwading the updated P-CSCF addresses received from PGW to UE in the CFG_REQUEST configuration payload within the INFORMATIONAL request and handling UE's CFG_REPLY Configuration Payload in INFORMATIONAL response
- Handling of cause "Reactivation requested" over S2b in Delete Bearer Request & as a result include REACTIVATION_REQUESTED_CAUSE Notify payload in the INFORMATIONAL request message containing a DELETE payload sent to UE

Use cases for ePDG P-CSCF restoration support

This section describes solutions to support P-CSCF restoration for UEs with WLAN access.

There are two existing mechanisms to handle the P-CSCF restoration support as there are with E-UTRAN access.

- The basic mechanism for the HSS-based solution and for the PCRF-based solution relies on the release of the PDN connection followed by its re-establishment to trigger a new IMS registration by the UE
- The extension mechanism untrusted WLAN accesses to avoid the release of the PDN connection and to trigger a new IMS registration by the UE over the existing PDN connection. The extensions between the UE and the PGW are common for the HSS-based and for the PCRF-based solutions and rely on the same UE behavior

Basic PCSCF Restoration Support For an untrusted WLAN access, on S2b interface the PGW initiates a Delete Bearer Request procedure (GTP) or a Proxy Mobile IPv6 LMA Initiated PDN Connection Deletion procedure (PMIP) to the ePDG which then initiates the release of the associated IKEv2 tunnel. A cause "reactivation requested" (as supported over 3GPP accesses) is added by the PGW over GTP-C based S2b and IKEv2 for untrusted WLAN

As a result of the release of the IMS PDN connection, the UE re-establishes the IMS PDN connection, and also perform a new P-CSCF discovery (as the IMS PDN connection was lost). After discovering a new P-CSCF, the UE will perform a new initial IMS registration towards IMS.

Extended PCSCF Restoration Support An ePDG which supports the P-CSCF restoration extension for untrusted WLAN forwards the UE capability (i.e. UE support of the P-CSCF restoration extension) in the APCO information element to the PGW over the S2b interface at the PDN connection establishment (or handover) over S2b.

Note The receipt by the PGW of the UE capability indicating the support of P-CSCF restoration for the untrusted WLAN access at the PDN connection establishment (or handover) over the untrusted WLAN access serves also as an indication that the ePDG supports this procedure.

In the P-CSCF restoration extension procedure for untrusted WLAN access, the PGW sends the updated list of the addresses of available P-CSCFs towards the UE via the ePDG, using the APCO IE in Update Bearer Request message. Same will be communicated to UE via Configuration payload in Information request message.

Assumptions and Limitations

1. P-CSCF restoration is valid only for GTP interface.(PMIP not covered.)
2. P-CSCF restoration in ICSR downgrade will return “success” message, which is not a correct message, but PGW will treat it as restoration is successful and will not further send DSR, which ideally should be the case.

Flows

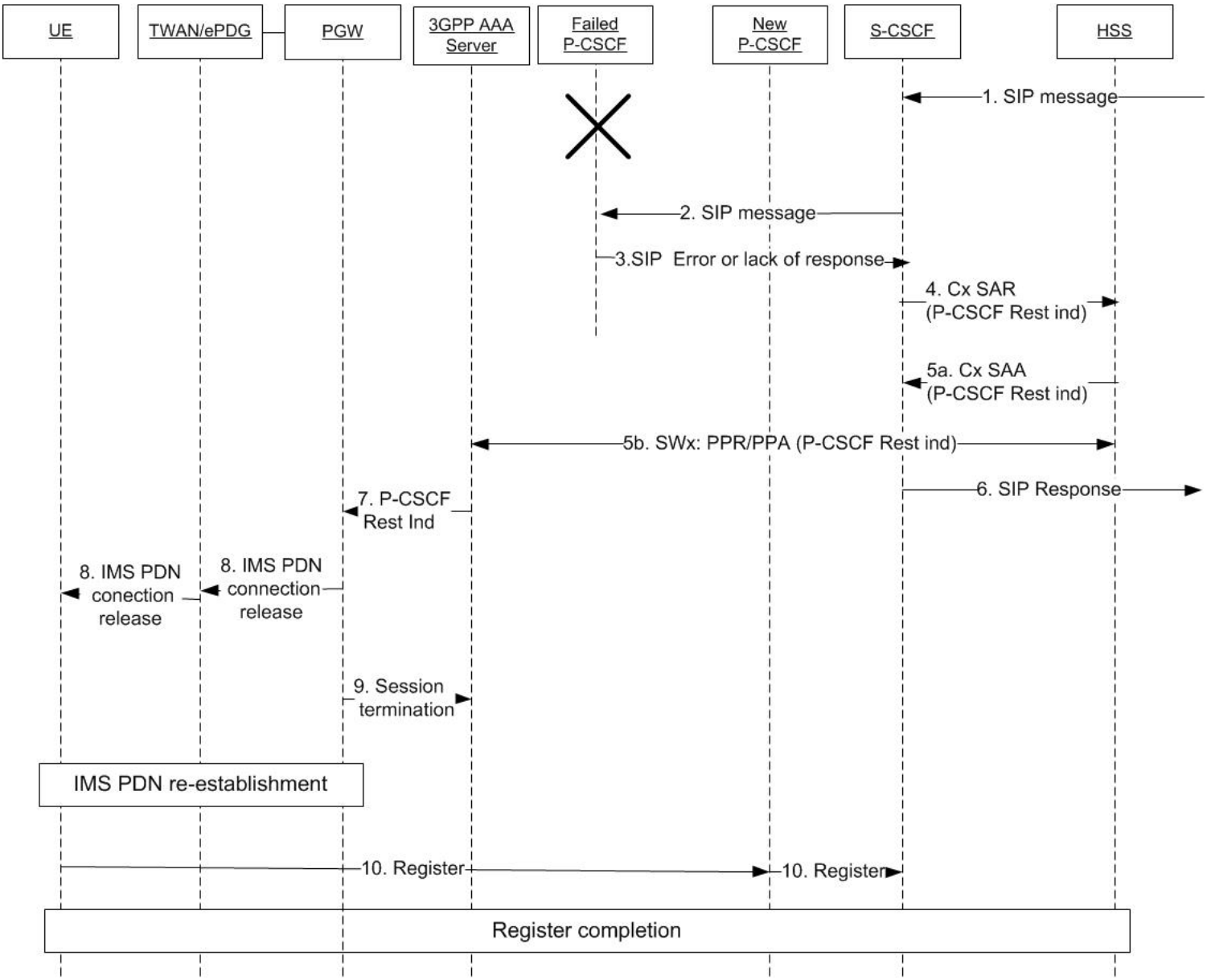
Basic Restoration Mechanism

HSS-based/PCRF-based basic mechanisms displayed in the below is based on the same principles i.e to disconnect the UE when P-CSCF failure is detected, which then re-establishes the connection via an alternate available P-CSCF.

Both the mechanisms have the same effect in ePDG, which will be handling PGW initiated Delete Bearer Request procedure (GTP) with cause "reactivation requested" (as supported over 3GPP accesses) and then translate it over IKEv2 (SWu) INFORMATIONAL request message containing DELETE payload with REACTIVATION_REQUESTED_CAUSE Notify payload towards UE resulting in deactivation.

After deactivation it is up to the UE to re-establish a new IMS PDN connection and performs a new P-CSCF discovery.

Figure 26: HSS based basic P-CSCF restoration for WLAN



Extended Restoration Mechanism

This mechanism aims to avoid the IMS PDN deactivation and re-activation, by introducing a update procedure to inform the UE about the change in P-CSCF address. This triggers the UE to initiate a new IMS registration towards an available P-CSCF over the existing IMS PDN connection.

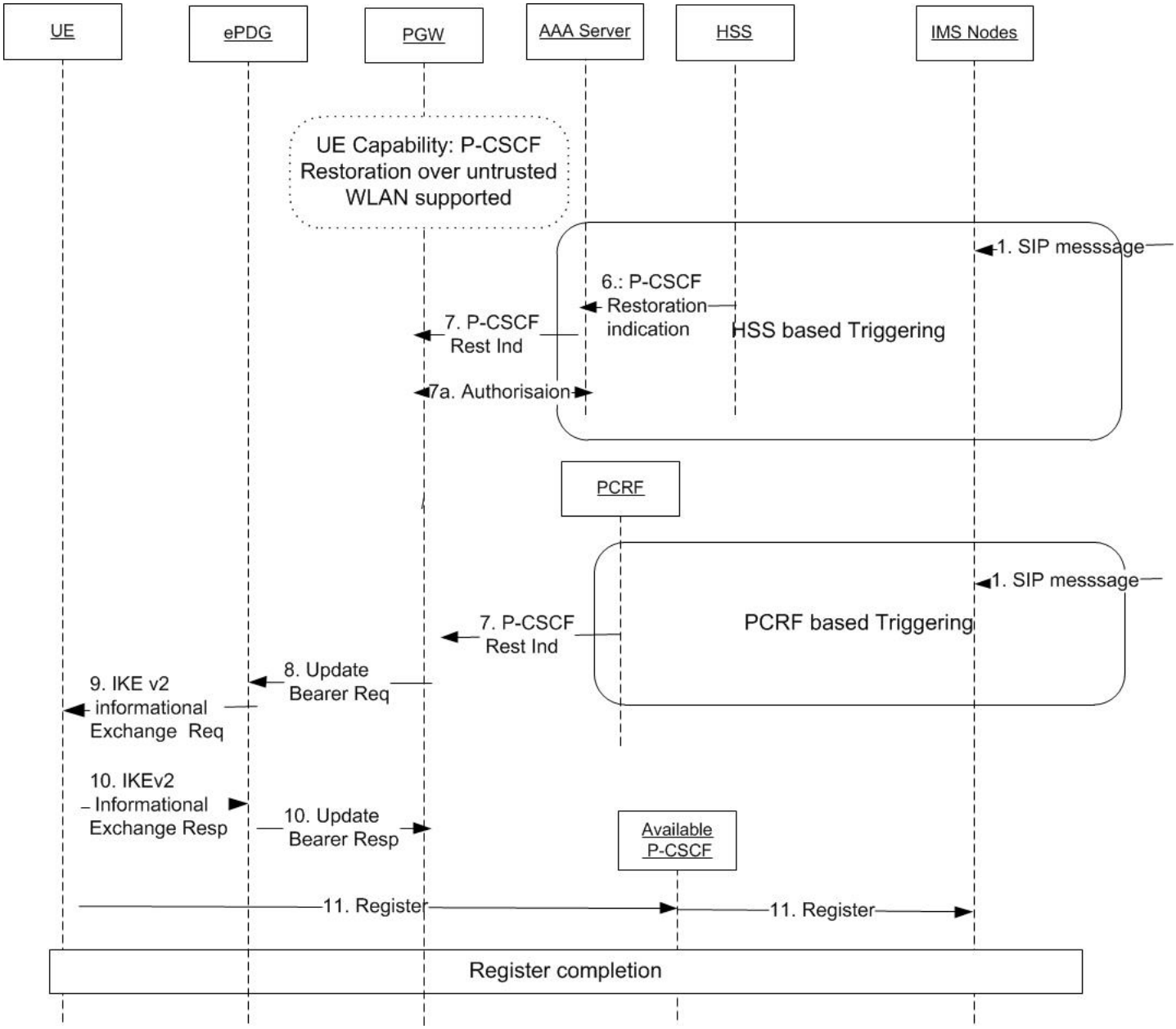
Extended Restoration Mechanism has the following phases:

- Capability exchange Phase i.e Swu notify exchange.
- Updation Phase [Post P-CSCF failure]: Getting new PCSCF info in UBR and conveying same to UE.

The UE which supports the P-CSCF restoration extension for the untrusted WLAN access, sends PCSCF_RESELECTION_SUPPORT notify payload to the ePDG in the IKEv2 message (IKE-AUTH) during establishment (or handover) of the IMS PDN connection over the untrusted WLAN access.

Upon receiving the UE capability, the P-CSCF restoration extension for untrusted WLAN supporting ePDG will forward the same in the APCO information element to the PGW over the S2b interface in Create Session Request.

Figure 27: PCRF Based Extended P-CSCF Restoration for Un-Trusted WLAN Access



In case of Extenstion P-CSCF restoration

- If both UE and ePDG support P-CSCF restoration and PGW was updated of this support in Create Session Request, the PGW will send an Update Bearer Request (as described in 3GPP TS 29.274 [10]) to the ePDG including the APCO information element set with a list of available P-CSCFaddresses.
- The ePDG will initiate an IKEv2 informational exchange procedure (as described in 3gpp 24.302) towards the UE to forward the list of available P-CSCF addresses received from the PGW.
- The UE will send a response to the ePDG which then sends an Update Bearer Response to the PGW.

Detailed Description

Capability support for a subscriber .

UE will share its P-CSCF restoration capability in 1st IKE_auth.

(First IKE AUTH request from Initiator)

HDR, SK { IDi, CERT, AUTH,

CP(CFG_REQUEST),

SAi2, TSi, TSr,

N(P-CSCF_RESELECTION_SUPPORT) } -----> ePDG

As part of this feature enhancement, the following new Private Notify Message status types will be supported.

Notify Message	Value (in decimal)	Descriptions
REACTIVATION_REQUESTED_CAUSE	40961	The IPsec tunnel associated to a PDN connection is released with a cause requesting the UE to reestablish the IPsec tunnel for the same PDN Connection after its release.
P-CSCF_RESELECTION_SUPPORT	41304	This status when present indicates that the UE supports the P-CSCF restoration extension for untrusted WLAN

P-CSCF_RESELECTION_SUPPORT Notify payload

The P-CSCF_RESELECTION_SUPPORT Notify payload is used to indicate the support by the UE of the P-CSCF restoration extension for untrusted WLAN.

The P-CSCF_RESELECTION_SUPPORT Notify payload is coded according to below figures.

Protocol id: Set to 0

SPI Size: Set to 0

Notify Message type: The Notify Message Type field is set to value 41304 to indicate the P-CSCF_RESELECTION_SUPPORT

Important -From Rel 13, 3gpp started using IANA number for notify payloads which belong to private range. For features, which configure notify-status-value from private range can lead to collision and operator will have to be careful while configuring non-collision numbers.

RFC 4306 IKEv2 Private Use Status Range - integer 40960 to 65535.

This can have conflict with above Notify 3gpp standard value, one should configure it carefully.

Message	IE	Descriptions
Delete Bearer Request	CAUSE	cause "reactivation requested" is sent over GTP-C based S2b during deactivation of IMS session in basic mechanism of P-CSCF restoration. This cause will come in Delete bearer request for default bearer. Value is 8
Create Session Request	APCO	Additional Parameter List : container identifier 0012H (P-CSCF Re-selection support); When the container identifier indicates P-CSCF Re-selection support, the container identifier contents field is empty and the length of container identifier contents indicates a length equal to zero. If the container identifier contents field is not empty, it shall be ignored. This PCO parameter may be present only if a container with P-CSCF IPv4 Address Request or P-CSCF IPv6 Address Request is present.
Update Bearer Request	APCO	Additional Parameter List : container identifier 0001H (P-CSCF IPv6 Address) or 000CH (P-CSCF IPv4 Address) or both.

Capability support on ePDg for said subscriber session:

During the set up (or handover) of the PDN connection, the ePDG should indicate capability to support the extended P-CSCF restoration using PCO/APCO.

Following Container ID is used for P-CSCF Re-Selection support indication (PCO/APCO):

0012H (P-CSCF Re selection support)

External Interfaces

S2b Interface:

Support of Additional Parameter list

0012H: MS->N/w IE: APCO: P-CSCF Re-selection support

0001H: N/w->MS IE: APCO: P-CSCF IPv6 Address

000CH: N/w->MS IE: APCO: P-CSCF IPv4 Address

Cause code: 8 Reactivation Requested

SWu:

Notify payload:

40961: REACTIVATION_REQUESTED_CAUSE

41304: P-CSCF_RESELECTION_SUPPORT

Configuring P-CSCF Restoration Support

Below new CLI commands are introduced to configure P-CSCF Restoration Support:

```
Configure
          call-control-profile profile_name
          [remove] wlan pcscf-restoration
       end
```

Monitoring and Troubleshooting the P-CSCF Restoration Support

Below show commands are introduced as part of P-CSCF Restoration Support:

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

- WLAN Access:
- P-CSCF Restoration

show crypto ikev2 security-associations

- P-CSCF Re-sel Supported
- 1 Total IKEv2 Informational CFG_REQ Sent
- 1 Total IKEv2 Informational CFG_RSP Rcvd
- 0 Total IKEv2 Informational CFG_REQ Collisions

show crypto ikev2 security-associations

Total IKEv2 Informational Statistics:

- CFG Req Sent
- CFG Reply Rcvd
- CFG Req Collisions

Total IKEv2 Notify Message Receive Statistics:

- P-CSCF Re-sel Supported

Total IKEv2 Notify Payload Sent Statistics

- Re-Activation Request

Total IKEv2 Notify Payload Received Statistics

- P-CSCF Re-sel Supported

show epdg statistics

- Total P-CSCF Re-sel success

GTP Related reasons:

- ePDG P-CSCF Restoration

show session disconnect-reasons

Disconnect Reason	Num Disc	Percentage
ePDG-pcscf-restoration		

show subs full

- P-CSCF Restoration Supported

Bulkstats

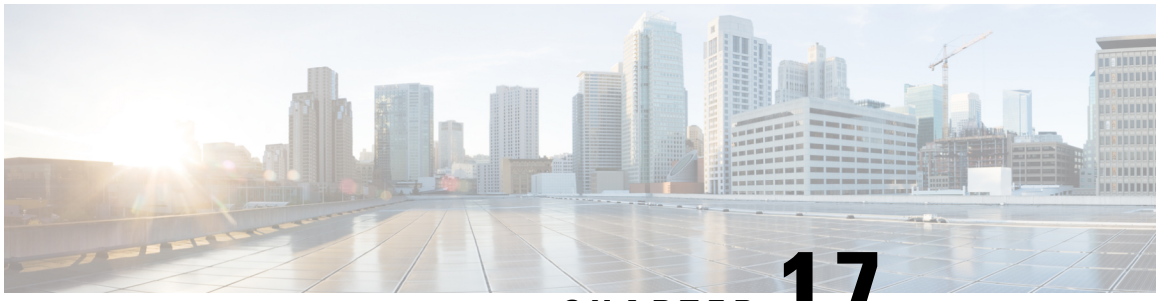
Below new statists are introduced to support P-CSCF Restoration Support.

epdg and epdg-apn schema

- num-gtp-pcscf-restoration-success
- sess-disconnect-epdg-pcscf-restoration

system schema

- ikev2-info-cfg-rsprecv
- ikev2-info-cfg-reqcoll
- ikev2-notifpaysent-reactreq
- ikev2-notifpayrecv-pcscfreselsupp
- ikev2-notifrecv-pcscfreselsupp



CHAPTER 17

ePDG Roaming Support

ePDG supports roaming for users with the support of Decorated NAI (IDi) as defined in 3GPP 23.0003.

ePDG Roaming Support Description

ePDG also processes VPLMN Dynamic Address Allowed. The HPLMN, VPLMN and VPLMN Dynamic Address Allowed will be used to decide whether the roaming user's traffic will be home routed (PGW from user's home PLMN is selected) or local breakout (PGW from Visited PLMN is selected).

Visited Network Identifier in APN-Configuration AVP in DEA on SWm interface will be used in case of handoff scenarios in which APN-OI sent in CSR is based on the MCC/MNC received with this AVP.

To override "VPLMN Dynamic Address Allowed" AVP received on SWm interface, a configuration under call control profile introduced.

For local PGW selection (IP or FQDN), PLMN is configurable so that correct APN-IO can be constructed and sent to PGW with CSR.

Decorated NAI support

As defined in TS 23.003, section 19.3.3, the decorated NAI format is defined as 'homerealm!username@otherrealm'(RFC 4282, sec 2.7). It consists of three parts as homerealm, username and otherrealm. For more details, please refer TS 23.003, section 19.3.3.

UE will send decorated NAI in IKE_AUTH message in IDi payload. ePDG processes decorated NAI format in SWu and also send the same on SWm interface.

Example: If the service provider has a PLMN ID and the IMSI is 234150999999999 (MCC = 234, MNC = 15) and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71, then the Decorated NAI takes the form either as below:

nai.epc.mnc015.mcc234.3gppnetwork.org!0234150999999999@nai.epc.mnc071.mcc610.3gppnetwork.org for EAP AKA authentication

Root-NAI Support

The root NAI format is "username@realm" as defined in TS 23.003, section 19.3.2. It consists of two parts as username and realm.

Example: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the Root NAI takes will be 0234150999999999@nai.epc.mnc015.mcc234.3gppnetwork.org for EAP AKA authentication

Roaming UE with Home Routed traffic

1. Roaming will be detected at ePDG for a particular session, if it sends decorated nai, or MNC/MCC extracted from root nai is different than PLMN-id configured under epdg-service.
2. Visited Network Identifier will be included in DER, for which PLMN-id will be taken from "otherrealm" of decorated nai, or serving PLMN ID configuration under ePDG service.
3. If AAA-Server sends DEA with AVP "VPLMN Dynamic Address Allowed" with NOT_ALLOWED(0) flag set, or may not include this AVP. It indicates that only home routed traffic is possible for this UE. Also, if the local configuration under call-control-profile is present as "vplmn-address not-allowed" then home routed traffic will be considered for this user, ignoring the AAA-Server provided AVP value (or its absence).

Note If Diameter Experimental result code Roaming-Not-Allowed (5004) is received from AAA server, the session will be rejected.

4. ePDG constructs APN-FQDN using HPLMN to get PGW IP address using DNS resolution. HPLMN is extracted from "homerealm" of decorated nai, or "realm" of root-nai. It both nai-formats are not received, then imsi will be used for initial attach of UICC users (not valid for fast reauth and non-UICC sessions). If APN-OI-Replacement string is received from AAA-Server in DEA, then it will take more precedence while constructing the APN-FQDN.
5. DNS-Server returns UE's home PGW address(es) and Create Session Request will be sent to PGW with APN-information. APN-OI part will be constructed using MNC/MCC extracted "homerealm" of decorated-nai, or "realm" of root nai. If both nai format is not received, then imsi will be used to extract MNC/MCC.
6. Create Session Request also contains Serving Network IE, in which MNC/MCC of Visited Network is sent. It may be either from “otherrealm” from decorated nai or from the configured value under epdg-service if UE does not support decorated nai. Below is the order of precedence for taking MNC/MCC for sending Serving Network IE:
7. Session is established with Create Session Response from UE's home PGW.

Roaming UE with Local Breakout Traffic

1. Roaming will be detected at ePDG for a particular session, if it sends decorated nai, or MNC/MCC extracted from root nai is different than PLMN-id configured under epdg-service.
2. Visited Network Identifier will be included in DER, for which PLMN-id will be taken from "otherrealm" of decorated nai, or serving PLMN ID configuration under ePDG service.
3. AAA-Server sends DEA with AVP “VPLMN Dynamic Address Allowed” with ALLOWED (1) flag set. It indicates that local breakout traffic is allowed for this user. Also, if the local configuration under call-control-profile is then local breakout traffic will be considered for this user, ignoring the AAA-Server provided AVP value (or its absence).

Note If Diameter Experimental result code Roaming-Not-Allowed (5004) is received from AAA-Server, the session will be rejected.

4. After successful authentication, ePDG constructs APN-FQDN to get PGW IP address using DNS resolution. ePDG constructs it using MNC/MCC from "otherrealm" part of decorated nai. If decorated nai is not supported, then PLNM-ID configured under ePDG service will be used. If APN-OI-Replacement string is ignored if it is received from AAA-Server in DEA.
5. After DNS based PGW address resolution in which DNS-Server returns UE's home PGW address(es), Create Session Request will be sent to PGW with APN-information. APN-OI part will be constructed from "otherrealm" of decorated nai or PLMN-ID configured under ePDG service.
6. Create Session Request also contains Serving Network IE, in which MNC/MCC of Visited Network is sent. It may be either from “otherrealm” from decorated nai or from the configured value under epdg-service if UE does not support decorated nai.
7. Session is established with Create Session Response from UE’s vPLMN PGW.

Roaming UE doing Handoff

1. For user doing LTE to wifi handoff, it will include IP address(es) in the Configuration Payload in first IKE_AUTH request to ePDG.
2. And, if the same user is roaming in vPLMN, it will construct FQDN using Visited PLMN ID as Operator Id (OI) and uses DNS resolution to get the ePDG ip address(es) in the Visited PLMN. UE may also construct decorated NAI to be sent in IKE_AUTH request.
3. Roaming will be detected at ePDG for a particular session, if it sends decorated nai, or MNC/MCC extracted from root nai is different than PLMN-id configured under epdg-service.
4. Visited Network Identifier will be included in DER, for which PLMN-id will be taken from "otherrealm" of decorated nai, or serving PLMN ID configuration under ePDG service.
5. In DEA, AAA-Server may include Visited Network Identifier along with PGW-Id under APN Configuration AVP. ePDG will send CSR to the PGW id received from AAA (PGW-Id can be either PGW-FQDN or IP-Address).

Note If Diameter Experimental result code Roaming-Not-Allowed (5004) is received from AAA-Server, the session will be rejected.

6. APN-OI part of the APN Information sent in Create Session Request is constructed from Visited Network Identifier received from AAA Server in DEA. APN-OI part will be constructed from Visited Network Identifier received in APN Configuration from AAA-Server or MNC/MCC extracted from "homerealm" of decorated-nai, or "realm" of root nai.

Note Can use imsi if the decorated/root nai is not received for UICC sessions. (not valid for fast-reauth and non-UICC sessions).

7. Create Session Request also contains Serving Network IE, in which MNC/MCC of Visited Network is sent. It may be either from “otherrealm” from decorated nai or from the configured value under epdg-service if UE does not support decorated nai.
8. Session is established with Create Session Response from the PGW with which UE was attached before handoff in LTE network.

Local PGW Selection

1. Roaming will be detected at ePDG for a particular session, if it sends decorated nai, or MNC/MCC extracted from root nai is different than PLMN-id configured under epdg-service.
2. Visited Network Identifier will be included in DER, for which PLMN-id will be taken from "otherrealm" of decorated nai, or serving PLMN ID configuration under ePDG service.

Note If Diameter Experimental result code Roaming-Not-Allowed (5004) is received from AAA-Server, the session will be rejected.

3. After successful authentication, ePDG will select local PGW IP or FQDN as per existing functionality (Please refer ePDG Admin guide/StarOS CLI guide for more details). DNS resolution will be done for PGW-FQDN to resolve IP address.
4. Create Session Request will be sent to PGW with APN-information. ePDG will construct APN-OI part of APN information from the MNC/MCC configured under APN-Profile configuration. If the configuration is not present then then MCC/MNC is taken either from "homerealm" if decorated nai is received or from "realm if root nai is received.

Note If root nai also is not received, then ePDG will use imsi to extract MNC/MCC from it. (not valid for Fast-Reauth and Non-UICC scenario.)

5. Create Session Request also contains Serving Network IE, in which MNC/MCC of Visited Network is sent. It may be either from "otherrealm" from decorated nai or from the configured value under epdg-service if UE does not support decorated nai.
6. Session is established with Create Session Response from the PGW selected locally.

NON-UICC Roaming Scenarios

1. For NON-UICC scenarios, a valid nai of the format "username@domain" must be received on either SWu with IDi or from SWm in Mobile-Node-Id AVP.
2. For NON-UICC roaming scenario, it would be mandatory that from SWu itself, IDi should be received in the format "username@domain".
3. Using the domain match, ePDG will select call-control-profile where MNC/MCC will be configured. It would be home PLMN for this device. The MNC/MCC will be compared with PLMN ID configured under ePDG service to decide if the user is roaming.

Note If the there is no call-control-profile present for the domain, or if the format in IDi is not of "username@domain", then UE will be considered to be present in its home PLMN (a Non-Roaming scenario).

4. On detection of roaming, ePDG will include Visited-Network-Identifier AVP in AAR towards AAA-Server. MNC/MCC will be taken from the PLMN id configured under ePDG service.

   The below two sections explains about the Local Breakout and Home Routed traffic scenarios for NON-UICC devices. The above four steps are same for both the scenarios.

   Non-UICC Roaming with Home-Routed Traffic

5. AAA-Server sends AAA with AVP "VPLMN Dynamic Address Allowed" with NOT_ALLOWED(0) flag set, or may not include this AVP. It indicates that only home routed traffic is possible for this UE. Also, if the local configuration under call-control-profile is present as "vplmn-address not-allowed", then home routed traffic will be considered for this user, ignoring the AAA-Server provided AVP value(or its absence).

Note If Diameter Experimental result code Roaming-Not-Allowed (5004) is received from AAA server, the session will be rejected.

6. After successful authentication, ePDG constructs APN-FQDN to get PGW IP address using DNS resolution. ePDG constructs it using MNC/MCC configured under call-control-profile. If APN-OI-Replacement string is received from AAA-Server in AAA, then it will take more precedence while constructing the APN-FQDN.
7. After DNS based PGW address resolution in which DNS-Server returns UE's home PGW address(es), Create Session Request will be sent to PGW with APN-information. APN-OI part will be constructed using MNC/MCC configured under call-control-profile.
8. Create Session Request also contains Serving Network IE, in which MNC/MCC of Visited Network is sent. MNC/MCC will be used from the PLMN Id configured under epdg-service.
9. Session is established with Create Session Response from UE's home.

   PGW Non-UICC Roaming with Local-Breakout Traffic

10. AAA-Server sends AAA with AVP "VPLMN Dynamic Address Allowed" with ALLOWED (1) flag set. It indicates that local breakout traffic is allowed for this user. Also, if the local configuration under call-control-profile is present as "vplmn-address allowed", then local breakout traffic will be considered for this user, ignoring the AAA-Server provided AVP value (or its absence).

Note If Diameter Experimental result code Roaming-Not-Allowed (5004) is received from AAA server, the session will be rejected.

11. After successful authentication, ePDG constructs APN-FQDN to get PGW IP address using DNS resolution. ePDG constructs it using MNC/MCC from PLMN Id configured under ePDG service. If APN-OI-Replacement string is ignored if it is received from AAA-Server in AAA message.

12. After DNS based PGW address resolution in which DNS-Server returns UE's home PGW address(es), Create Session Request will be sent to PGW with APN-information. APN-OI part will be constructed using MNC/MCC configured under ePDG Service.
13. Create Session Request also contains Serving Network IE, in which MNC/MCC of Visited Network is sent. MNC/MCC will be used from the PLMN Id configured under epdg-service.
14. Session is established with Create Session Response from UE's vPLMN PGW.

Assumptions and Limitations

- For NON-UICC UE case, IDi must be received with format “username@domain” to detect whether it is roaming or not.
- If the MNC of the PLMN ID under ePDG service is two digits, then zero will be added at the beginning while comparing root nai to detect whether it is roaming or not.
- There is minor SR/ICSR impact (will recover roaming user detail to have current session count after SR/ICSR)
- PMIPv6 protocol is not supported for roaming scenario.
- The UE which does not support decorated nai, should send root nai in format "username@realm". If realm has MNC/MCC is should be constructed using its HPLMN.
- Different mobility protocols combination is not supported. Roaming is supported only when all the PGWs (in VPLMN/HPLMNs) support GTPv2 S2b protocol.
- If AAA sends PGW-id, PGW allocation type as static and optionally include Visited Network Identifier, then in all the roaming scenarios, these value will take more preference as below:
  - Create Session Request will be sent to the PGW-id received from AAA.
  - PLMN of APN-OI part of the APN information to be send in CSR is used from Visited Network Identifier received from AAA.

Roaming Support for ePDG Configuration

Command Changes

pgw-address

plmn id mcc *mcc_name* mnc *mnc_name* are introduced in APN Profile Configuration mode.

Syntax

pgw-address plmn id mcc *mcc_name* **mnc** *mnc_name*

Performance Indicator Changes

As part of "ePDG Roaming Support" feature below show commands output are introduced:

show apn-prpfile full [all | name]

P-GW PLMN-ID

- MCC
- MNC
- If it is not configured

  P-GW PLMN-ID : Not Configured

show call-control-profile full [all | name]

SAMOG/ePDG Home PLMN

- MCC
- MNC

When it is not configured:

- SAMOG/ePDG Home PLMN : Not Configured

show call-control-profule full [all | name]

- VPLMN Address

show epdg-service statistics [name | apn-name]

Roaming Sessions

Table 31: UICC Sessions

Initial	Handoff
Active	Active
Setup	Setup
Attempts	Attempts
Failures	Failures

Table 32: Non UICC Sessions

Active
Setup
Attempts
Failures

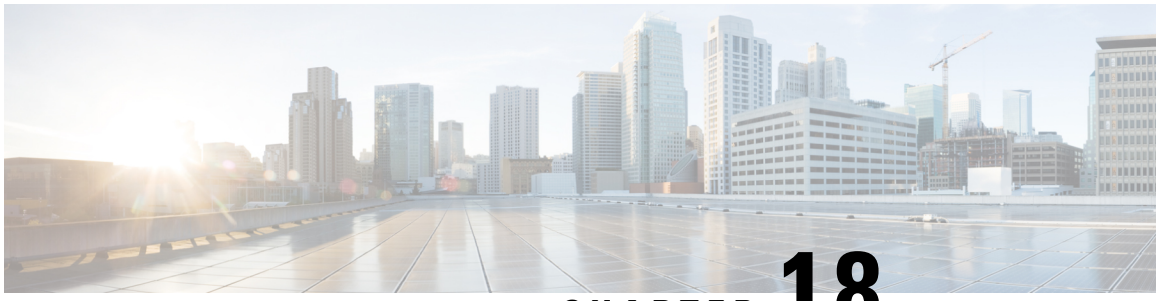
show subscriber full

- Roaming
- handoff

ePDG Roaming Support Bulkstats

Below Bulkstats are introduced in epdg-apn Schema to support ePDG Roaming feature support:

- roaming-sess-uicc-active
- roaming-sess-uicc-setup
- roaming-sess-uicc-attempts
- roaming-sess-uicc-failures
- roaming-ho-sess-uicc-active
- roaming-ho-sess-uicc-setup
- roaming-ho-sess-uicc-attempts
- roaming-ho-sess-uicc-failures
- roaming-sess-nonuicc-active
- roaming-sess-nonuicc-setup
- roaming-sess-nonuicc-attempts
- roaming-sess-nonuicc-failures



CHAPTER 18

ePDG S2b Piggybacking Support

Feature Information

Summary Data

Status:	New Feature
Introduced-In Release:	21.2
Modified-In Release(s):	ePDG
Applicable Product(s):	Cisco ASR 5500, VPC-SI, VPC-DI, UGP
Customer Specific:	No
Default Setting:	Disabled
CDETS ID(s)	CSCvc97504
Related Changes in this Release:	NA
Related Documentation:	ePDG Admin Guide, CLI Ref Guide and RCR

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

During LTE to WiFi handover, if Create Bearer Request reaches ePDG before Create Session Response, then it is dropped, as dedicated bearer is created only after session establishment is done. In this scenario, PGW will try to Create Bearer Request after 3 seconds, which in turn delays bearer creation.

S2b piggybacking resolves this issue by sending Create Session Response and Create Bearer Request in one message from PGW so that ePDG can process sequentially. This feature is nonstandard feature (non-3GPP). S2b Piggybacking support is controlled by CLI present under call-control-profile, this is disabled by default.

Assumptions and Limitations

1. Piggybacking Supported flag will be set for both initial attach and handoff sessions.
2. Only Create Bearer Request and Create Session Response messages will be supported as piggybacked during session creation.

Configuring ePDG S2b Piggybacking Support

Use the below configuration to configure Piggybacking Support. A new key word *wlan piggybacking* is introduced to support this feature.

```
config
             call-control-profile call_control_progile_name
               [remove] wlan piggybacking
            exit
            exit
```

Monitoring and Troubleshooting the S2B Piggybacking Support

Below show command output is introduced to support s2b Piggybacking:

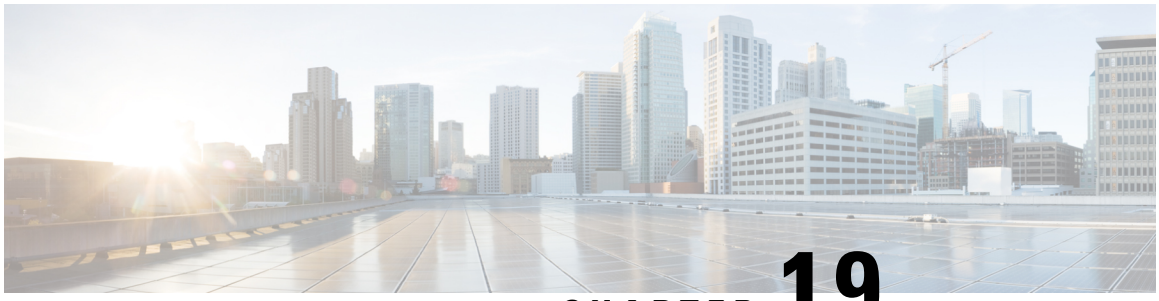
show call-control-profile full { name *profile_name* | all }

WLAN Access:

- piggybacking

show subscriber full

- Piggybacking Supported



CHAPTER 19

Hardware Crypto Assist for ePDG

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• VPC-DI • VPC-SI
Feature Default	Enabled - Always-on (if Coleto Creek Card is present)
Related Changes in This Release	Not applicable
Related Documentation	*ePDG Administration Guide*

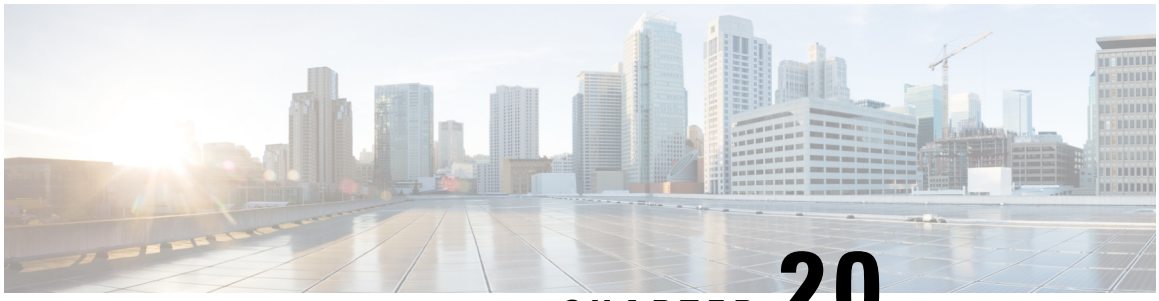
Revision History

Revision Details	Release
First introduced.	21.5

Feature Changes

Important The *ePDG Hardware Crypto Assist* feature is not fully qualified in this release. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

ePDG supports Hardware Crypto assist on VPC-DI and VPC-SI. This support is applicable only if an optional accelerator card (Coleto Creek Card) is present.



CHAPTER 20

Idle Seconds Micro-checkpoint

This chapter describes the implementation of a timer to track inactive sessions and to cleanup the sessions once the timer expires.

Feature Description

Idle timeout is used to track the inactive sessions on ePDG and clean them up once they have been idle for certain duration as defined by the idle timeout value. AAA provides PDN Inactivity timer value per session to ePDG via SWm interface. Both active and standby chassis track idle time of inactive sessions so that they can be removed from the chassis post timeout. The active chassis tracks the active sessions and notifies the standby chassis at every periodic timer expiry that the session is not idle. On the active chassis, both the Session Manager and ICSR framework track the active sessions and notify the standby periodically that the session is not idle.

Session managers send idle micro checkpoints every 10 seconds to corresponding session manager on the standby chassis.

To avoid frequent periodic idlesec micro checkpoints, Interval at which these checkpoints are sent is made configurable.

Also an event driven mechanism for idlesec micro checkpoints for ePDG is allowed to eliminate the overhead associated with periodic idlesec micro checkpoints.

Configuration based on Periodic Idle Seconds Micro-checkpoints

In this approach the existing hard coded idle timer of Session Manager is configurable per APN.

This approach involves:

- A new CLI is provided to configure the periodic idle second micro checkpointing timer.
- Timer is configurable on per APN basis. The default timer value is 10 Seconds.
- Value "0" means disabled i.e. the change from micro checkpointing to standby does not take place.
- ICSR framework will remove the 30 seconds timer and keep 15 min periodic timer notification.

Event Based Idle Seconds Micro-checkpoint

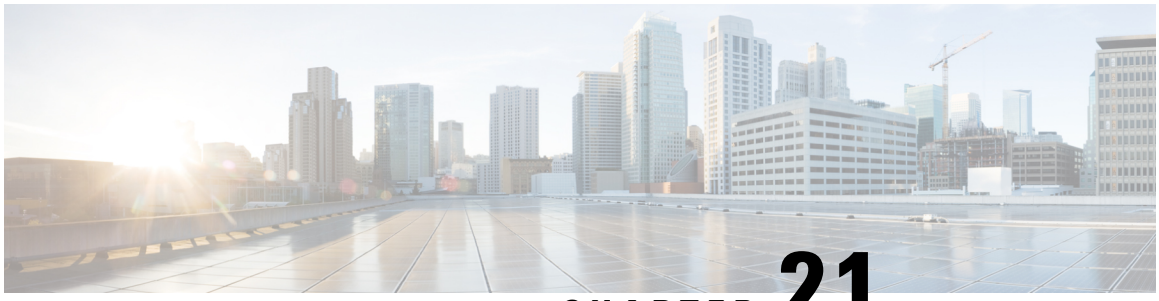
In this approach an idle second micro checkpoint is sent from Active to Standby chassis when session changes from active to idle or vice versa. The micro checkpoint carries the timestamp when session became active or idle. Upon receipt of the micro checkpoint, standby chassis updates the active/idle time using the timestamp received in the micro checkpoint. This process enables the Active and Standby chassis to be synchronized with respect to when a particular session became active or idle

This approach involves the following processes:

- Active chassis sends an idle second micro checkpoint with timestamp to Standby chassis when a session changes from *active* to *idle* or *idle* to *active* state.
- Upon receipt of the idlesec micro checkpoint, the Standby chassis records the timestamp at which session became *active* or *idle* .
- When switch over happens, standby uses the timestamp that was stored to adjust the inactivity time. For example, if session becomes inactive at time T, and switch over occurs at time T+1000 seconds, standby will set initial value of the PDN Inactivity timer after subtracting 1000 seconds.
- The configuration is available on per APN level to enable this functionality, and also to configure the duration after which a session is considered as idle if data is not received or sent.
- The default value for this configuration is 180 seconds.
- A similar option is provided at ePDG service level in case APN configuration is not being used on the system. APN configuration overrides the service level configuration.

Assumptions and Limitations

1. Per APN configurations will be done under apn-profile and per service configurations will be done under ePDG service configuration mode.
2. The idle timeout configuration under default-subscriber mode would be retained only for backward compatibility and will have last preference.
3. The idle second micro-checkpoint timer configuration and the deemed idle time configuration under subscriber mode will not have any impact even if configured.
4. The order of priority of idle timeout configuration would be AAA received > configured under default-subscriber > configured under apn-profile > configured under service. However, default-subscriber configuration is not recommended and should be used only for backward compatibility.
5. The order of priority of idle second micro-checkpoint timer configuration and the deemed idle time configuration would be configured under apn-profile > configured under service.
6. When encoding of IDLE second micro checkpoint by ICSR is successful and just before the checkpoint is to be sent to standby chassis, if there is a link flap the checkpoint is lost. But anyways the ICSR framework will again send the same after 15 minutes. If any switch over happens after flap and within 15 minutes, the transition information is lost.



CHAPTER 21

IFTASK Restart Capability for ePDG

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	VPC-DI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not applicable
Related Documentation	• *Statistics and Counters Reference* • *VPC-DI System Aministration Guide*

Revision History

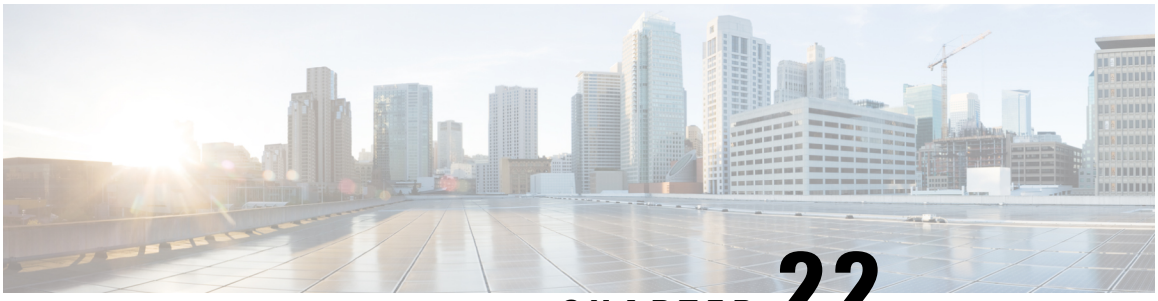
Revision Details	Release
First introduced.	21.6

Feature Changes

A new functionality was added to the StarOS to enable the automatic restarting of the IFTASK process in the event of a failure in the release 21.4. IFTASK process restart is enabled by default. With this release IFTASK Restart Capability for ePDG service is supported.

Important IFTASK_SERVICE_TYPE=2 (EPDG) is not supported. For more details, refer *Configuring IFTASK CPU* in the *VPC-DI System Administration Guide*

Note For more details, refer *IFTASK Process Startup Enhancements* in the *VPC-DI System Administration Guide*.



CHAPTER 22

IMSI Encryption Support

This chapter describes the following topics:

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

Revision History

Revision Details	**Release**
First introduced.	21.6

Feature Description

During the IMSI Encryption scenario, UE sends encrypted IMSI to AAA server with EAP payload, and in IKE_AUTH payload to ePDG. All UEs send a common-identity in IDi payload due to which all the sessions were being processed on same IPSec Manager, which limited the capacity of ePDG to maximum sessions supported by one IPSec Manager. With this feature, ePDG supports distribution of sessions across all IPSec Managers. ePDG decodes and process the string “anonymous” or any mutually agreed value received in IDi payload in first IKE_AUTH request. ePDG receives real username with Mobile-Node Identifier AVP from AAA in Final Diameter-EAP-Answer. IMSI is extracted from it, and it is used to find any pre-existing session(s) present in the system and clean it. All the old calls from same IMSI will be deleted once authentication of new session is successful

Note Multi-PDN sessions are also treated as re-attach sessions. Any older Multi-PDN session will be deleted once new session’s authentication is successful.

Configuring ePDG IMSI Encryption Support

This section provides information on CLI commands available in support of this feature.

Configuring Common ID

Use the following configuration in Cytpto Template configuration mode to enable this feature.

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
      ikev2-ikesa idi idi_value  { common-id | request-eap-identity }
       no ikev2-ikesa idi idi_value
      end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association parameters.
- **idi**: Configures the IKEv2 IKESA idi related parameters.
- *idi_value* : This is the Peer idi value to be used. This is a string of size 1 to 127.
- **common-id**: Configures the Common IDi(peer) session.
- **request-eap-identity**: Requests the EAP-Identity from peer.
- **no**: Disables the IKEv2 IKESA idi related parameters.

Monitoring and Troubleshooting

This section provides information on the show commands and bulk statistics available for the ePDG IMSI Encryption feature.

Show Commands and Outputs

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

show crypto template

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

IKE SA IDi [peer]:

- anonymous@realm [Common-Id Session]

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

show crypto statistics ikev2

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

- Common-Id Session Attempt:

  it will increment once the Configured IDi with common-id action is matched with Incoming session's IDi.
- Common-Id Session Success:

  It will increment once the Common-id session is successfully established.

show crypto ikev2-ikesa security-associations

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

- Common ID Session

show subscribers full

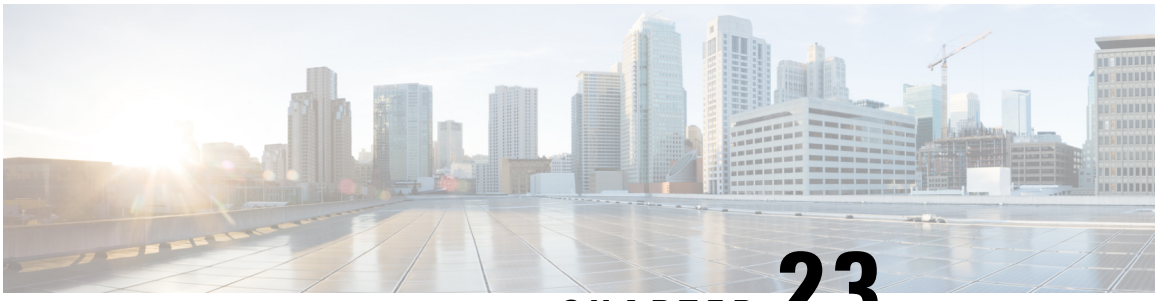
The following new fields are added to the output of this command:

- Common ID Session

Bulk Statistics

The following bulk statistics are added in the System Schema in support of the ePDG IMSI Encryption Support feature.

- ikev2-auth-common-id-sess-attempt - Increment once the Configured IDi with common-id action is matched with Incoming session's IDi.
- ikev2-auth-common-id-sess-success - Increment once the Common-id session is successfully established.



CHAPTER 23

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 33: Bulk Statistics Variables in the ePDG Schema

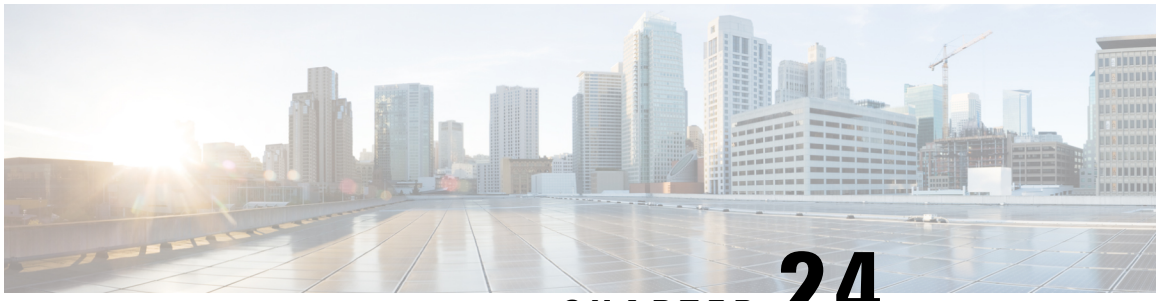
Variables	Description
vpnname	The name of the VPN associated with the interface.
vpnid	The identification number of the context configured on the system is facilitating the ePDG service. VPN ID is an internal reference number.
servname	The name of the ePDG service for which these statistics are being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

Variables	Description
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.
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.

Variables	Description
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.
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.

Variables	Description
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 24

Multiple ePDG Certificates Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	ASR 5500
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *Command Line Interface Reference* • *ePDG Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.3

Feature Changes

ePDG now supports multiple device certificates as described below.

- Crypto template supports additional four device certificates, retaining the existing associated certificate, thus maintaining the backward compatibility

- A new CLI command is introduced to configure CA certificate list in order of their issuance. Maximum four CA-Certificate lists are allowed
- The existing configuration to associate ca-certificates is enhanced to associate sixteen ca-certificates from four, so that certificate chaining can be configured for each device certificate
- In the certificate request from peer, there can be multiple CA-Hash present, and ePDG will send the Certificate (and its intermediate CA Cert) with first match. If there is no match, then the certificate configured under existing configuration will be treated as default certificate and it will be sent
- If the certificate sent is selected from new configuration, then CN name will be extracted from it and sent with ID payload in IKE_AUTH response, otherwise the existing implementation of using the configured value of ID under crypto template is used

Use Cases

Peer does not send Certificate Request Payload:

If peer does not send Certificate Request payload in first IKE-AUTH request, then ePDG will not send any certificate, even if they are associated with crypto template. It is existing behaviour.

Peer sends Certificate Request payload:

- Receiving Certificate Request payload itself enables ePDG to send the device certificate. Sending of intermediate CA for certificate chaining will be decided after matching of CA Hash received with Certificate Request payload.
- Below are two scenarios to be taken care after receiving Certificate Request payload:
  - Hash of only one CA (or Intermediate CA) is received :
    - ePDG will match the received CA-Hash, with the CA-Hash of configured CA-Certificates
    - If a matching CA-Certificate is found, then the Certificate signed by it will be sent in Certificate Payload
    - Also, there is possibility that peer has sent CA-Hash of an intermediate CA-Certificate, and then all the intermediate CA-Certificates will be sent, forming a Certificate Chain
    - The first Certificate Payload will contain ePDG Certificate and rest will be Intermediate CA Certificates. The last Intermediate CA Certificate will the one, which is signed by the Intermediate CA-Hash received from peer
    - Maximum of four Certificate Payload will be supported, first one will be ePDG Certificate and rest three will be Intermediate CA certificates.
  - Hash of multiple CA (or Intermediate CA) are received
    - All the steps mentioned in above case is applicable here also, except that the first match for CA-Hash found from the CA-Hash list received will be used to send ePDG Certificate(with Certificate Chain if applicable)

Important If there is no matching CA certificate or Intermediate CA certificate present under crypto template configuration, then the default certificate associated with “certificate <>” cli will be sent with certificate Payload. No intermediate CA certificate(s) will be sent in this scenario.

Assumptions and Limitations

- If there is no CA-Hash match found, then default ePDG certificate configured with CLI “certificate <>” under crypto template will be sent
- Maximum of five ePDG certificates can be configuration under crypto template. One is existing(default) and four more will be allowed with new CLI
- If ePDG Certificate is selected from the new configuration, then the ID payload of IKE_AUTH response will be filled with CN name extracted from the certificate. Using ID from the crypto template when default ePDG Certificate sent will be retained for backward compatibility
- Only four Certificate Payload is sent in case of Certificate Chaining scenario, so care should be taken to configure at maximum of three Intermediate CA Certificates for an ePDG certificate
- While sending CA-Hash in Certificate Request Payload, only first four CA-Certificate will be used, this is can be configured by CLI which is under Crypto Template
- A maximum of 20 CA certificates can be configured at global level of which 16 certificates are in support.

Command Changes

ca-certificate-list name

The **ca-certificate-list name** CLI command is introduced to configure multiple ePDG certificates.

```
configure
   ca-certificate-list name ca_cert_list_name ca-cert-name ca_cert_name_1
ca-cert-name ca_cert_name_2 ca-cert-name ca_cert_name_3  ca-cert-name ca_cert_name_4

   no ca-certificate-list name
   end
```

server-certificate

The **server-certificate** CLI command is added in the Crypto Template Configuration Mode to configure multiple ePDG certificates.

```
configure
   context context_name
      crypto template template_name ikev2-dynamic
      server-certificate server_certificate_name ca-certificate-list
```

```
ca_cert_list_name [ validate ]
     no server certificate server_certificate_name [ validate ]
     end
```

clear ca-certificate-list statistics

The **clear ca-certificate-list statistics** command has been added to clear certificate list statistics.

clear ca-certificate-list statistics

Performance Indicator Changes

ePDG Schema

Below new statistics are introduced to support Multiple ePDG Certificates in ePDG Schema:

Counter	Description	Trigger
ikev2-ca-cert-chains-sent	Total IKEv2 certification statistics (CA certificate chains sent)	Increments when CA certificate chain is sent in IKE payload
ikev2-server-certs-sent	Total IKEv2 certification statistics (server certificates sent excluding CA certificates)	Increments when non CA certificate is sent in IKE payload

show ca-certificate-list statistics

The following new fields are added to the output of this command to display the Certificate-list Statistics:

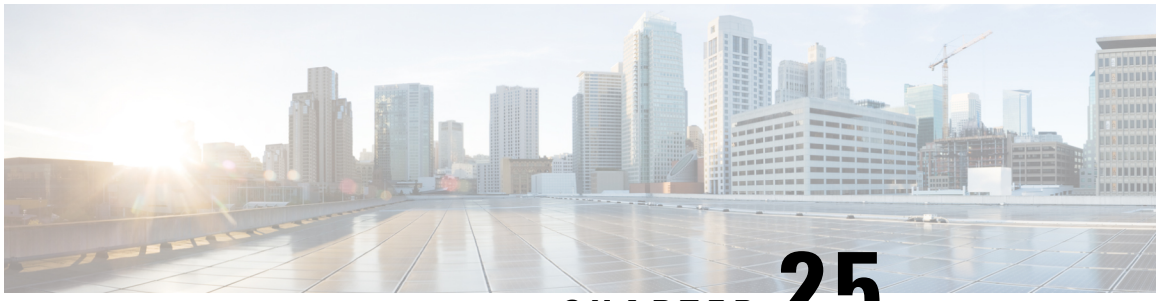
CA-Certificate-Lists:

- ca_cert_list_name
- ca_cert_name_1
- ca_cert_name_2
- ca_cert_name_3
- ca_cert_name_4

show crypto statistics

The following new fields are added to the output of this command to display the Crypto Statistics

- Server Certificates Sent
- CA Certificate Chains Sent



CHAPTER 25

Network Provided User Location Information reporting extensions over S2b interface

ePDG supports Network Provided User Location Information reporting extensions over S2b interface.

Feature Description

P-CSCF receives location information from the network when an IMS session is set-up, media is added / modified / removed within a session and when the session is released. This applies to emergency sessions and also to regular sessions set-up over an Untrusted access to EPC. The following IEs are added to the Create Session Request, Create Bearer Response, Update Bearer Response, Modify bearer Request, Delete Session Request and Delete Bearer Response messages over the S2b interface:

- WLAN Location Information
- WLAN Location Timestamp
- UE Local IP address
- UE UDP Port

The Retrieve Location Information flag is also added to the Update Bearer Request message over the S2b interface.

User location Information reporting extensions over S2b interface Supports the following features:

- ePDG provides WLAN Location Information and WLAN Location Timestamp in Create Session request, Create Bearer response, Delete Session request, Delete Bearer response, Update bearer response to PGW on S2b interface.
- ePDG provides UE Local IP/Port in Create Session request, Create Bearer response, Modify Bearer request, Delete Session request, Delete Bearer response, Update bearer response to PGW over S2b interface. UE Port will be included only if NAT is detected between UE and ePDG.
- ePDG processes WLAN Location Information and WLAN Location Timestamp sent by AAA over SWm interface in DEA/AAA messages.

- ePDG deletes stored WLAN Location Information/Timestamp if it doesn't receive same in AAA when AAR was sent with bit set for location retrieval.
- ePDG can trigger AAR towards AAA over SWm interface when it needs updated WLAN location information to be sent towards PGW.

The NPLI (Network Provided Location Information) of an UE in case of a TWAN access

The TWAN reports over S2a TWAN related Access Network Information at PDN connection establishment, at bearer creation / modification / release and at PDN connection release. Such TWAN related Access Network Information may correspond to a "TWAN Identifier" and/or to a UE Time Zone. Same is applicable on S2b interface for WLAN access in untrusted UE attachment on EPC.

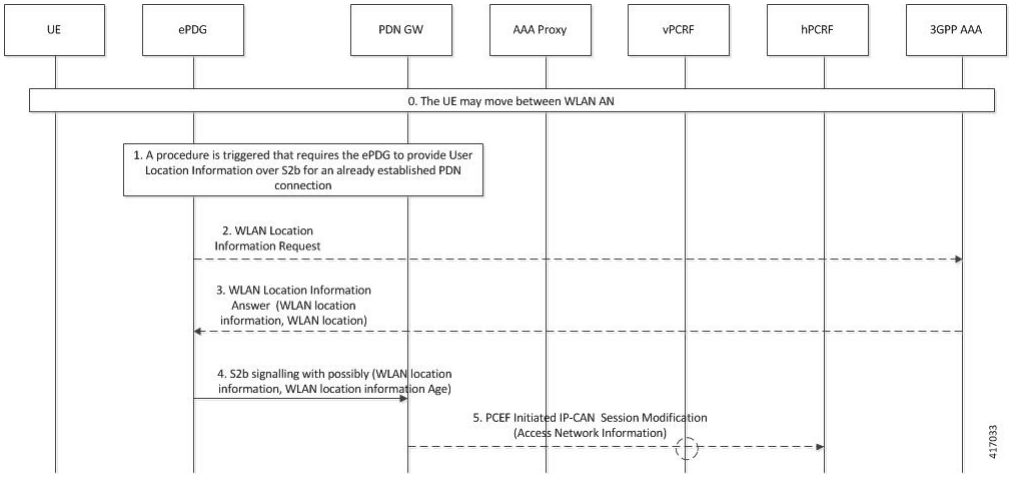
When as part of procedures for Authentication and Authorization on an Access Point based on USIM credentials, the WLAN Access Network provides WLAN Access Network location information to the 3GPP AAA server that it considers as network provided location, the 3GPP AAA server stores this information and provides it to the ePDG at the SWm Authentication and or Authorization procedure or upon request of the ePDG.

This location information is called WLAN Location Information and contains the same information as is contained in the TWAN Identifier. The Age of the WLAN Location information is provided in conjunction with the WLAN Location information.

The ePDG stores WLAN Location Information associated with an UE when it receives WLAN Access Network location information from the 3GPP AAA server. The ePDG removes the stored WLAN Location Information associated with an UE when it receives from the 3GPP AAA server an indication that no WLAN Access Network location information is available for this UE.

The WLAN Location Information information and its Age, when available, are propagated by the ePDG to the PDN(Config driven). This takes place at the UE-initiated connectivity to an initial PDN connection (Attach Procedure), at the UE-initiated connectivity to an additional PDN connection or, as described below, when the ePDG needs to send Network Provided User Location Information about an already established PDN connection.

When the AAA server has sent WLAN Location Information at the UE-initiated connectivity to an initial (Attach Procedure) or additional PDN connection, and when later the ePDG needs to send Network Provided User Location Information towards the PDN GW over S2b, the ePDG may initiate a WLAN Location Information Request to fetch the most up to date WLAN Location Information in conjunction with the age of this Information(CLI controlled).



0. When the 3GPP AAA server detects that the UE has moved between WLAN AN, it locally updates or removes the WLAN Location information and its Age it stores for the UE.

1. A procedure is triggered that requires the ePDG to provide Network Provided User Location Information over S2b for an already established PDN connection. The corresponding procedures are:
   - UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with GTP on S2b.<Delete Session Request>
   - PDN GW initiated Resource Allocation Deactivation with GTP on S2b.<Delete Bearer Response>
   - Dedicated S2b bearer activation with GTP on S2b.<Create Bearer Response>
   - S2b bearer modification with GTP on S2b.<Update Bearer Response>
2. When the AAA server has sent WLAN Location Information at the set-up of a SWm session and the ePDG has detected a change of the outer IP address of the UE, the ePDG initiates a WLAN Location Information Request towards the 3GPP AAA server by sending AAR message with "WLAN-Location-Info-Request" bit set.
3. The 3GPP AAA server provides a WLAN Location Information Answer that may contain WLAN location information and WLAN location information Age or an indication that no WLAN location information is available. The ePDG replaces any WLAN location information and WLAN location information Age it may have stored beforehand by the information received from the 3GPP AAA server. When the WLAN Location Information Answer contains an indication that no WLAN location information is available, the ePDG removes any WLAN location information and WLAN location information Age it may have stored beforehand about the UE.
4. The ePDG issues S2b signalling with Network Provided User Location Information. The Network Provided User Location Information includes UE local IP address and optionally UDP source port number (if NAT is detected). The Network Provided User Location Information includes WLAN Location Information (and its age) only when the ePDG has such information currently available about the UE. When the PDN GW receives no WLAN Location Information from the ePDG it will delete any such information it may have stored for the PDN connection.
5. If requested by the PCRF the PDN GW forwards to the PCRF following information extracted from Network Provided User Location Information it may have received from the ePDG:
   - The UE local IP address
   - WLAN location information in conjunction with the Age of this information

     When the PCRF receives no WLAN location information from the PDN GW within Network Provided User Location Information the WLAN location information is considered as not any longer valid.

WLAN location support in initial attach: Create Session Request

If NPLI configuration enabled and AAA has provided, WLAN information in DEA during initial attach, ePDG will update same in CSR towards ePDG.

WLAN location support during other S2b procedure

This section describes producers like Create Bearer Response, Delete Bearer Response, Delete Session Request.

There are three scenarios:

1. If WLAN Location Information/Timestamp is available at ePDG, it will send the same in this messages. If the last updated WLAN info received from AAA is still present and there is no change in UE IP/Port, ePDG will send last received WLAN info towards PGW in procedure like Create Bearer Response, Delete Bearer Response, Delete Session Response if NPLI config is enabled.
2. If there is a change in UE Local IP/Port (Mobike triggered procedure) from last updated WLAN info and the NPLI configuration is enabled and the configuration to take the latest WLAN info from AAA is also enabled, ePDG will trigger AAR and get the updated WLAN info from 3GPP-AAA-Server and now this new updated info will be sent in any of above message (Create Bearer Response, Delete Bearer Response, Delete Session Request) on S2b interface.
3. If no WLAN information present, none will sent in any of above message.

WLAN location support during Update bearer request/response

Update bearer response will have Location information. If request has " Retrieve Location bi t " set, it will be treated as specific request for getting WLAN Location information and ePDG. If it doesn't have same, it will still send UE Local IP/Port.

Exchange will be treated as success even if no WLAN info is available from AAA Server. With respect to triggering AAR towards AAA, ePDG will check if bit is set and Mobike has happened before triggering AAR. In case either bit is not set or Mobike has not happened, AAR will not be triggered.

UE local IP change(Mobike)

When ePDG detects UE IP/Port change in case of Mobike, it will trigger Modify Bearer request (MBR) with updated UE IP/port included. Triggering MBR on UE IP change will be driven by a new configuration under call-control-profile.

Note Refer section 7.2.7 of 3gpp specs 29.274 d50 for additional information.

Important Modify Bearer Request is triggered only if Mobike is enabled. i.e. IP address/ port is being updated by Update SA address request. IP address change with NAT reboot will not trigger Modify Bearer Request.

Following two IEs are sent in Modify Bearer request.

Information elements	IE Type
UE Local IP Address	IP Address
UE UDP Port	Port Number

Assumptions and Limitations

- If NPLI configuration is enabled and WLAN Location Information not received from AAA, ePDG will not send the same in S2b messages.
- If UBR has bit set, ePDG will respond with UE Local IP/Port and WLAN info. In case WLAN info is not available, ePDG will still respond IP/Port and treat exchange as sucess.

Configuring NPLI e2e VoWiFi on ePDG and PGW

A new keyword " **wlan-location-info-timestamp** " introduced as part of PLI e2e for VoWiFi on ePDG and PGW. Use the following configuration to configure PLI e2e for VoWiFi on ePDG and PGW.

```
config
       call-control-profile  ccp1
            epdg-s2b-gtpv2 send wlan-location-info-timestamp
          end
```

A new keyword " **message** " introduced as part of PLI e2e for VoWiFi on ePDG and PGW. Use the following configuration to configure PLI e2e for VoWiFi on ePDG and PGW.

```
config
       call-control-profile  ccp1
             epdg-swm send message aar trigger location-retrieval
          end
```

A new keyword " **mobike** " introduced as part of PLI e2e for VoWiFi on ePDG and PGW. Use the following configuration to configure PLI e2e for VoWiFi on ePDG and PGW.

```
config
       call-control-profile  ccp1
              epdg-s2b-gtpv2 send message mbr trigger mobike
          end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature to support Sending SWm 3GPP AAA FQDN Address in CSReq

Show Configuration

call-control-profile *ccp_name*

- epdg-s2b-gtpv2 send aaa-server-id

When CLI is disabled, with "*remove epdg-s2b-gtpv2 send aaa-server-id*" Show commands outputs added as part of this feature for "*show configuration verbose*":

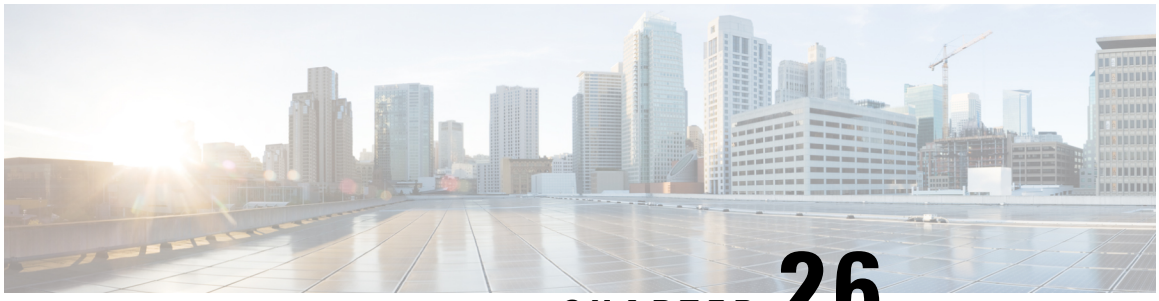
- remove epdg-s2b-gtpv2 send aaa-server-id

Show commands outputs added for "*show call-control-profile full {all | name <>}*" if enabled :

- Sending AAA Origin-host and origin-realm

Show commands outputs added for "*show call-control-profile full {all | name <>}*" if disabled:

- Sending AAA Origin-host and origin-realm



CHAPTER 26

Packet Capture (PCAP) Trace

Feature Information

Summary Data

Applicable Product(s) or Functional Area	• ePDG • IPSec • MME • SaMOG
Applicable Platform(s)	ASR 5500 VPC-DI VPC-SI
Feature Default	Disabled
Related Changes in This Release	Not Applicable
Related Documentation	• *ASR 5000 System Administration Guide* • *ASR 5500 System Administration Guide* • *Command Line Interface Reference Guide* • *ePDG Administration Guide* • *IPSec Reference Guide* • *SaMOG Administration Guide* • *VPC-SI System Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release
PCAP Tracing support for MME S1-AP interface is added in this release.	21.4
First introduced.	21.2

Feature Description

This feature enables the output of the **monitor subscriber** and **monitor protocol** commands to be captured using the packet capture (PCAP) functionality. The output can be stored in a text file in a hard disk, and later transferred to an external server through SFTP using a PUSH or PULL method. The text file can then be converted to a pcap file using external tools such as text2pcap, or imported directly as PCAP using packet analyzer tools such as wireshark.

PCAP trace and hexdump file collection can be enabled or disabled under the **monitor protocol** and **monitor subscriber** commands. For more information, refer *Enabling or Disabling Hexdump* section of this chapter.

Note For VPC-DI deployments, a separate function is available to perform packet captures on specific cards (VMs) and card interfaces on the internal DI-network. Refer to the Exec mode command **system packet-dump** command in the *Command Line Interface Reference* for more information.

Configuring PCAP Trace

Enabling Multiple Instances of CDRMOD

Use the following configuration to enable multiple instances of CDRMOD (one per packet processing card):

```
config
   cdr-multi-mode
   end
```

Notes:

- Although hexdump record generation is supported on both single-mode and multi-mode, it is recommended to enable the CDR multi-mode.

Important After you configure the **cdr-multi-mode** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- Use the **default cdr-multi-mode** command to configure this command with its default setting.

Important After you configure the **default cdr-multi-mode** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- **Default**: Single CDRMOD mode

Configuring the Hexdump Module

Use the following configuration to specify the handling characteristics of the hexdump files:

```
config
   context context_name
      hexdump-module
         hexdump { purge { storage-limit megabytes | time-limit seconds } [
 max-files max_records ] | push-interval interval | push-trigger
space-usage-percent trigger_percent | remove-file-after-transfer |
transfer-mode { pull [ module-only ] | push primary { encrypted-url | url
 } url [ secondary { encrypted-secondary-url | secondary-url } secondary_url
 ] [ via local-context ] [ max-files files ] [ max-tasks max_tasks ] [
module-only ] } | use-harddisk }
         end
```

Notes:

- Use the **default hexdump [purge | push-interval | push-trigger [space-usage-percent] | remove-file-after-transfer | transfer-mode [module-only] | use-harddisk] +** command to configure the keywords to its the default setting.
  - **purge**: Not enabled
  - **push-interval**: 60 seconds
  - **push-trigger**: 80 percent
  - **remove-file-after-transfer**: Disabled
  - **transfer mode**: PUSH
  - **use-harddisk**: Disabled
- Use the **no hexdump [purge | remove-file-after-transfer | use-harddisk] +** command to disable the configured hexdump file storage and processing.

- **purge**: Disables the deleting of record files on the hard disk based on a storage limit or a time limit.
- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the system's hard disk.

- Use the **purge { storage-limit** *megabytes* **| time-limit** *seconds* **} [max-files** *max_records* **]** keywords to configure parameters for deleting hexdump records from the hard drive. This command is not enabled by default.
  - **storage-limit** *megabytes*: Specifies that hexdump records are to be deleted from the hard drive upon reaching a storage limit defined in megabytes.

    bytes must be an integer from 10 through 143360.
  - **time-limit** *seconds*: Specifies that hexdump records are to be deleted from the hard drive upon reaching a time limit defined in seconds.

    seconds must be an integer from 600 through 2592000.
  - **max-files** *max_records*: Specifies the maximum number of files to purge. If configured to 0, all records will be purged until the limit is reached.

    max_records must be an integer that is of value 0, or from 1000 through 10000.

- Use the **push-interval** *interval*keyword to specify the transfer interval (in seconds) when hexdump files will be pushed to an external file server.
  - *interval* must be an integer from 30 through 3600.
  - **Default**: 60

- Use the **push-trigger space-usage-percent** *trigger_percent* to specify the disk space utilization percentage threshold at which an automatic push is triggered and files are transferred to the external server.
  - *trigger_percent* must be an integer from 10 through 80.
  - **Default**: 80

- Use the **remove-file-after-transfer** keyword to specify that the system must delete hexdump files after they have been transferred to the external file server.

  Default: Disabled.

Important This keyword must be enabled for hexdump records.

- Use the **transfer-mode { pull [module-only] | push primary { encrypted-url | url }** *url* **[secondary { encrypted-secondary-url | secondary-url }** *secondary_url* **] [via local-context] [max-files** *files* **] [max-tasks** *max_tasks* **] [module-only] }** keywords to specify the transfer mode to be used when transferring hexdump files to an external file server
  - **pull**: Specifies that the destination server (external storage) will pull the hexdump files.
  - **push**: Specifies that the system will push hexdump files to the destination server. This is the default mode.

- **primary encrypted-url** *url*: Specifies the primary URL location to which the system pushes the files in encrypted format.

  url must be an alphanumeric string of 1 through 8192 characters.

- **primary url** *url*: Specifies the primary URL location to which the system pushes the hexdump files.

  url must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/direct*.

- **secondary encrypted-secondary-url** *secondary_url*: Specifies the secondary URL location to which the system pushes the files in encrypted format.

  secondary_url must be an alphanumeric string of 1 through 8192 characters.

- **secondary secondary-url** *secondary_url*: Specifies the secondary URL location to which the system pushes the hexdump files.

  secondary_url must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/direct*.

- **via local-context**: Specifies that the local context, and, subsequently, the SPIO management ports, will be used to pull or push hexdump files.

- **max-files** *files*: Specifies the maximum number of files that can be transferred per push.

  files must be an integer from 4 to 4000.

- **max-tasks** *max_tasks*: Specifies the maximum number of files per push.

  max_tasks must be an integer from 4 through 8.

- **module-only**: Specifies that the transfer of hexdump records is to be applied only to the module type for which the configuration was originally created. If this option is not enabled, the transfer will occur for all record types.

- Use the **use-harddisk** keyword to specify that the hard disk drive on the SMC is to be used to store hexdump records.

  Default: Disabled.

Important This keyword must be enabled for hexdump records.

Configuring the Hexdump File Parameters

Use the following configuration to specify the format of the hexdump files:

```
config
   context context_name
      hexdump-module
         file [ compression { gzip | none } | current-prefix prefix |
delete-timeout seconds | directory directory_name | exclude-checksum-record |
 field-separator { hyphen | omit | underscore } | headers | name file_name
 | reset-indicator | rotation { num-records number | tariff-time minute
```

```
minutes hour hours | time seconds | volume bytes } | sequence-number { length
 length | omit | padded | padded-six-length | unpadded } | storage-limit
limit | time-stamp { expanded-format | rotated-format | unix-format } |
trailing-text string | trap-on-file-delete | xor-final-record ] +
          end
```

Notes:

- Use the **default file [compression | current-prefix | delete-timeout | directory | field-separator | headers | name | reset-indicator | rotation { num-records | tariff-time | time | volume } | sequence-number | storage-limit | time-stamp | trailing-text | trap-on-file-delete] +** command to configure the default setting for the specified keyword(s).
- Use the **compression { gzip | none }** keyword to specify the compressions of hexdump files.
  - **gzip**: Enables GNU zip compression of the hexdump file at approximately 10:1 ratio.
  - **none**: Disables Gzip compression.
- Use the **current-prefix** *prefix* keyword to specify a string to add at the beginning of the hexdump file that is currently being used to store records.
  - *prefix* must be an alphanumeric string of 1 through 31 characters.
  - **Default**: curr
- Use the **delete-timeout** *seconds* keyword to specify a time period, in seconds, after which the hexdump files are deleted. By default, files are never deleted.
  - *seconds* must be an integer from 3600 through 31536000.
  - **Default**: Disabled
- Use the **directory** *directory_name* keyword to specify a subdirectory in the default directory in which to store hexdump files.
  - *directory_name* must be an alphanumeric string of 0 through 191 characters.
  - **Default**: */records/hexdump*
- Use the **exclude-checksum-record** keyword to exclude the final record containing #CHECKSUM followed by the 32-bit Cyclic Redundancy Check (CRC) of all preceding records from the hexdump file.

  Default: Disabled (a checksum record is included in the hexdump file header)
- Use the **field-separator { hyphen | omit | underscore }** to specify the type of separators between two fields of a hexdump file name:
  - **hyphen**: Specifies the field separator as a "-" (hyphen) symbol between two fields.
  - **omit**: Omits the field separator between two fields.
  - **underscore**: Specifies the field separator as an "_" (underscore) symbol between two fields.
- Use the **headers** keyword to include a file header summarizing the record layout.
- Use the **name** *file_name* to specify a string to be used as the base file name for hexdump files.

file_name must be an alphanumeric string from 1 through 31 characters.

- Use the **reset-indicator** to specify the inclusion of the reset indicator counter (value from 0 through 255) in the hexdump file name.

  The counter is incremented whenever any of the following conditions occur:

  - A peer chassis has taken over in compliance with Interchassis Session Recovery (ICSR).
  - The sequence number (see **sequence-number** keyword) has rolled over to zero.

- Use the **rotation { num-records** *number* **| tariff-time minute** *minutes* **hour** *hours* **| time** *seconds* **| volume** *bytes* **}** keyword to specify when to close a hexdump file and create a new one.

  - **num-records** *number*: Specifies the maximum number of records that should be added to a hexdump file. When the number of records in the file reaches this value, the file is complete.

    number must be an integer from 100 through 10240. **Default**: 1024

  - **tariff-time minute** *minutes* **hour** *hours*: Specifies to close the current hexdump file and create a new one based on the tariff time (in minutes and hours).

    minutes must be an integer from 0 through 59.

    hours must be an integer from 0 through 23.

  - **time** *seconds*: Specifies the period of time to wait (in seconds) before closing the current hexdump file and creating a new one.

    seconds must be an integer from 30 through 86400. **Default**: 3600

Important It is recommended to set the rotation time to 30 seconds.

  - **volume** *bytes*: Specifies the maximum size of the hexdump file (in bytes) before closing it and creating a new one.

    bytes must be an integer from 51200 through 62914560. Note that a higher setting may improve the compression ratio when the compression keyword is set to gzip. **Default**: 102400

- Use the **sequence-number { length** *length* **| omit | padded | padded-six-length | unpadded }** keyword to exclude or include the sequence number with a specified format in the file name.

  - **length** *length*: Includes the sequence number with the specified length.

    length must be the file sequence number length with preceding zeroes in the file name, and must be an integer from 1 through 9.

  - **omit**: Excludes the sequence number from the file name.
  - **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
  - **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
  - **unpadded**: Includes the unpadded sequence number in the file name.

- Use the **storage-limit** *limit* keyword to set the storage limit. Files will be deleted when the specified amount of space (in bytes) is reached.

  limit must be an integer from 10485760 through 268435456.

- Use the **time-stamp { expanded-format | rotated-format | unix-format }** keyword to specify the format of the file creation timestamp to be included in the file name.
  - **expanded-format**: Specifies the UTC (Universal Time Coordinated) MMDDYYYYHHMMSS format.
  - **rotated-format**: Specifies the time stamp format to YYYYMMDDHHMMSS format.
  - **unix-format**: Specifies the UNIX format of x.y, where x is the number of seconds since 1/1/1970 and y is the fractional portion of the current second that has elapsed.

- Use the **trailing-text** *string* keyword to specify the inclusion of an arbitrary text string in the file name as an alphanumeric string of 1 through 30 characters.

  string must be an alphanumeric string from 1 through 30 characters.

- Use the **trap-on-file-delete** keyword to instruct the system to send an SNMP notification (trap) when a hexdump file is deleted due to lack of space.

  Default: Disabled

- Use the **xor-final-record** keyword to insert an exclusive OR (XOR) checksum (instead of a CRC checksum) into the hexdump file header, if the exclude-checksum-record is left at its default setting.

  Default: Disabled

- The + symbol indicates that more than one of the previous keywords can be entered within a single command.

Enabling or Disabling Hexdump

Hexdump captures can be enabled for protocols in the **monitor subscriber** and **monitor protocol** commands in the Exec Mode. Subscriber information for PCAP trace can be specified using the filters in the **monitor subscriber** command. For protocols and filters supported for a specific product, refer the respective product Administration and Reference guides.

When the **monitor subscriber** or **monitor protocol** command is running, use the **U** or **V** option to enable hexdump capturing:

- **U - Mon Display (ON)**: Use this option to display message captures on the terminal.
  - **Default**: ON
  - When this option is turned off, monitoring will still run in the background.

- **V - PCAP Hexdump (NONE)**: Use this option to enable or disable capturing hexdump packets globally.
  - **Default**: None
  - **V - PCAP Hexdump (ON)**: Hexdump capture is enabled with the prompt:

    Warning :Turning ON/OFF will impact other cli logging terminals, You will interupt others already using hexdump.

- **V - PCAP Hexdump (OFF)**: Hexdump capture is disabled (paused).

Enabling PCAP Trace for MME

This section describes how to enable PCAP trace for MME S1-AP interface and SGsAP interface.

- Under monitor protocol (monpro), enable S1-AP and SGS, or SCTP protocol option along with V - PCAP Hexdump (ON), to capture all S1-AP messages in PCAP hexdump.
- Monitor subscriber (monsub) supports PCAP tracing on S1-AP and SGS filter options.
- When S1-AP or SGS filter option is selected in monpro/monsub, PCAP Hexdump will have dummy SCTP header. The following fields are set as dummy in the SCTP header:
  - Verification tag
  - Checksum
  - Chunk flags
  - Transmission Sequence Numbers (TSN)
  - Stream identifier
  - Stream sequence number
- When the SCTP protocol option is selected in monpro, PCAP hexdump will have the original SCTP header.

Monitoring and Troubleshooting PCAP Trace

Show Command(s) and/or Outputs

The show command(s) in this section are available in support of PCAP trace.

show cdr statistics

The following fields are available in the output of the **show cdr statistics** command in support of this feature:

```
EDR-UDR file Statistics:
------------------------
CDRMOD Instance Id: 2
 Hexdump-module Record Specific Statistics:
  Hexdump-module files rotated:                       0
  Hexdump-module files rotated due to volume limit:   0
  Hexdump-module files rotated due to time limit:     0
  Hexdump-module files rotated due to tariff-time:    0
  Hexdump-module files rotated due to records limit:  0
  Hexdump-module file rotation failures:              0
  Hexdump-module files deleted:                       0
  Hexdump-module records deleted:                     0
  Hexdump-module records received:                    0
  Current open Hexdump-module files:                  0
  Time of last Hexdump-module file deletion:          0
```

*Table 34: **show cdr statistics** Command Output Descriptions*

Field	Description
EDR-UDR file Statistics:	
CDRMOD Instance Id	Indicates the CDRMOD instance id for which the statistics are collected.
Hexdump-module Record Specific Statistics:	
Hexdump-module files rotated	Total number of times a hexdump file was closed and a new hexdump file was created.
Hexdump-module files rotated due to volume limit	Total number of times a hexdump file was closed and a new hexdump file was created since the volume limit was reached.
Hexdump-module files rotated due to time limit	Total number of times a hexdump file was closed and a new hexdump file was created since the time limit was reached.
Hexdump-module files rotated due to tariff-time	Total number of times a hexdump file was closed and a new hexdump file was created since the tariff time was reached.
Hexdump-module files rotated due to records limit	Total number of times a hexdump file was closed and a new hexdump file was created since the records limit was reached.
Hexdump-module file rotation failures	Total number of times hexdump file rotation failed.
Hexdump-module files deleted	Total number of times hexdump files were deleted.
Hexdump-module records deleted	Total number of times hexdump records were deleted.
Hexdump-module records received	Total number of times hexdump records were received.
Current open Hexdump-module files	Total number of hexdump files currently open.
Time of last Hexdump-module file deletion	Time of the last deleted hexdump file.

show { hexdump-module | cdr } file-space-usage

The following fields are available in the output of the **show { hexdump-module | cdr } file-space-usage** command in support of this feature:

```
CDRMOD Instance Id: 2
   Hexdump-module File Storage LIMIT              : 33554432 bytes
   Hexdump-module File Storage USAGE              : 196608 bytes
   Percentage of Hexdump-module file store usage  : 0.585938
```

*Table 35: **show { hexdump-module | cdr } file-space-usage** Command Output Descriptions*

Field	Description
CDRMOD Instance Id	Indicates the CDRMOD instance id for which the statistics are collected.
Hexdump-module File Storage LIMIT	Indicates the maximum storage space (in bytes) that can be used for hexdump files.
Hexdump-module File Storage USAGE	Indicates the total storage space (in bytes) used for hexdump files.
Percentage of Hexdump-module file store usage	Indicates the total percentage of storage used for hexdump files.

show hexdump-module statistics

The following fields are available in the output of the **show hexdump-module statistics** command in support of this feature.

```
Hexdump-module-Record file Statistics:
-----------------------
CDRMOD Instance Id: 2
  Hexdump-module files rotated:                       0
  Hexdump-module files rotated due to volume limit:  0
  Hexdump-module files rotated due to time limit:    0
  Hexdump-module files rotated due to tariff-time:   0
  Hexdump-module files rotated due to records limit: 0
  Hexdump-module file rotation failures:             0
  Hexdump-module files deleted:                      0
  Hexdump-module records deleted:                    0
  Hexdump-module records received:                   0
  Current open Hexdump-module files:                 0
  Time of last Hexdump-module file deletion:         0

Hexdump-module PUSH Statistics:
-----------------------------------
  Successful File Transfers   : 0
  Failed File Transfers       : 0
  Num of times PUSH initiated : 0
  Num of times PUSH Failed    : 0
  Num of times PUSH cancelled
            due to HD failure : 0
  Num of periodic PUSH        : 0
  Num of manual PUSH          : 0
  Current status of PUSH      : Not Running
  Last completed PUSH time    : N/A

Primary Server Statistics:
  Successful File Transfers   : 0
  Failed File Transfers       : 0
  Num of times PUSH initiated : 0
  Num of times PUSH Failed    : 0
  Num of periodic PUSH        : 0
  Num of manual PUSH          : 0
  Current status of PUSH      : Not Running
  Last completed PUSH time    : N/A

Secondary Server Statistics:
```

```
Successful File Transfers   : 0
Failed File Transfers       : 0
Num of times PUSH initiated : 0
Num of times PUSH Failed    : 0
Num of periodic PUSH        : 0
Num of manual PUSH          : 0
Current status of PUSH      : Not Running
Last completed PUSH time    : N/A
```

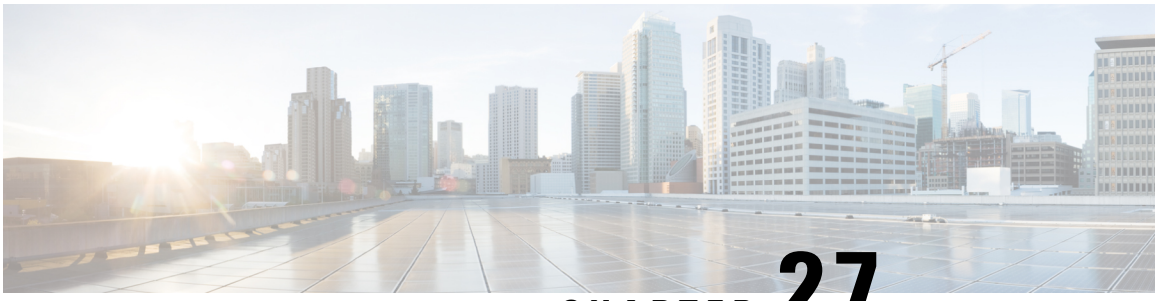
Important Use the **clear hexdump-module statistics** command under the Exec Mode to clear and reset the hexdump module statistics.

*Table 36: **show hexdump-module statistics** Command Output Descriptions*

Field	Description
Hexdump-module-Record file Statistics:	
CDRMOD Instance Id	Indicates the CDRMOD instance id for which the statistics are collected.
Hexdump-module files rotated	Total number of times a hexdump file was closed and a new hexdump file was created.
Hexdump-module files rotated due to volume limit	Total number of times a hexdump file was closed and a new hexdump file was created since the volume limit was reached.
Hexdump-module files rotated due to time limit	Total number of times a hexdump file was closed and a new hexdump file was created since the time limit was reached.
Hexdump-module files rotated due to tariff-time	Total number of times a hexdump file was closed and a new hexdump file was created since the tariff time was reached.
Hexdump-module files rotated due to records limit	Total number of times a hexdump file was closed and a new hexdump file was created since the records limit was reached.
Hexdump-module file rotation failures	Total number of times hexdump file rotation failed.
Hexdump-module files deleted	Total number of times hexdump files were deleted.
Hexdump-module records deleted	Total number of times hexdump records were deleted.
Hexdump-module records received	Total number of times hexdump records were received.
Current open Hexdump-module files	Total number of hexdump files currently open.
Time of last Hexdump-module file deletion	Time of the last deleted hexdump file.
Hexdump-module PUSH Statistics:	
Successful File Transfers	Total number of hexdump files that were successfully transferred.
Failed File Transfers	Total number of hexdump files that failed to transfer.

Field	Description
Num of times PUSH initiated	Total number of times the PUSH operation was initiated.
Num of times PUSH Failed	Total number of times PUSH operation failed.
Num of times PUSH cancelled due to HD failure	Total number of times PUSH operation failed due to hard disk failure.
Num of periodic PUSH	Total number of periodic times PUSH operation was performed.
Num of manual PUSH	Total number of times the PUSH operation was performed manually.
Current status of PUSH	Indicates if the PUSH operation is currently running.
Last completed PUSH time	Indicates the time when the last PUSH operation was completed.
Primary Server Statistics:	
Successful File Transfers	Total number of hexdump files successfully transferred to the primary storage server.
Failed File Transfers	Total number of hexdump files that failed transfer to the primary storage server.
Num of times PUSH initiated	Total number of times PUSH operation was initiated to transfer hexdump files to the primary storage server.
Num of times PUSH Failed	Total number of times PUSH operation failed to transfer hexdump files to the primary storage server.
Num of periodic PUSH	Total number of periodic times PUSH operation was performed to the primary storage server.
Num of manual PUSH	Total number of times the PUSH operation to the primary storage server was performed manually.
Current status of PUSH	Indicates if the PUSH operation to the primary storage server is currently running.
Last completed PUSH time	Indicates the time when the last PUSH operation to the primary storage server was completed.
Secondary Server Statistics:	
Successful File Transfers	Total number of hexdump files successfully transferred to the secondary storage server.
Failed File Transfers	Total number of hexdump files that failed transfer to the secondary storage server.
Num of times PUSH initiated	Total number of times PUSH operation was initiated to transfer hexdump files to the secondary storage server.

Field	Description
Num of times PUSH Failed	Total number of times PUSH operation failed to transfer hexdump files to the secondary storage server.
Num of periodic PUSH	Total number of periodic times PUSH operation was performed to the secondary storage server.
Num of manual PUSH	Total number of times the PUSH operation to the secondary storage server was performed manually.
Current status of PUSH	Indicates if the PUSH operation to the secondary storage server is currently running.
Last completed PUSH time	Indicates the time when the last PUSH operation to the secondary storage server was completed.



CHAPTER 27

PLMN Level Statistics for ePDG Services

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Description

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

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

Configuring PLMN-list

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

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

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

Note List of MCCs with 3 digit MNCs are:

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

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

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

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

Associate PLMN List to ePDG Services

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

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

Notes:

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

Removing PLMN List Configuration

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

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

NOTES:

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

Add or Remove PLMN to or from PLMN list

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

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

NOTES:

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

clear epdg-service statistics

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

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

Notes:

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

Configuring epdg-plmn schema

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

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

NOTES:

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

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

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show epdg-service name

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

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

show plmn-list summary

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

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

show epdg-service statistics plmn mcc mcc_value mnc mnc_value

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

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

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

Field	Description
EAP Server Stats:	
Pass through mode:	
Total Msgs Received	Shows total number of EAP server messages received on pass through mode.
Success Received	Shows total number of successful EAP server messages received on pass through mode.
Diameter Authentication Statistics	
DER TX	Total number of DER messages transmitted.
DEA Challenge RX	Total number of DEA Challenge messages received.
DEA Accept RX	Total number of DEA Accept messages received.
RAR RX	Total number of RAR messages received.
RAA TX	Total number of RAA messages transmitted.
ASR RX	Total number of ASR messages received.
ASA TX	Total number of ASA messages transmitted.
STR TX	Total number of STR messages transmitted.
STA RX	Total number of STA messages received.
S2b Statistics	
GTP Attempts	.Total number of GTP attempts.
GTP Success	Total number of successful GTP sessions.
GTP Failures	Total number of failed GTP sessions.
Create Bearer Request RX	Total number of Create Bearer Request messages received.
Create Bearer Response Accepted TX	Total number of Create Bearer Response Accepted messages transmitted.
Create Bearer Request Discarded RX	Total number of Create Bearer Request Discarded messages received.
Create Bearer Response TX	Total number of Create Bearer Response transmitted.
Create Bearer Response Denied TX	Total number of Create Bearer Response Denied messages transmitted.
Delete Session Request TX	Total number of Delete session requests transmitted.
Delete Session Response Accepted RX	Total number of Delete session response accepted messages received.

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

Bulk Statistics

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

show bulkstats variables ePDG-plmn

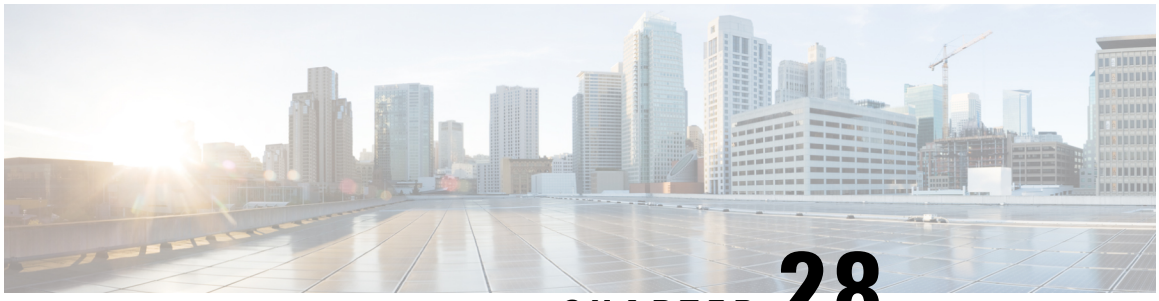
The following PLMN level statistics are added for the existing system level statistics.

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

Variables	Description
plmn-totgtp-curr-ue-in-sys	Displays the total GTP active UEs in the sys
plmn-curses	Displays the total number of current ePDG s
plmn-tot-success-handoff	Displays the total number of successful hand sessions.
plmn-pgw-fallback-succeeded	Displays the total number of P-GW Fallback succeeded.
plmn-pgw-fallback-attempted	Displays the total number of P-GW Fallback attempted.
plmn-reauthor-success	Displays the total number of successful reauth
plmn-reauthor-attempt	Displays the total number of reauthorization a
plmn-eap-rxsuccsrvrpassthru	Displays the total number of EAP-Success m received from the EAP server in pass-throug
plmn-eap-rxttlsrvrpassthru	Displays the total number of EAP messages from the EAP server in pass-through mode.
plmn-sess-disconnect-remote	Displays the total number of Remote disconn sessions.
plmn-sess-disconnect-admin	Displays the total number of Administrator d sessions at PLMN level.
plmn-sess-disconnect-idle-timeout	Displays the total number of disconnect sess to idle timeout reasons.
plmn-sess-disconnect-abs-timeout	Displays the total number of disconnect sess to absolute timeout reasons.
plmn-sess-disconnect-longdur-timeout	Displays the total number of disconnect sess to long duration timeout.
plmn-sess-disconnect-sesssetup-timeout	Displays the total number of sessions discon to setup timeout.
plmn-sess-disconnect-noresource	Displays total number of sessions disconnec nonavailability of resources.
plmn-sess-disconnect-authfail	Displays the total number of session disconn to authentication failure.
plmn-sess-disconnect-flowadd-failure	Displays the total number of session disconn to flow add failure.
plmn-sess-disconnect-invalid-dest	Displays the total number of session disconn to invalid destination context.

Variables	Description
plmn-sess-disconnect-srcaddr-violation	Displays the total number of session disconnects to source address violation.
plmn-sess-disconnect-lmarevoc	Displays the total number of session disconnects to LMA revocation.
plmn-sess-disconnect-dupreq	Displays the total number of sessions disconnec to duplicate requests.
plmn-sess-disconnect-addrassign-failure	Displays the total number of sessions disconnec to address assignation failure.
plmn-sess-disconnect-handoff	Displays the total number of sessions disconnec to LTE and other handoff reasons.
plmn-sess-disconnect-misc	Displays the total number of sessions disconnec to miscellaneous reasons.
SWu Stats	
plmn-ikev2-auth-p1req	Displays the total number of IKEv2 authentication 1 request messages.
plmn-ikev2-auth-p1succ	Displays the total number of IKEv2 authentication 1 success messages.
plmn-ikev2-auth-p1fail	Displays the total number of IKEv2 authentication 1 failure messages.
plmn-ikev2-ikesadelrep-recv	Displays the total number of IKEv2 SA delete r received.
plmn-ikev2-ikesadelrep-sent	Displays the total number of IKEv2 SA delete re sent.
Diameter Authentication Statistics	
plmn-der-req-id-sent	Displays the total number of DER messages transm
plmn-dea-chal-rcvd	Displays the total number of DEA Challenge me received.
plmn-dea-acpt-rcvd	Displays the total number of DEA Accept messa received.
plmn-diamauth-msg-rar	Displays total number of RAR messages receive
plmn-diamauth-msg-raa	Displays the total number of RAA messages transm
plmn-diamauth-msg-asr	Displays the total number of ASR messages rec
plmn-diamauth-msg-asa	Displays the total number of ASA messages transm

Variables	Description
plmn-diamauth-msg-str	Displays the total number of STR messages tr
plmn-diamauth-msg-sta	Displays the total number of STA messages
S2b Statistics	
plmn-totgtp-attempt	Displays the total number of GTP attempts o interface.
plmn-totgtp-success	Displays the total number of successful GTP on S2b interface.
plmn-totgtp-failure	Displays the total number of failed GTP sess
plmn-tun-recv-crebear	Displays the total number of Create Bearer R messages received.
plmn-tun-sent-crebearrespaccept	Displays the total number of Create Bearer R Accepted messages transmitted.
plmn-tun-recv-crebearDiscard	Displays the total number of Create Bearer R Discarded messages received.
plmn-tun-sent-crebearres	Displays the total number of Create Bearer R transmitted.
plmn-tun-sent-crebearrespdenied	Displays the total number of Create Bearer R Denied messages transmitted.
plmn-tun-sent-delsessreq	Displays the total number of Delete session r transmitted.
plmn-tun-recv-delsessrespaccept	Displays the total number of Delete session r accepted messages received.
plmn-tun-recv-delbearreq	Displays the total number of Delete Bearer R messages received.
plmn-tun-sent-delbearrespaccept	Displays the total number of Delete Bearer R messages transmitted.



CHAPTER 28

Pre-ESP Fragmentation Support

This chapter describes ePDG Pre-ESP Fragmentation support.

Feature Description

Inner Fragmentation

EPDG does ESP encapsulation and sends it to the NPU for IPv4 Payload without DF bit set. NPU will fragment the packet before sending out if the packet size exceeds MTU configured on the interface. NPU will do fragment only if the DF bit is not set. Whether to set DF bit or not on outer IP header can be controlled by crypto template configuration. So by default NPU will do a fragmentation if the packet size is more than MTU. This can cause issues if there is NAT device which can't handle fragments. In this case UE will not receive all packets.

To avoid this ePDG can do a fragmentation before ESP encapsulation there by avoiding the fragmentation at NPU. ePDG decides when to do fragmentation is based on existing MTU configuration available under the crypto template. So when the User payload is more than the configured MTU size the packet is fragmented into multiple packets, now each packet is encrypted and ESP encapsulated and sent out.

Memory and Performance Impact

Implementation of pre-ESP Fragmentation support will have performance impact on overall performance. Throughput will be impacted as each fragment will be encrypted and encapsulated. As the throughput mainly depends on the PPS(Packets/Second) and each fragmented packet will result in multiple packets and each packet needs to be encrypted this decreases the throughput of the whole system.

ePDG Pre-ESP Fragmentation Configuration

Configuring Pre-ESP Fragmentation Configuration

Syntax

```
configure
    crypto template
        ip { inner | outer } | ikev2-mtu value  | mtu value }
        default ip { fragment | ikev2 | mtu }
    end
```

show crypto {map | template}

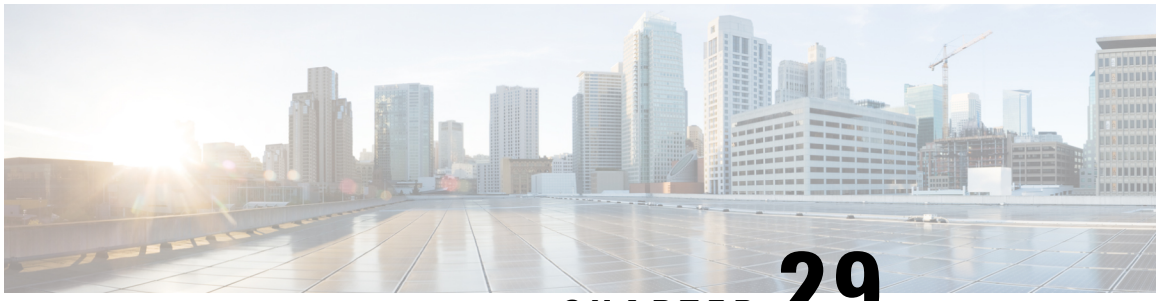
The following show output is added to **show crypto {map | template}** command.

- IPv4 Payload fragment type

show epdg-service statistics

The following show output is added to **show epdg-service statistics** command.

- Total Fragmented Packets
- Total Fragments Sent



CHAPTER 29

RAN/NAS Cause IE support in S2b Messages

Feature Information

Summary Data

Status:	New Feature
Introduced-In Release:	21.2
Modified-In Release(s):	ePDG
Applicable Product(s):	Cisco ASR 5500, VPC-SI, VPC-DI, UGP
Customer Specific:	No
Default Setting:	Disabled
CDETS ID(s)	CSCvd28732
Related Changes in this Release:	NA
Related Documentation:	ePDG Admin Guide, CLI Ref Guide and RCR

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

This feature supports RAN/NAS Cause IE in S2b messages, IE is sent in the below S2b messages:

- Delete Session Request
- Create Bearer Response
- Update Bearer Response

Key functionalities of RAN/NAS Cause IE in S2b Messages:

- IE is sent in delete session request to denote the internal/UE/Diameter cause, which will result in session termination.
- IE is sent in Create Bearer Response to denote the internal cause due to which the "request bearer creation" have to be rejected. As ePDG does not interact with UE/AAA for create bearer request it will send internal cause codes.
- IE is sent in Update Bearer Response to denote the internal cause due to which the "request bearer update" have been rejected. As ePDG does not interact with UE/AAA for update bearer request, so ePDG will send internal cause codes.
- New CLI is introduced under call-control profile which enables/disables sending of RAN/NAS Cause IE and internal failure causes.

Assumptions and Limitations

- eGTPC rejected requests do not have RAN/NAS Cause IE stack.
- If Notify Payload is not received as part of Delete request from UE, internal failure cause would be sent in RAN/NAS cause IE.

Configuring RAN/NAS Cause IE support in S2b

New CLI introduced as part of RAN/NAS Cause IE support in S2b

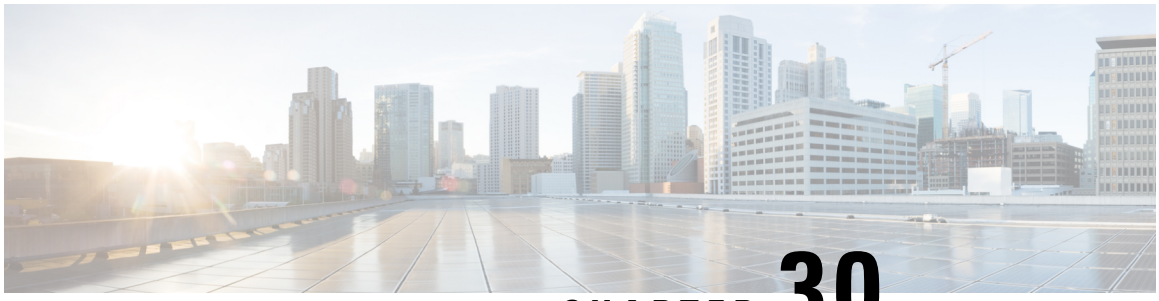
```
config
         call-control-profile  profile_name
         epdg-s2b-gtpv2 send ran-nas-cause internal-failure protocol-type
 8
           [remove] epdg-s2b-gtpv2 send ran-nas-cause internal-failure
        exit
     exit
```

Monitoring and Troubleshooting the ePDG RAN/NAS Cause IE Support In S2b

New show command outputs introduced as part of RAN/NAS Cause IE support in S2b:

show call-control-profile full name

- Sending RAN NAS CAUSE
- Sending RAN NAS CAUSE Internal Failures
- RAN NAS CAUSE Internal Failures Protocol Type



CHAPTER 30

Release 13 Emergency PDN support

Release 13 emergency PDN Support enables UE to make emergency calls when LTE network is not available. This feature is implemented as defined in 3GPP.

Feature Description

Release 13 Emergency PDN Support features

- ePDG will take incoming call as emergency based on presence of "EMERGENCY" in IDr payload in IKE_AUTH_REQUEST message
- ePDG supports Emergency NAI on SWu interface as defined in 3GPP. i.e presence of SOS instead of nai keyword, though whether call is emergency or not is decided by presence of IDr "emergency"
- ePDG blocks all other procedures those are not applicable to emergency sessions
- ePDG provides configuration option for Emergency data of APN name, PGW identity (address/FQDN), default QoS and APN-AMBR
- UE deletes previous IKE sessions when an emergency call is setup and ePDG ensures that no other PDN connections from UE are present when emergency call is setup
- Service Selection AVP will be absent if the UE indicates the establishment of an emergency session during the IKEv2 tunnel establishment

Emergency-Indication AVP in DER and DEA

ePDG which supports emergency services will include Emergency-Indication AVP information element if the UE indicated the establishment of an emergency session during the IKEv2 tunnel establishment.

The 3GPP AAA Server interprets the receipt of the Emergency-Indication AVP as an indication that the UE requests to access the EPC for emergency services.

Introduction of new DPD timer explicit to Emergency Calls

New DPD timer controlled by CLI for emergency calls is introduced. UE may send non-emergency call after emergency call without sending delete for emergency call. With this feature new timer will clear emergency call, post which new non-emergency call will be handled.

With this timer, emergency call gets deleted after sometime if the response is not received. Ideally this timer will be kept low to identify stale session as early as possible. Normal call will be rejected when emergency call is still there.

Assumptions and Limitations

- Ideally UE initiating emergency session deletes the current IKE session
- ePDG will delete previous IKE sessions if any present when emergency call is setup
- The ePDG does not consider HSS provided information to setup a connection, rather uses locally configured PGW and APN information to setup the PDN connection.

Configuring Release 13 Based Emergency APN Support

Use the following configuration to configure Release 13 Based Emergency APN Support:

```
config
   context context_name
        crypto template  crypto_templet_name ikev2-dynamic
           ikev2-ikesa emergency keepalive interval   keepalive_interval
timeout timeout num-retry
         end
```

This feature requires the below existing CLI for configuring Release 13 Based Emergency APN Support:

- lte-policy - lte-emergency-profile *profile_name*
  - ambr
  - apn
  - pgw
  - qos qci
- epdg-service - associate lte-emergency-profile *profile_name*

Performance Indicator Changes

Below are the show commands outputs added as part of Release 13 Emergency PDN Support:

show epdg-service *service_name*

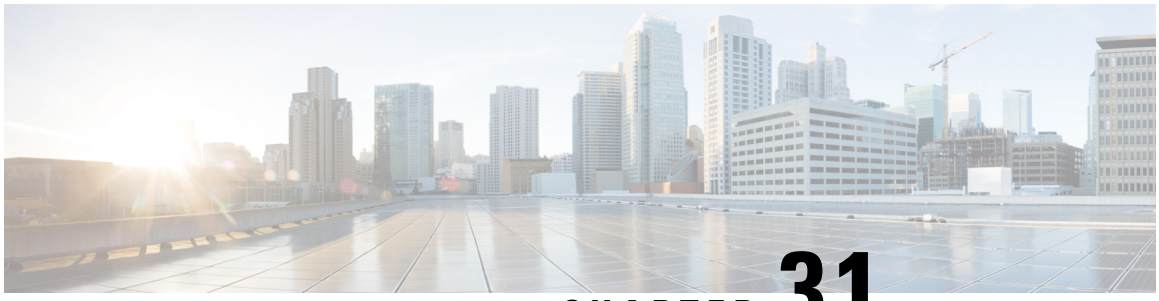
LTE Emergency Profile: <name>/None

- Timeout Idle

show epdg-service statistics

Emergency Sessions:

UICC Sessions:	**Non UICC Sessions:**
Active:	Active:
Setup:	Setup:
Attempts:	Attempts:



CHAPTER 31

Send DSReq if new PGW is selected during re-attach

The ePDG will send the delete session request during reattach if another PGW is selected for current session. If the same PGW is selected for current session during reattach, ePDG will not send the delete session request to PGW and will do local purge.

In case of session creation failure during reattach, ePDG will always trigger delete session request to PGW.

This feature can be enabled by configuring “newcall duplicate-session notify-delete” in ePDG Configuration Mode.

Scope and Assumptions

Scope

1. ePDG will trigger the delete session request if another PGW is selected in case of session successfully created.
2. In case of session creation failure, ePDG will always trigger the delete session request to old PGW.
3. If CLI is not configured then ePDG will do local purge during reattach.

Assumption

ePDG will recover PGW address in session recovery as well as ICSR.

Configuring Send DSReq if new PGW is selected feature

ip

ip { inner | outer } | ikev2-mtu | `mtu value` } is introduced in Crypto Template config mode.

```
configure
    crypto template
        ip { inner | outer } | ikev2-mtu value  }
        default ip { fragment | ikev2 | mtu }
    end
```

Performance Indicator Changes

show crypto {map | template}

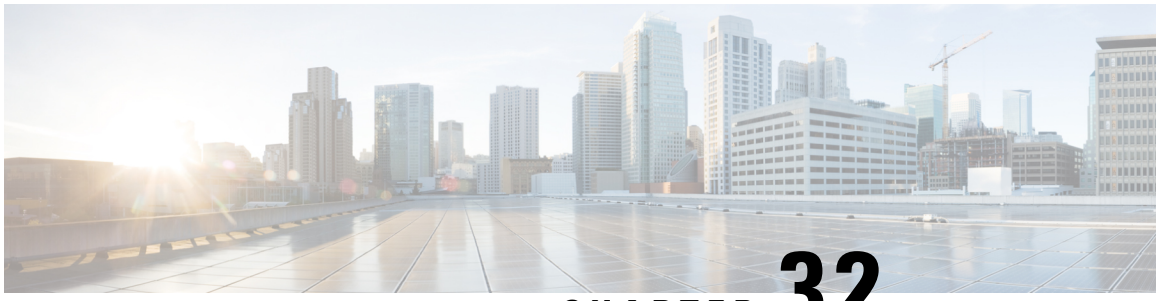
The following show output is added to **show crypto {map | template}** command.

- IPv4 Payload fragment type

show epdg-service statistics

The following show output is added to **show epdg-service statistics** command.

- Total Fragmented Packets
- Total Fragments Sent



CHAPTER 32

Sending SWm 3GPP AAA FQDN Address in CSReq

Sending SWm 3GPP AAA FQDN Address in CSReq feature is CLI controlled feature. This feature is disabled by default.

Feature Description

Overview

- ePDG sends AAA origin-host and origin-realm to PGW in Create Session Request, so that PGW can contact same AAA server for a particular UE for S6b interface. Origin-host and origin-realm are received from AAA server in Diameter-EAP-Answer and Authorization-Authentication-Answer with AVP Origin-Host and Origin-Realm
- These values are sent in optional GTPv2 IE named "3GPP AAA Server Identifier", which is of type "Node Identifier" as defined in TS 29.274

Configuring Sending SWm 3GPP AAA IP Address in CSreq

Use the following configuration to configure Sending SWm 3GPP AAA IP Address in CSreq.

```
config
   context context_name
        call-control-profile  ccp1
           remove epdg-s2b-gtpv2 send aaa-server-id
          end
```

Performance Indicator Changes

Below are the show commands outputs added as part of NPLI e2e for VoWiFi on ePDG and PGW feature.

show subscribers full epdg-service *service_name*

WLAN Location:

- SSID:
- BSSID:
- Civic Address:
- Operator PLMNID:
- RelayAgent Id:
- Circuit Id:
- Timestamp:

show epdg-service statistics

- S2B Context Not Found:

show config

- epdg-s2b-gtpv2 send ue-local-ip-port
- epdg-s2b-gtpv2 send wlan-location-info-timestamp
- epdg-s2b-gtpv2 send message mbr trigger mobike
- epdg-swm send message aar trigger location-retrieval

show call-control-profile full all

ePDG S2b GTPv2 IE Options:

- Sending UE Local IP and UDP Port
- Sending WLAN Location Information/TimeStamp

ePDG S2B GTPv2 Message Options:

Modify Bearer Request:

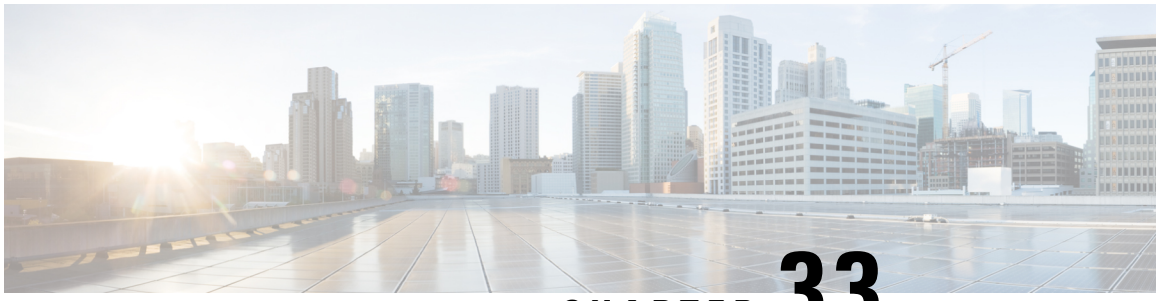
- Triggers
- Mobike

ePDG s2b Swm Message Options:

Authorization and Authenticate Request

- Triggers

  Location-retrieval



CHAPTER 33

Send User location info to PGW

Feature Description

This feature enables 3gpp-user-location-info AVP from SWm interface for constructing ULI and MCCC/MNC of Serving-Network IEs on S2b.

Assumptions and Limitations

- If ULI configuration is enabled and 3GPP-User-Location-Info is not received from AAA, ePDG will not send the same in S2b CSR
- If the MCC/MNC on ServingNetwork is enabled using only CLI, on receiving 3GPP-User-Location-Info, MCC/MNC of Serving Network will be updated and sent on S2b CSR

On receiving 3gpp-user-location-info AVP on SWm interface, ePDG provides ULI IE with TAI or ECGI or TAI-ECGI information on CreateSession Request on S2b

3GPP-User-Location-Info Support on SWm Interface

SWm is existing interface between AAA Server and ePDG which is used to authenticate and authorize UE. There are various procedures between AAA server and ePDG which are used to provide many existing information to two entities.

3GPP-User-Location-Info AVP will be provided to ePDG in DEA/AAA messages at the time Session establishment.

Authenticate and Authorize Procedure: DER/DEA

This information is provided to ePDG first during Authentication and Authorization request procedure i.e DER/DEA or AAR/AAA(for non UICC) exchange which happens during session establishment.

AVP info in Authenticate and Authorization Answer procedure.

Information Element Name	Mapping to Diameter AVP	Cat	Description	Procedure exchange
User Location Information	3GPP-User-Location-Info	O	If present, this IE will contain the location information of the TAI/ECGI/TAI-ECGI info	DEA/AAA
Serving Network	3GPP-User-Location-Info	C	This IE will contain MCC and MNC received on 3GPP-User-Location-Info	DEA/AAA

AAA behavior: If 3GPP-User-Location-Info (that contains last attached LTE location of UE) is present on AAA, it will be provided to ePDG over SWm interface during session establishment in both UICC and non-UICC case.

ePDG Behaviour: On receiving 3GPP-User-Location-Info ePDG stores this information and sends TAI/ECGI/TAI-ECGI information on ULI IE and MCC/MNC information on Serving Network IE over S2b. In case absence of this AVP, ULI will not sent and MCC/MNC values on Serving Network IE will be populated as earlier.

Support on S2b Interface

Information on 3GPP-User-Location-Info received by ePDG will be sent by ePDG to PGW on ULI and Serving Network IE. This feature is CLI controlled under "*call-control-profile*".

Information Element Name	P	Condition / Comment	IE Type	Ins.
User Location Information (ULI)	CO	The ePDG includes this IE on the S2b interface if the 3GPP-User-Location-Info AVP is available.	ULI	0
Serving Network	CO	The ePDG shall include MCC/MNC on this IE, derived from ULI	Serving Network	0

Configuring Use MCC MNC Value Provided by Network

Use the following configuration to configure Use MCC MNC Value Provided by Network.

```
config
       call-control-profile  ccp1
           [ remove ] epdg-s2b-gtpv2 send serving-network value uli
         end

config
       call-control-profile  ccp1
```

```
  [ remove ] epdg-s2b-gtpv2 send uli
end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature to support MCC MNC Value Provided by Network show

call-control-profile full

ePDG S2b GTPv2 IE Options:

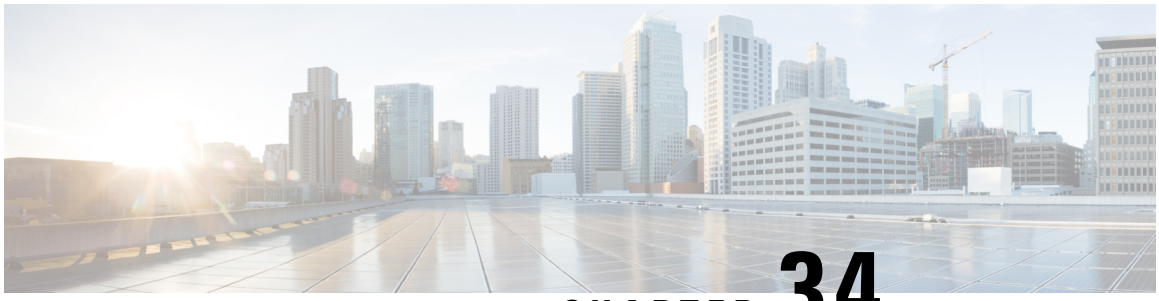
- Sending ULI
- Sending ServingNetwork[Value ULI]

show configuration:

- epdg-s2b-gtpv2 send uli
- epdg-s2b-gtpv2 send serving-network value uli

show configuration verbose:

- remove epdg-s2b-gtpv2 send uli
- remove epdg-s2b-gtpv2 send serving-network value uli



CHAPTER 34

Smart Licensing On/Off for CP Owned Licenses

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.6

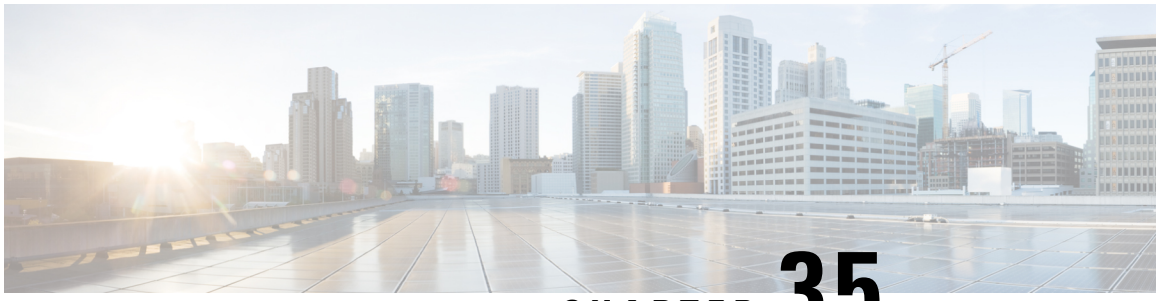
Feature Description

The Smart Licensing model is the contractual model based on trust and verify, and the users are not required to install licenses on their devices making the licensing operations simpler and easier for end users. The Smart Licensing model will work based on client-server, where clients are Cisco products in which smart agent will

be integrated and server is the Cisco Smart Software Manager (CSSM) smart license server residing on Cisco Cloud.

Smart Licensing is supported from release 21.3. With this release ePDG Re-Selection and IPSec additionally support Smart Licensing On/Off feature.

Note For more details, refer *ASR 5500 System Administration Guide/VPC-DI System Administration Guide/VPC-SI System Administration Guide*.



CHAPTER 35

Support for 3gpp IKEv2 Private Notify Error Types

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.5.5

Feature Description

ePDG treats every error returned on S2b from P-GW in the same way and translates to "Internal Address Failure",ePDG also treats SWM from AAA in the same way and translates it to "AUTH Fail" towards UE. This feature translates the errors received on the S2b from the P-GW and SWm from the AAA into 3GPP defined errors on the SWu interface.

A new backoff timer notify payload is introduced to restrict the UE from retrying immediately after certain permanent errors as defined in 3GPP. New CLI command is introduced to control, enable/disable the back off timer value.

Table 37: SWm to SWu Error Mappig Table

Notify Message	Value	Descriptions
NON_3GPP_ACCESS_TO_EPC_NOT_ALLOWED	9000	SWM Result code IE #DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION
USER_UNKNOWN	9001	SWM Result code IE #DIAMETER_ERROR_USER_UNKNOWN
NO_APN_SUBSCRIPTION	9002	SWM Result code IE #DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION or Other scenarios when the requested APN is not included in the user's profile
AUTHORIZATION_REJECTED	9003	SWM Result code IE #DIAMETER_AUTHORIZATION_REJECTED
ILLEGAL_ME	9006	SWM Result code IE #DIAMETER_ERROR_ILLEGAL_EQUIPMENT
NETWORK_FAILURE	10500	SWM Result code IE #DIAMETER_ERROR_UNABLE_TO_COMPLY
RAT_TYPE_NOT_ALLOWED	11001	SWM Result code IE #DIAMETER_RAT_TYPE_NOT_ALLOWED
IMEI_NOT_ACCEPTED	11005	NA
PLMN_NOT_ALLOWED	11011	SWM Result code IE #DIAMETER_ERROR_ROAMING_NOT_ALLOWED
UNAUTHENTICATED_EMERGENCY_NOT_SUPPORTED	11055	The emergency PDN connection request has been rejected due to authentication has failed

Table 38: S2b to SWu Error Mapping Table

Notify Message	Value	Descriptions
PDN_CONNECTION_REJECTION	8192	UE PGW selection failure during attach or handoff scenario.
MAX_CONNECTION_REACHED	8193	The maximum number of PDN connections per UE allowed to be established simultaneously. Max value is 11 due to a limitation in the network mobility procedures. or With “ebi range start <> end <>” CLI under epdg-service max PDN connection per UE change be modified.
SEMANTIC_ERROR_IN_THE_TFT_OPERATION	8241	S2B Error #74 Semantic error in the TFT operation.
SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION	8242	S2B Error #75 Syntactic error in the TFT operation.
SEMANTIC_ERRORS_IN_PACKET_FILTERS	8244	S2B Error #76 Semantic errors in packet filter(s).
SYNTACTICAL_ERRORS_IN_PACKET_FILTERS	8245	S2B Error #77 Syntactic errors in packet filter(s).

Configuring Support for 3GPP IKEv2 Private Notify Error Types

This section provides information on CLI commands available in support of this feature.

Configuring 3GPP IKEv2 Private Notify Error Types

Use the following configuration to enable this feature.

```
configure
  context context_name
    epdg-service service_name
      [ no ] allow 3gpp-swu-priv-notify-error-types
      end
```

Important Either the *Custom S2b/SWm to SWu Error Code Mapping* (existing feature) or the Configuring 3GPP IKEv2 Private Notify Error Types feature can be enabled for epdg-service at a given time.

NOTES:

- **epdg-service** : Creates ePDG service and enters ePDG service configuration mode.

.

- **allow 3gpp-swu-priv-notify-error-types** : Configures 3GPP Rel.13 SWu Private Notify Error Types for S2b, SWm failures.
- **no**: Disables the 3GPP Rel.13 SWu Private Notify Error Types for S2b, SWm failures related parameters.

Configuring the Backoff-Timer

Use the following configuration to enable this feature.

```
configure
   context context_name
      crypto template template_name ikev2-dynamic
       ikev2-ikesa notify-msg-error { network-failure | no-apn-subscription
 } backoff-timer { backoff_timer | deactivate }
        end
```

NOTES:

- **crypto template**: Configures the context level name to be used to identify the Crypto Template.
- **notify-msg-error**: Configures the notify message error type for backoff Timer.
- **network-failure**: Configures backoff timer for notify message error type network-failure(10500).
- **no-apn-subscription**: Cofigures backoff timer for notify message error type no-apn-subscription(9002).
- *backoff_timer*: Configures the number of seconds to inform UE Backoff Timer via notify payload after IKE setup failure.

  Backoff timer must be an Integer from 0 to 35712000 seconds. Default 3600 seconds.
- **deactivate**: Backoff timer value set to deactivate in the notify payload sent to UE after IKE setupfailure.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot the Support for 3GPP IKEv2 Private Notify Error Types feature.

Show Commands and Outputs

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

show epdg-service all

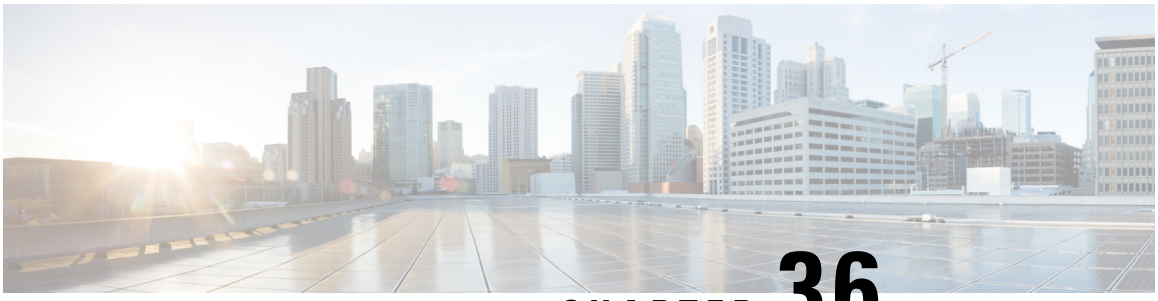
The following new fields are added to the output of this command:

- 3GPP SWu Private Notify Error Types

show crypto template tag test

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

- IKE SA Backoff Timer per Notify Msg Type
  - No APN Subscription
  - Network failure



CHAPTER 36

Support for Diameter Error Code Counters

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG SaMOG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not applicable
Related Documentation	• *ePDG Administration Guide* • *SaMOG Administration Guide* • *AAA Interface Administration and Reference* • *Statistics and Counters Reference, StarOS Release Guide*

Revision History

Revision Details	Release
Supports Diameter error code counters and 5001, 5004 and 5041 experimental result codes for ePDG and SaMOG services.	21.21

Feature Description

In ePDG and SaMOG services, the diameter result code counters are displayed as aggregate counters for different result code ranges, such as 1000-1999, 2000-2999, 3000-3999, 4000-4999 and 5000-5999. For example, 3xxx counter is the cumulative of all result codes that range 3000–3999. These counters are displayed at the global level, for each AAA server group and AAA server levels.

Each answer message from the diameter server, for the request sent from the ePDG and SaMOG, includes a result code or/and an experimental result code AVP. If both, result code and experimental result code AVPs are present, the result code AVP takes precedence. The result codes and experimental result codes are classified as follows:

- 1xxx (Informational) – Errors that fall within this Informational category are used to inform the requester that a request could not be satisfied, and more action is required on its part before access is granted.
- 2xxx (Success) – Result-code that fall within the Success category are used to inform a peer that a request has been successfully completed..
- 3xxx (Protocol Errors) – Errors that fall within the Protocol Errors category is treated on a per-hop basis, and Diameter proxies attempts to correct the error.

Note Protocol errors must only be used in answer messages whose 'E' bit is set.

- 4xxx (Transient Failures) – Errors that fall within the Transient failures category are used to inform a peer that the request could not be satisfied at the time it was received but may be able to satisfy the request in the future.

Note Transient errors must be used in answer messages whose 'E' bit is not set.

- 5xxx (Permanent Failure) – Errors that fall within the Permanent failures category are used to inform the peer that the request failed and should not be attempted again.

Note Permanent errors should be used in answer messages whose 'E' bit is not set.

Counters on each diameter result code help the operators to understand the type of failures. Result code-specific counters are available in the new show command output and in bulk statistics. These counters are available at each AAA server level or as summary of all the AAA servers associated with this ePDG/SaMOG service.

ePDG and SaMOG support the following set of result code-specific counters.

Table 39: Result Code Specific Counters

Error Category	Result Code	t e e	l u s e d o u l a
Protocol Errors [E-bit set] [3XXX]	DIAMETER_UNABLE_TO_DELIVER	2	0 0
	DIAMETER_TOO_BUSY	4	0 0
	DIAMETER_LOOP_DETECTED	5	0 0
	DIAMETER_INVALID_HDR_BITS	8	0 0
	DIAMETER_INVALID_AVP_BITS	9	0 0
Transient Failures [Could not satisfy request at this moment] [4XXX]	DIAMETER_AUTHENTICATION_REJECTED	1	0 0
	DIAMETER_OUT_OF_SPACE	2	0 0
Permanent Failures [To inform peer, request is failed, should not be attempted again] [5XXX]	DIAMETER_ERROR_USER_UNKNOWN	1	0 0
	DIAMETER_UNKNOWN_SESSION_ID	2	0 0
	DIAMETER_AUTHORIZATION_REJECTED	3	0 0
	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	4	0 0
	DIAMETER_MISSING_AVP	5	0 0
	DIAMETER_RESOURCES_EXCEEDED	6	0 0
	DIAMETER_UNABLE_TO_COMPLY	2	1 0
	DIAMETER_USER_UNKNOWN	0	3 0
	DIAMETER_ERROR_USER_NO_WLAN_SUBSCRIPTION	1	4 0

Monitoring and Troubleshooting

Show Commands and Outputs

Show diameter aaa-statistics result-code [all] | [server <server_name>] [group <group_name>]

This command displays the following error codes and descriptions.

Table 40:

Field	Description
Authentication Servers Summary	

Field	Description
Protocol Errors (3xxx]	
Result Code 3002	Shows the aggregate total count of DIAMETER_UNABLE_TO_DELIVER result code value (3002) for all the AAA servers associated with the ePDG service. This error is displayed, if Diameter cannot deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request or because the Destination-Host AVP was specified without the associated Destination-Realm AVP.
Result Code 3004	Shows the aggregate total count of DIAMETER_TOO_BUSY error result code value (3004) only when a specific server is requested and it cannot provide the requested service.
Result Code 3005	Shows the aggregate total count of DIAMETER_LOOP_DETECTED result code value (3005), when an agent detected a loop while trying to get the message to the intended recipient. The message may be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem.
Result Code 3008	Shows the aggregate total count of DIAMETER_INVALID_HDR_BITS result code value (3008), if a request was received whose bits in the Diameter header were set either to an invalid combination or to a value that is inconsistent with the Command Code definition.
Result Code 3009	Shows the aggregate total count of DIAMETER_INVALID_AVP_BITS result code value (3009), if a request was received that included an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition.
Result Code Others	Total number of aggregate count results for 3xxx result codes. This Result Code Others does not match with any of the other specific result codes counter.
Transient Failures (4xxx)	
Result Code 4001	Shows the aggregate total count of DIAMETER_AUTHENTICATION_REJECTED result code value (4001), when the authentication process fails, due to an invalid password used by the user. Further attempts must only be allowed after prompting the user for a new password.
Result Code 4002	Shows the aggregate total couunt of DIAMETER_OUT_OF_SPACE Result code value (4002), when a Diameter node receives the accounting request but was unable to commit it to stable storage due to a temporary lack of space.
Result Code Others	Total number of aggregate count result for 4xxx result codes. This Result Code Others does not match with any of the other specific result codes counter.
Permanent Failures (5xxx]	

Field	Description
Result Code 5002	Displays the aggregate total count of DIAMETER_UNKNOWN_SESSION_ID result code value (5002), if the request contains an unknown Session-Id.
Result Code 5003	Displays the aggregate total count of DIAMETER_AUTHORIZATION_REJECTED (5003) result code value, if a request was received for which the user could not be authorized. This error occurs if the requested service is not permitted to the user.
Result Code 5005	Displays the aggregate total count of DIAMETER_MISSING_AVP (5005) result code value, if a request did not contain an AVP that is required by the Command Code definition. **Important** If this value is sent in the Result-Code AVP, a Failed-AVP should be included in the message. The Failed-AVP must contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes.
Result Code 5006	Displays the aggregate total count of DIAMETER_RESOURCES_EXCEEDED (5006) result code value, when a request was received that cannot be authorized because the user has already used the allowed resources. For example, error occurs when a user is restricted to one dial-up PPP port, attempts to establish a second PPP connection.
Result Code 5012	Displays the aggregate total count of DIAMETER_UNABLE_TO_COMPLY (5012) result code value, if an error is returned when a request is rejected for unspecified reasons.
Result Code 5030	Displays the aggregate total count of DIAMETER_USER_UNKNOWN (5030) result code value.
Result Code Others	Total number of aggregate count result for 5xxx result codes. This Result Code Others does not match with any of the other specific result codes counter.
Experimental Result Code Stats	
Exp Result Code 5001	Total number of times the Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN (5001) is received in the authentication response message.
Exp Result Code 5004	Total number of times the Experimental-Result-Code DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004) is received in the authentication response message.
Accounting Servers Summary	
Protocol Errors (3xxx]	

Field	Description
Result Code 3002	Shows the aggregate total count of DIAMETER_UNABLE_TO_DELIVER result code value (3002), if Diameter cannot deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request or because the Destination-Host AVP was specified without the associated Destination-Realm AVP.
Result Code 3004	Displays the aggregate total count of DIAMETER_TOO_BUSY error result code value (3004) only when a specific server is requested and it cannot provide the requested service.
Result Code 3005	Shows the aggregate total count of DIAMETER_LOOP_DETECTED result code value (3005), when an agent detected a loop while trying to get the message to the intended recipient. The message may be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem.
Result Code 3008	Shows the aggregate total count of DIAMETER_INVALID_HDR_BITS result code value (3008), if a request was received whose bits in the Diameter header were set either to an invalid combination or to a value that is inconsistent with the Command Code definition.
Result Code 3009	Shows the aggregate total count of DIAMETER_INVALID_AVP_BITS result code value (3009), if a request was received that included an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition.
Result Code Others	Total number of aggregate count results for 3xxx result codes. This Result Code Others does not match with any of the other specific result codes counter.
Transient Failures (4xxx)	
Result Code 4001	Shows the aggregate total count of DIAMETER_AUTHENTICATION_REJECTED result code value (4001), when the authentication process fails, due to an invalid password used by the user. Further attempts must only be allowed after prompting the user for a new password.
Result Code 4002	Shows the aggregate total count of DIAMETER_OUT_OF_SPACE Result code value (4002), when a Diameter node receives the accounting request but was unable to commit it to stable storage due to a temporary lack of space.
Result Code Others	Total number of aggregate count results for 4xxx result codes. This Result Code Others does not match with any of the other specific result codes counter.
Permanent Failures (5xxx]	
Result Code 5002	Displays the aggregate total count of DIAMETER_UNKNOWN_SESSION_ID result code value (5002), if the request contains an unknown Session-Id.

Field	Description
Result Code 5003	Displays the aggregate total count of DIAMETER_AUTHORIZATION_REJECTED (5003) result code value, if a request was received for which the user could not be authorized. This error occurs if the requested service is not permitted to the user.
Result Code 5005	Displays the aggregate total count of DIAMETER_MISSING_AVP (5005) result code value, if a request did not contain an AVP that is required by the Command Code definition. **Important** If this value is sent in the Result-Code AVP, a Failed-AVP should be included in the message. The Failed-AVP must contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes.
Result Code 5006	Displays the aggregate total count of DIAMETER_RESOURCES_EXCEEDED (5006) result code value, when a request was received that cannot be authorized because the user has already expended allowed resources. For example, error occurs when a user is restricted to one dial-up PPP port, attempts to establish a second PPP connection.
Result Code 5012	Displays the aggregate total count of DIAMETER_UNABLE_TO_COMPLY (5012) result code value, if an error is returned when a request is rejected for unspecified reasons.
Result Code 5030	Displays the aggregate total count of DIAMETER_USER_UNKNOWN (5030) result code value.
Result Code Others	Total number of aggregate count results for 5xxx result codes. This Result Code Others does not match with any of the other specific result codes counter.
Experimental Result Code Stats	
Exp Result Code 5001	Total number of times the Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN (5001) is received in the authentication response message.
Exp Result Code 5004	Total number of times the Experimental-Result-Code DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004) is received in the authentication response message.

Bulk Statistics

This section provides bulkstats related to diameter-auth and diameter-acct schemas for ePDG and SaMOG services.

diameter-acct Schema

The following counters are available in the Diameter Accounting schema for the following error codes.

Bulk Statistics	Description
acct-result-unable-to-deliver	Shows the total number of Diameter account results with a result code 3002 that cannot be delivered to the destination.
acct-result-too-busy	Shows the total number of Diameter account results with a result code 3004 that cannot be allowed for the requested service, when specific servers are requested for.
acct-result-loop-detected	Shows the total number of Diameter account results with a result code 3005 that an agent detected a loop while trying to get the message to the inteded recipient.
acct-result-invld-hdr-bits	Shows the total number of Diameter account results with a result code 3008 for an invalid header bits request received. A request received could be related to bits in the diameter header , which is set either to an invalid combination or to a value that is inconsistent with the definition of the Command Code.
acct-result-invld-avp-bits	Shows the total number of Diameter account results with a result code 3009 for a request received. The diameter code includes an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition.
acct-result-authen-rej	Shows the total number of Diameter account results with a result code 4001 for the user authentication failure due to an invalid password used by the user.
acct-result-out-of-space	Shows the total number of Diameter account results with a result code 4002 for a Diameter node received but was unable to commit due to a temporary lack of space.
acct-exp-result-user-unknown	Shows the total number of Diameter account expected results with a result code 5001 for the unknown user error.
acct-result-unk-sess-id	Shows the total number of Diameter account results with a result code 5002 that contains unknown session Identifiers.
acct-result-author-rej	Shows the total number of Diameter account results with a result code 5003 where the user requests could not be authorized.
acct-exp-result-roaming-not-allowed	Shows the total number of Diameter expected account results with a result code 5004 for which roaming calls are not allowed.

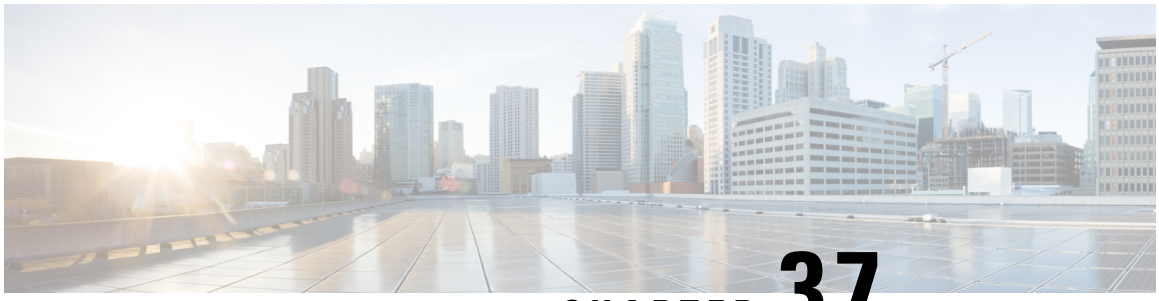
Bulk Statistics	Description
acct-result-missing-avp	Shows the total number of Diameter account results with a result code 5005 that does not contain an AVP.
acct-result-resrc-exceed	Shows the total number of account results with a result code 5006 that cannot be authorized because the user has already used allowed resources.
acct-result-unable-to-comply	Shows the total number of account results with a result code 5012 rejected for unspecified reasons.
acct-result-user-unknown	Shows the total number of account results with a result code 5030 that contains unknown users.
acct-exp-result-no-wlan-subs	Shows the total number of expected account results with a result code 5041 for no VLAN sub band.

diameter-auth Schema

The following counters are available in the Diameter Authentication/Authorization schema for the following error codes.

Bulk Statistics	Description
auth-result-unable-to-deliver	Shows the total number of diameter authentiction/authroization results with a result code 3002 that cannot be delivered to the destination.
auth-result-too-busy	Shows the total number of Diameter authentication/authorization results with a result code 3004 that cannot be allowed for the requested service, when specific servers are requested for.
auth-result-loop-detected	Shows the total number of Diameter authentication/authorization results with a result code 3005 that an agent detected a loop while trying to get the message to the inteded recipient.
auth-result-invld-hdr-bits	Shows the total number of Diameter authentication/authorization results with a result code 3008 for an invalid header bits request received. A request received could be related to bits in the diameter header that is set either to an invalid combination or to a value that is inconsistent with the definition of the Command Code.
auth-result-invld-avp-bits	Shows the total number of Diameter authentication/authorization results with a result code 3009 for a request received. This Diameter authentication/authorization results includs an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition.

Bulk Statistics	Description
auth-result-authen-rej	Shows the total number of Diameter authentication/authorization results with a result code 4001 for the user authentication failure due to an invalid password used by the user.
auth-result-out-of-space	Shows the total number of Diameter authentication/authorization results with a result code 4002 for a Diameter node received but was unable to perform stable commit due to a temporary lack of space.
auth-exp-result-user-unknown	Shows the total number of Diameter authentication/authorization expected results with a result code 5001 for the unknown user error.
auth-result-unk-sess-id	Shows the total number of Diameter authentication/authorization results with a result code 5002 that contains unknown session Identifiers.
auth-result-author-rej	Shows the total number of Diameter authentication/authorization results with a result code 5003 where the user requests could not be authorized.
auth-exp-result-roaming-not-allowed	Shows the total number of Diameter authentication/authorization expected results with a result code 5004 for which roaming calls are not allowed.
auth-result-missing-avp	Shows the total number of Diameter authentication/authorization results with a result code 5005 that does not contain an AVP.
auth-result-resrc-exceed	Shows the total number of Diameter authentication/authorization results with a result code 5006 that cannot be authorized because the user has already used allowed resources.
auth-result-unable-to-comply	Shows the total number of Diameter authentication/authorization results with a result code 5012 rejected for unspecified reasons.
auth-result-user-unknown	Shows the total number of Diameter authentication/authorization results with a result code 5030 that contains unknown users.
auth-exp-result-no-wlan-subs	Shows the total number of expected diameter authentication/authorization results with a result code 5041 for no VLAN sub band.



CHAPTER 37

Support for RFC 5685 Redirect Mechanism for Internet Key Exchange Protocol V2(IKEv2)

This chapter describes support for RFC 5685 Redirect Mechanism for Internet Key Exchange Protocol V2 (IKEv2).

Feature Description

Overview

ePDG complies with RFC 5685 partially. The Internet Key Exchange Protocol version 2 (IKEv2) is a protocol for setting up Virtual Private Network (VPN) tunnels from a remote location to a gateway so that the VPN client can access services in the network behind the gateway. The SWu interface between UE and ePDG also uses IKEv2 to establish secured tunnel over untrusted Wifi access. RFC 5685 defines an IKEv2 extension that allows an overloaded ePDG or an ePDG that is being shut down for maintenance to redirect the UE to attach to another ePDG.

ePDG supports the following:

- Additional payloads specified in RFC 5685 in the IKEv2 stack.
- Optimized backhaul utilization by redirecting a UE to another ePDG closer to the last-visited (and possibly topologically closest to UE) PGW for the UICC devices. This redirection is implemented based on RFC5685.
- For non-UICC devices the HSS may not have any entry of last visited PGW and the location of the device is identified based on the IPSec tunnel endpoint address. The AAA server can access a database which maps IP address range to the closest PGW identity and with that the same mechanism is used to redirect the UE to the closest PGW.

Limitations

With this release 20.1 compliance to RFC 5685 is limited to get peak hour traffic redirection from one zone to another zone to achieve better overall capacity management.

Scope & Assumptions

Scope

1. ePDG supports validation and parsing of REDIRECT_SUPPORTED and REDIRECTED_FROM payloads in IKE_INIT messages from UE as per RFC 5685.
2. ePDG supports inclusion of REDIRECT payload with IPv4 or IPv6 address in the final IKE_AUTH message to UE.
3. REDIRECT payload in IKE_INIT Response and Information Request message will not be supported.
4. REDIRECT payload in IKE_AUTH message will not support sending ePDG FQDN.
5. In case the AAA server sends multiple APN configurations in DEA message and more than one has a PGW FQDN present in APN configuration, ePDG will just use the one associated with the selected APN. All other PGW identities will be ignored and will not be used for DNS query and filtering of the alternate ePDG node.

Assumptions

1. UE supports IKEv2 redirection as per RFC 5685.
2. DNS servers can be configured with APN FQDN for APNs serviced by ePDG with the service parameter.
3. HSS will always retain the last visited PGW identity (FQDN) and will send it to ePDG via AAA server on Swm interface.
4. The LTE network will perform PGW selection based on topological proximity and if the UE performs LTE attach the last visited PGW identify in HSS closest to the UE location.
5. The ePDG will be configured to do topology based DNS query for PGW nodes during initial attach. This would ensure that WiFi attach also goes to the topologically closest PGW once an ePDG is selected after re-direction.

ePDG Reselection Configuration

Configuring ePDG Reselection Configuration

Syntax

```
configure
    apn-profile
        gateway-selection alternate-epdg strip-labels strip_labels
max-alternate-pgw max_alternate_pgw_attempts
        remove gateway-selection alternate-epdg strip-labels strip_labels
max-alternate-pgw
    end
```

show crypto ikev2 security-association

The following show output is added to **show crypto ikev2 security-association** command as part of this release.

- Redirection Supported
- Redirection From

show apn-profile full all

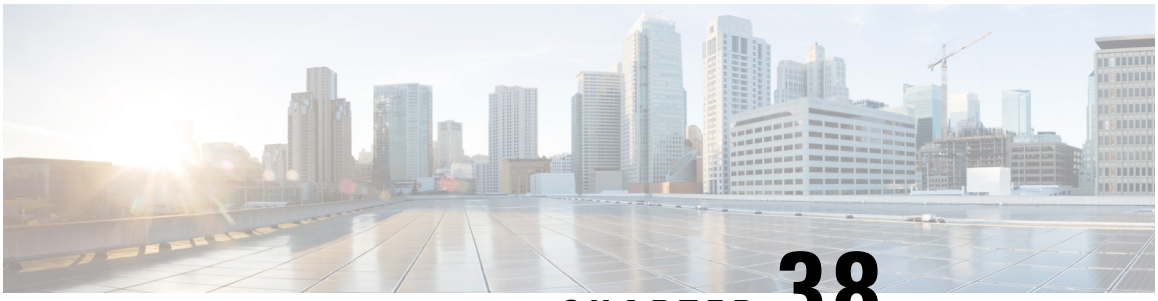
The following show output is added to **show apn-profile full all** command as part of this release.

- Alternate ePDG Selection
- Num Stripped Labels

show epdg statistics

The following bulk statistics are added under Alternate ePDG Selection Stats section.

- Redirect-enabled UE
- Selection Required
- Selection Aborted
- Selection Initiated
- Selection Succeeded
- Selection Failed



CHAPTER 38

Transition Rate KPIs

This chapter describes the following topics:

Feature Description

Session Events Per Second, key performance indicators (KPIs) did not differentiate between successful or unsuccessful PDN session activations and deactivations. In addition, the KPIs did not provide any information related to the Voice-over-LTE (VoLTE) service.

To calculate CEPS(Call Event Per Second) which measures the signaling load on the system, operator needs to use historical data (via bulkstats) collected periodically. Also, the meaning of CEPS is defined as setting up and tearing down a call (PDN session, not VoLTE calls) along with all the interactions (messages) on ePDG interfaces (SWu, SWm and S2b). In StarOS release 20, Session Events Per Second (SEPS) KPIs have been implemented to address these issues.

1. **Session Events Per Second (SEPS)**

   New KPI that measures a total number of session setup (IKE session setup) and session tear down (IKE SA Delete Request from peer) events (both successful and unsuccessful) per second. SEPS KPI will be calculated at ePDG and provided using CLI show commands and bulkstats data.

   The SEPS KPI have the following counters:

   - **Session Events:** Increments when a new IKE_SA_INIT Request and IKE_SA_DELETE Request received from peer. It will not increment for retry messages and IKE_SA_DELETE Request received for rekeyed IKE_SA.
   - **Successful Session Events:** Increments when a successful session creation (when final IKE_AUTH rsp is sent after PGW allocates UE's internal IP address). It also increments for successful IKE_SA_DELETE response sent for peer initiated delete request received.
   - **Unsuccessful Session Events:** Increments to an unsuccessful session creation attempt which failed at IKE_SA_INIT, IKE_AUTH or PGW PDN allocation phase. In summary, any session deletion before it was successfully created. (Failure sent by peer, setup timer expiry etc). The counter also increments if IKE_SA_DELETE Request was dropped, or response was sent with error notify, if any.

2. **Call Events Per Second (CEPS)**

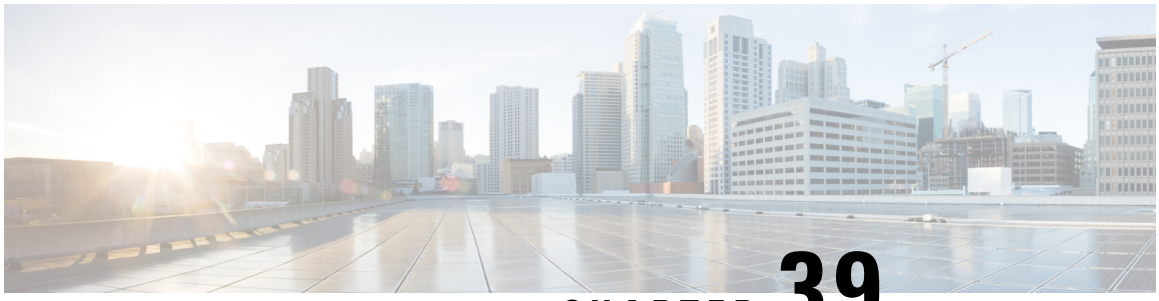
New KPI that measures a total number voice VoLTE (QCI=1, configurable) calls setup (Create Bearer Request) and tear down (Delete Bearer Request) events (both successful and unsuccessful) per second. CEPS KPI will be calculated at ePDG and provided using CLI show commands and bulkstats data.

The CEPS KPI have the following counters:

- **Call Events:** Increments when Create Bearer Req received for QCI-1. It also increments when Delete Bearer Request received for QCI-1. Delete session Request received, where a dedicated bearer with QCI-1 was present.
- **Successful Call Events:** Increments when Created Bearer Response sent successfully for QCI-1 and Delete Bearer Response sent successfully for QCI-1. Delete session Rsp sent successfully, where dedicated bearer with QCI-1 was present.
- **Unsuccessful Call Events:** Increments when Create Bearer Response and Delete Bearer Response was sent with cause IE not equal to "Request Accepted" or either of messages was dropped due to any reason. (for QCI-1).

Assumptions and Limitations

1. The SEPS or CEPS counter do not incremented if the packet is dropped at npu.
2. Change in bucket interval using CLI will reset all(both SEPS and CEPS) the pegged counters to zero including historical data.
3. Change in QCI value to peg CEPS counters will reset all historical data for CEPS.
4. SR will reset the counters for respective ipsecmgr or sessmgr.
5. Unplanned card migration will reset the counters for all sessmgr and ipsecmgrs on the card.
6. The SEPS/CEPS values will sync on ICSR standby chassis, so there is no impacts for ICSR upgrade or downgrade scenarios.
7. The SEPS statistics is not collected from ipsecdemux (if dropped), so some SEPS attempts would be lost if it is a non Cisco ASR 5500 platform.
8. If the final IKE_AUTH resp is rejected by peer due to invalid syntax or authentication failure etc are not taken into consideration for unsuccessful SEPS event. It would be counted as successful SEPS event for session creation and session deletion separately.



CHAPTER 39

Tunnelling of Explicit Congestion Notification

This chapter describes the tunneling of Explicit Congestion Notification (ECN) for ePDG in the following sections:

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	Enabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

ePDG supports tunneling of Explicit Congestion Notification (ECN) so that the network can detect and react to network congestions. This feature is compliant to *RFC 6040 - Tunnelling of Explicit Congestion Notification*.

ECN tunneling supports the default tunnel ingress behavior (encapsulation) and default tunnel egress behavior (decapsulation) as per RFC 6040. The "normal mode" and "compatibility mode", are two modes of encapsulation required for ECN. These modes are specific only to the ingress tunnel endpoint, and not the whole tunnel. A tunnel ingress must implement the normal mode and the compatibility mode for backward compatibility with tunnel egresses that do not propagate explicit congestion notifications.

The ECN tunneling feature can be enabled in normal mode or compatible mode using the S2b-GTP and SWu-IPsec interfaces.

- **S2b interface**: For GTP tunneling in the S2b interface, the ECN enabling is done for the session based on the configuration in the call control profile associated with the session. The same configuration controls both ingress and egress for the S2b-GTP interface.
- **SWu interface**: For IPsec tunneling in the SWu interface, the ECN enabling is done based on the configuration in the crypto template associated with the ePDG service. The same configuration controls both ingress and egress for the SWu-IPsec interface.

Relationships to Other Features

SR/ICSR Recovery: For session recovery or unplanned card migration, the ECN must be updated properly based on the mode during encapsulation and decapsulation.

Standards Compliance

The ECN Tunneling feature complies with the following standards:

- *RFC 6040 - Tunnelling of Explicit Congestion Notification*

Configuring ECN Tunneling

This section describes the configuration to enable ECN in normal or compatible mode in GTP tunnel over S2b interface and IPsec tunnel over SWu interface.

Configuring ECN for GTP Tunnel

Use the following configuration to enable explicit congestion notification (ECN) in normal mode or compatible mode for the GTP tunnel in S2b interface.

```
configure
  call-control-profile profile_name
    ecn gtp mode normal
    remove ecn gtp mode
    end
```

Notes:

- **ecn**: Specifies ECN over GTP tunnel in normal mode.
- **gtp**: Enables ECN handling over GTP tunnel.
- **mode**: Specifies the tunnel ingress encapsulation mode.
- **normal**: Specifies the normal mode of encapsulation.
- **remove**: Enables ECN in compatible mode for GTP tunnel in the S2b interface. The default mode is the compatible mode, supported for backward compatibility.

Verifying the Configuration

Use the following command to verify the ECN configuration for GTP tunnel in the S2b interface:

```
show call-control-profile full all
```

Configuring ECN for IPsec Tunnel

Use the following configuration to enable explicit congestion notification (ECN) in normal mode or compatible mode for IPsec tunnel in the SWu interface.

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
      [ no ] ecn
      end
```

Notes:

- **ecn**: Specifies ECN over IPsec tunnel in normal mode.
- **no**: Enables ECN in compatible mode for IPsec tunnel in the SWu interface. The default mode is the compatible mode, supported for backward compatibility.

Verifying the Configuration

Use the following command to verify the ECN configuration for IPsec tunnel in the SWu interface:

```
show crypto template tag map_name
```

Monitoring and Troubleshooting ECN Tunneling

This section provides information on how to monitor and troubleshoot the ECN Tunneling feature.

Show Commands and Outputs

This section provides information on show commands and their corresponding outputs for the ECN Tunneling feature.

show call-control-profile full all

The **Gtp Tunnel ECN Ingress Mode** field is added to the output of this command to display the mode of ECN configured for the GTP tunnel.

show crypto template tag

The **Ipsec Tunnel Ecn Ingress Mode** field is added to the output of this command to display the mode of ECN configured for the IPsec tunnel.

show daughtercard counters

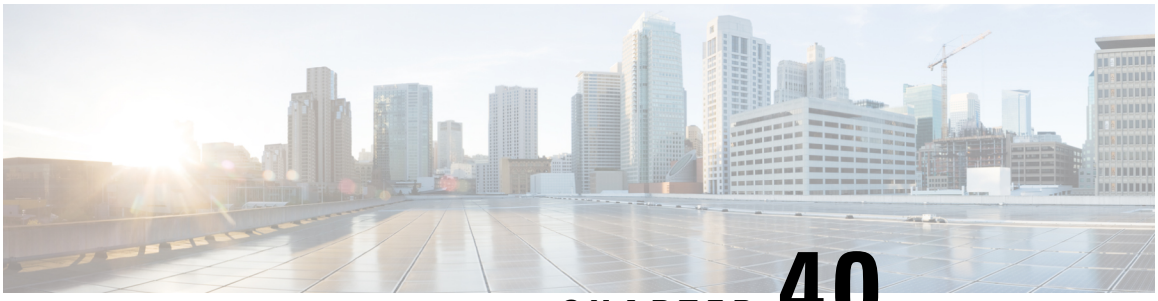
The following new fields are added to the output of this command:

- ECN Total Pkts drop: Total number of packet drops due to unexpected ECN field.
- ECN CU Pkts: Total number of packets with currently unused (CU) combination of ECN handling.

show epdg-service statistics

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

- ECN Total Pkts drop: Total number of packet drops due to unexpected ECN field.
- ECN CU Pkts: Total number of packets with currently unused (CU) combination of ECN handling.



CHAPTER 40

User Equipment Identity in IKE_AUTH Message

The following topics are discussed:

Feature Description

Overview

On untrusted WLAN networks that support Mobile Equipment Identity signalling, ePDG can request the subscriber's User Equipment (UE) for the International Mobile Equipment Identity (IMEI) or IMEI SV (Software Version) information, when the UE does not share this information in the first IKE_AUTH_REQ message in the configuration attributes. On receiving the IMEI or IMEI SV information from the UE, ePDG can share this information with the AAA server in the Diameter EAP Request (DER) message over the SWm interface, and in the ME Identity (MEI) IE with P-GW in the second Create Session Request (CSR) message over the S2b interface.

How UE Identity in IKE_AUTH Message Works

Architecture

During IKEv2 authentication and security association (SA) establishment for UICC devices, when the UE does not share the IMEI or IMEI SV information in the first IKE_AUTH_REQ message, ePDG can request the UE for this information. ePDG includes a DEVICE_IDENTITY notify payload in the IKE_AUTH_RESP message to UE. Based on the availability of IMEI or IMEI SV information, the UE includes the value in the DEVICE_IDENTITY attribute with the Identity Type field set to IMEI or IMEI SV. The UE then shares this information with ePDG in the second IKE_AUTH_REQ message. The structure of the DEVICE_IDENTITY notify payload is as defined in *3GPP TS 24.302*.

ePDG can be configured to request the UE for the IMEI or IMEISV information using the **notify-payload device-id** command under the Crypto Template Configuration Mode. For more configuration information, refer the configuration section of this chapter.

For non-UICC devices, ePDG will not request for the IMEI or IMEI SV information from the UE for single exchange authentication methods like certificate-based authentication. For other authentication methods that uses multiple IKE_AUTH exchanges, the behaviour to request for the IMEI or IMEI SV information is the same as that of UICC devices.

Standards Compliance

This feature complies with the following standards:

- **3GPP TS 24.302**: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3"

Configuring UE Identity in IKE_AUTH Message

Use the following configuration to enable ePDG to request the UE for the IMEI or IMEI SV information using the DEVICE_IDENTITY notify payload:

```
config
    context context_name
        crypto template template_name ikev2-dynamic
           notify-payload device-id
           end
```

Notes:

- Use the **no notify-payload device-id** command to disable the configuration.
- Use the **default notify-payload device-id** command to restore the configuration to its default value.
- **Default:** Enabled

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

show crypto statistics ikev2

The following fields are available in the output of the **show crypto statistics ikev2** command in support of this feature:

```
Total IKEv2 Notify Statistics:
    Device ID Req Sent:   0
    Device ID Rsp Rcvd:   0
```

*Table 41: **show crypto statistics ikev2** Command Output Descriptions*

Field	Description
Total IKEv2 Notify Statistics:	
Device ID Req Sent	Total number of IKEv2 Notify payloads sent (device id).
Device Identity Rsp Rcvd	Total IKEv2 Notify payloads received (device id).

show crypto template

The following field is available in the output of the **show crypto template** command in support of this feature:

```
IKEv2 Notify Payload:
    Device Identity: Enabled [Default]
```

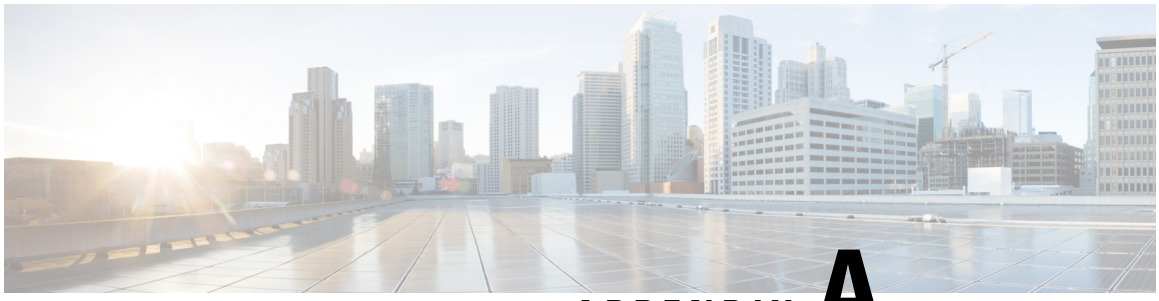
*Table 42: **show crypto template** Command Output Descriptions*

Field	Description
IKEv2 Notify Payload:	
Device Identity	Indicates if ePDG is configured to request for device identity in the IKEv2 Notify payload message.

Bulk Statistics

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

Variable	Description	Data Type
ikev2-notifpaysent-deviceid	**Description:** Total number of IKEv2 Notify payloads sent (device id). **Triggers:** Increments when ePDG sends a Device Identity Notify Payload. **Availability:** ePDG Service **Type:** Counter	Int32
ikev2-notifpayrecv-deviceid	**Description:** Total IKEv2 Notify payloads received (device id). **Triggers:** Increments when ePDG receives a Device Identity Notify Payload. **Availability:** ePDG Service **Type:** Counter	Int32



APPENDIX A

Evolved Packet Data Gateway Engineering Rules

This appendix provides ePDG (evolved Packet Data Gateway) engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

The following rules are covered in this appendix:

IKEv2/IPSec Restrictions

The following is a list of known restrictions for IKEv2 and IPSec:

- IKEv2 as per RFC 5996 is supported. IKEv1 is not supported.
- MOBIKE is not supported.
- Only one Child SA is supported.
- Each ePDG service must specify one crypto template.
- Per RFC 4306 and RFC 4718, the following known restrictions apply with respect to the payload and its order. Violations result in INVALID_SYNTAX being returned which is being enabled or disabled through a configuration CLI.
-
  - While RFC 4306 Section 2.19 specifies that the "CP payload MUST be inserted before the SA payload," the ePDG does not force strict ordering of this. The ePDG processes these payloads as long as the UE sends a CP payload anywhere inside the encryption data.
  - While RFC 4306 Section 2.23 specifies "The location of the payloads (Notify payloads of type NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP) in the IKE_SA_INIT packets are just after the Ni and Nr payloads (before the optional CERTREQ payload)," the ePDG does not force strict ordering of this and still can process these NOTIFY payloads.
- ePDG egress processing will ensure that payloads are in order.
- As described above, when the ePDG receives IKEv2 messages, the ePDG does not enforce the payloads to be in order. However, when the ePDG sends the response or generates any IKEv2 messages, the ePDG will ensure that payloads are ordered according to RFC 4306.

- Traffic selector payloads from the UE support only traffic selectors by IP address range. In other words, the IP protocol ID must be 0. The start port must be 0 and the end port must be 65535. IP address range specification in the TSr payload is not supported.
- Only IKE and ESP protocol IDs are supported. AH is not supported.
- The IKE Protocol ID specification may not use the NONE algorithm for authentication or the ENCR_NULL algorithm for encryption as specified in Section 5 (Security Considerations) of RFC 4306.
- In ESP, ENCR_NULL encryption and NONE authentication cannot be simultaneously used.

X.509 Certificate (CERT) Restrictions

The following are known restrictions for the creation and use of X.509 CERT:

- The maximum size of a CERT configuration is 4096 bytes.
- The ePDG includes the CERT payload only in the first IKE_AUTH Response for the first authentication.
- If the ePDG receives the CERT-REQ payload when it is not configured to use certificate authentication and if the CRITICAL bit is set in the IKE_AUTH request, the ePDG will reject the exchange. If the ePDG receives the CERT-REQ payload when it is not configured to use certificate authentication and if the CRITICAL bit is not set, the ePDG ignores the payload and proceeds with the exchange to be authenticated using EAP.
- Only a single CERT payload is supported. While RFC 4306 mandates the support of up to four certificates, the ePDG service will support only one X.509 certificate per context. This is due to the size of an X.509 certificate. Inclusion of multiple certificates in a single IKE_AUTH may result in the IKE_AUTH message not being properly transmitted.

GTPv2 Restrictions

The following are known restrictions for the creation and use of GTPv2:

- The ePDG should not send Delete PDN connection set request message per 23.007 for the FQ-CSID failure.
- The ePDG does not support allowing the UE to have more than one PDN connection with one APN.
- The ePDG should not handle the delete PDN connection set request received from PGW, basically terminating all the sessions corresponding to the PGW FQ-CSID present in "delete PDN connection set request" message.
- The ePDG should not be allowed to send "Trace Activation/Deactivation" message to PGW for subscriber tracing when same is notified to ePDG on the SWm interface with presence of "Trace Information" AVP.
- The ePDG should not do any policy (QoS) enforcement, ePDG should only be doing the UL traffic QCI to DSCP mapping and marking. Downlink traffic marking shall be done at PGW and ePDG should not handle DSCP for same including the pass through mode marking. ePDG should be be communicating the static QoS profile received from the AAA to the PGW.
- The ePDG does not have CAC/Admission control functionality.
- The ePDG does not supports handling the piggy backed message as specified by 3GPP. ePDG does expects the separate create bearer request message post handling of create session request and response for the creation of dedicated bearer.

S2b Interface Rules

This section describes the engineering rules for the S2b interface for communications between the MAG (Mobility Access Gateway) service residing on the ePDG and the LMA (Local Mobility Anchor) service residing on the P-GW.

EGTP Service Rules

The following engineering rules apply to the S2b interface from the EGTP service residing on the ePDG:

- First GTPU service is defined and then eGTP service is defined with association of previously defined GTPU service and later on the eGTP service is associated with the ePDG service residing in same or different contex.
- An S2b interface is created once the IP address of a logical interface is bound to a eGTP and GTPU service.
- The eGTP and GTPU services must be configured within same egress context.
- The eGTP service must be associated with an ePDG service.
- **no gtpc path-failure detection-policy** CLI must be configured under eGTP service to avoid path failure detection action. When this configuration is used the ePDG does not cleans up session if the retransmission timeout has happened for the echo request sent by ePDG.

ePDG Service Rules

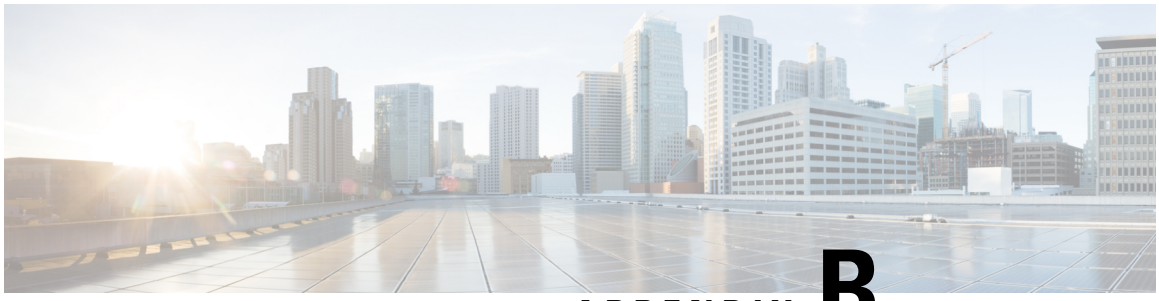
The following engineering rule applies to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.

ePDG Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

- Default subscriber templates must be configured per ePDG service.



APPENDIX B

IKEv2 Error Codes and Notifications

This appendix lists the IKEv2 error codes and notifications supported by the ePDG (evolved Packet Data Gateway).

IKEv2 Error Codes

The following table lists the IKEv2 error codes generated by the ePDG.

Table 43: IKEv2 Error Codes Generated by the ePDG

Value	Error Code	ePDG Support
1	UNSUPPORTED_CRITICAL_PAYLOAD	The ePDG sends this code if the Critical Bit exists in the received message and the Payload Type is unrecognized.
4	INVALID_IKE_SPI	The ePDG does not send this code. The ePDG ignores messages with an unrecognized SPI in order to minimize the impact of DoS attacks.
5	INVALID_MAJOR_VERSION	The ePDG sends this code in response to messages with an invalid Major Version. The ePDG supports a CLI command to suppress sending this error notification in response to IKE_SA_INIT Request messages. This is done in order to avoid DoS attacks.

Value	Error Code	ePDG Support
7	INVALID_SYNTAX	The ePDG sends this code upon receiving messages with an inappropriate format, or when necessary payloads are missing. The ePDG does not send this code during IKE_SA_INIT exchanges for an unknown IKE SA. The ePDG sends this code for non-IKEv2 INIT exchanges only (such as IKE_AUTH, CREATE_CHILD_SA, or INFORMATIONAL exchanges). The ePDG also supports a CLI command to suppress sending this error notification. This is done in order to avoid DoS attacks.
9	INVALID_MESSAGE_ID	The ePDG sends this code in INFORMATIONAL Request messages only. The ePDG also supports a CLI command to suppress sending this error notification in response to IKE_SA_INIT Request messages. This is done in order to avoid DoS attacks.
11	INVALID_SPI	The ePDG does not send this code. The ePDG ignores ESP packets with an unrecognized SPI in order to minimize the impact by DoS attacks.
14	NO_PROPOSAL_CHOSEN	The ePDG sends this code when it cannot not choose a proposal from the UE. The ePDG supports a CLI command to suppress sending this code.
17	INVALID_KE_PAYLOAD	The ePDG sends this code when the IKE payload from the UE is invalid.
24	AUTHENTICATION_FAILED	The ePDG sends this code during the EAP authentication when EAP authentication fails.
35	NO_ADDITIONAL_SAS	The ePDG sends this code when a CREATE_CHILD_SA Request message is unacceptable because the ePDG is unwilling to accept any more CHILD SAs on the IKE_SA.
36	INTERNAL_ADDRESS_FAILURE	The ePDG sends this code when the ePDG experiences a failure in address assignment.
37	FAILED_CP_REQUIRED	The ePDG sends this code when the CP payload (CFG_REQUEST) was expected but not received.
38	TS_UNACCEPTABLE	The ePDG sends this code when the TSi and/or TSr parameters contain IP protocol values other than 0.

Value	Error Code	ePDG Support
39	INVALID_SELECTORS	The ePDG does not send this code because the selector range is not checked and ingress filtering is applied instead.
40	TEMPORARY_FAILURE	when it is under collision scenarios as specified in RFC 5996.
41	CHILD_SA_NOT_FOUND	when it is under collision scenarios as specified in RFC 5996.

The following tale lists the IKEv2 error codes expected by the ePDG from the WLAN UEs.

Table 44: IKEv2 Error Codes Expected by the ePDG

Value	Error Code	ePDG Behavior Upon Receipt
1	UNSUPPORTED_CRITICAL_PAYLOAD	The ePDG sends an INFORMATIONAL (Delete) message and deletes the session information.
4	INVALID_IKE_SPI	The ePDG ignores the error message and maintain the state of existing SAs.
7	INVALID_SYNTAX	The ePDG sends an INFORMATIONAL (Delete) message and deletes the session information.
9	INVALID_MESSAGE_ID	The ePDG deletes the session information without sending an INFORMATIONAL (Delete) message.
11	INVALID_SPI	When notified in an IKE_SA message, the ePDG sends an INFORMATIONAL (Delete) message and deletes the session information. When notified outside an IKE_SA message, the ePDG ignores the error message and maintain the state for any existing SAs.
39	INVALID_SELECTORS	The ePDG sends an INFORMATIONAL (Delete) message for the IKE SA and deletes the session information.
40	TEMPORARY_FAILURE	On receipt of temporary_failure - If ePDG receives this for a rekey initiated by ePDG, ePDG shall retry rekey after some time.
41	CHILD_SA_NOT_FOUND	On receipt of CHILD_SA_NOT_FOUND - Epdg deletes the CHILDSA existing in ePDG, based on SPI.

The following table lists the notify status types defined in RFCs 4306 and 4739 that are supported by the ePDG.

Table 45: Notify Status Types Supported by the ePDG

Value	Notify Status Type
16388	NAT_DETECTION_SOURCE_IP
16389	NAT_DETECTION_DESTINATION_IP
16390	COOKIE
16393	REKEY_SA