

ePDG Interworking with SMF+P-GW-IWK Support

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- License Requirements, on page 3
- Standards Compliance, on page 3
- How it Works, on page 3
- Configuring ePDG to Enable 5G Interworking, on page 16
- Configuring ePDG for SMF+PGW-IWK or P-GW, on page 16
- Configuring ePDG to Select P-GW based on the UE-Usage-Type, on page 18
- Configuring Local P-GW with a Specific UE-Usage-Type, on page 19
- SNMP Traps for 5G and Total ePDG License, on page 19
- Monitoring and Troubleshooting, on page 21

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* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
ePDG determines the gateway type (P-GW or SMF+PGW-C) based on UE-Usage-Type.	21.28
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) and **UE-Usage-Type** 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 call flow is followed only when 5G Interworking feature is enabled.

Call Flow

Figure 1: ePDG Setup Procedure Call Flow

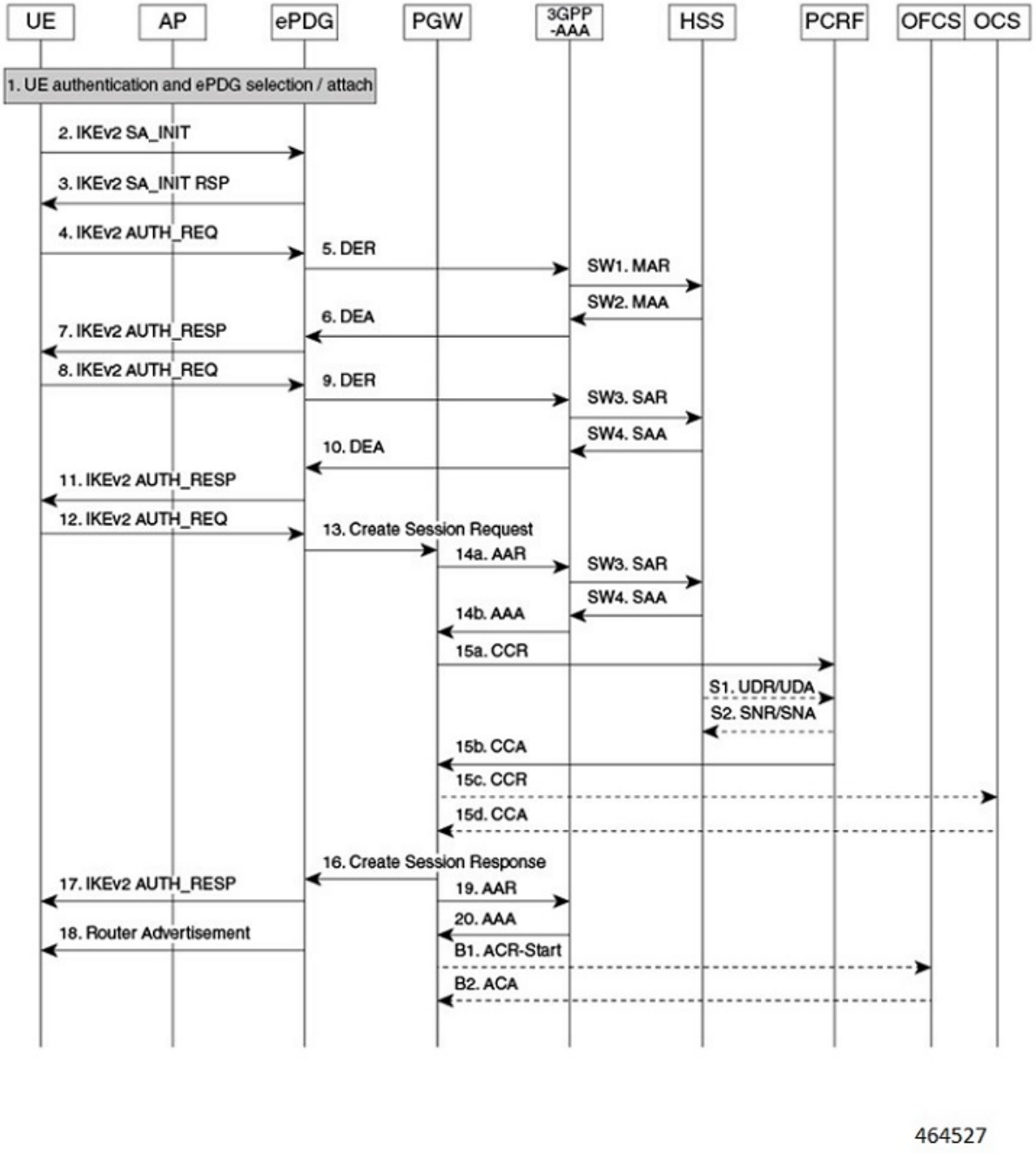


Table 1: ePDG Setup Procedure Call Flow Description

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 the 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 2: 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 a 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** are 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 2: P-GW or SMF+PGW-IWK Decision Matrix Table

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

464608

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

NOTE 1:

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

NOTE 2:

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

NOTE 3:

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

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

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

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 3: 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+PGW-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.

Note There is no new CLI introduced to enable UE-Usage-Type interworking with 5G. The CLIs introduced for “interworking-5g” and “PGW selection based on UUT” would be used for enabling UUT interworking with 5G. The CLI behavior remains same as per the existing implementation.

Configuring ePDG to Select P-GW based on the UE-Usage-Type

Use the following configuration commands to enable or disable the UE-Usage-Type.

```
configure
```

```
context context_name
  epdg-service service_name
     [ no ] pgw-selection ue-usage-type
     end
```

NOTES:

- **pgw-selection ue-usage-type** : Enables P-GW selection based on the UE-Usage-Type.
- **no pgw-selection ue-usage-type** : Disables P-GW selection based on the UE-Usage-Type.

  By default, the P-GW selection based on the **UE-Usage-Type** feature is disabled. If **UE-Usage-Type** is not enabled or not associated with the subscriber, then the Gateway selection is performed as per the existing implementation.

Configuring Local P-GW with a Specific UE-Usage-Type

Use the following configuration command to configure the P-GW with a specific UE-Usage-Type (UUT).

Note A single P-GW can serve multiple UE-Usage-Type and single UE-Usage-Type can be served by multiple P-GW.

```
configure
    apn-profile apn_name
      pgw-address ip_address ue-usage-type value
      end
```

NOTES:

- **pgw-address** *ip_address* **ue-usage-type** *value*: Configures the UE-Usage-Type for the gateway service.

  The UE-Usage-Type integer value must be 1–255. If the P-GW is configured in either primary or secondary mode, then you cannot configure more than two IPs for the P-GW regardless of the **UE-Usage-Type**.

SNMP Traps for 5G and Total ePDG License

SNMP Traps for License Limit

The SNMP traps are enhanced to indicate the comparison of the active session count with the total number of 5G licence and total ePDG license:

SNMP Trap	5G License	Total ePDG License
LicenseExceeded	Triggered when the active 5GIWK session count reaches the maximum 5G license limit with service type as ePDG 5G.	Triggered when the total active session (4G + 5G) count reaches the total ePDG service maximum license (4G License + 5G License) limit with service type as ePDG 5G.
LicenseUnderLimit	Triggered when the active 5GIWK session count is below the maximum 5G license limit with service type as ePDG 5G.	Triggered when the total active session (4G + 5G) count is below the maximum (4G License + 5G License) license limit with service type as ePDG 5G.

SNMP Trap for Configured Congestion Limit

The SNMP traps are enhanced to indicate the comparison of the active session count to the configured congestion limit in the 5G licence and total ePDG license:

SNMP Trap	5G License	Total ePDG License
Congestion	Triggered when the 5G active session count exceed the configured congestion limit of 5G license with service type as ePDG 5G.	Triggered when the total ePDG active session count (4G+5G) exceed the configured congestion limit of total ePDG license with service type as ePDG 5G.
CongestionClear	Triggered when the 5G active session count is less than the configured congestion limit of 5G license with service type as ePDG 5G.	Triggered when the total ePDG active session (4G+5G) is less than the configured congestion limit of total ePDG license with service type as ePDG 5G.

Important Refer Threshold Configuration Guide for configuring license threshold limit, tolerance level and verifying generated traps.

Note OverloadSystem SNMP trap is not generated for 5G license Overload, when the given overload-disconnect is configured:

```
config
congestion-control overload-disconnect
end
```

Congestion Policy for 5GIWK Sessions

Congestion policy is not applied for 5G sessions when the congestion threshold is hit against the 5G license. Only the congestion Traps for 5GIWK shall be generated.

Congestion policy is applied for ePDG calls, only when the congestion threshold is hit against total ePDG (4G+5G) license limit.

Verify SNMP Trap Generated for Session Count and Congestion

Use the **show snmp trap history** command to verify the SNMP trap generated for congestion:

```
[pdif]ePDG# show snmp trap history
Tue Aug 13 14:12:46 2024 Internal trap notification 65 (LicenseExceeded) license exceeded
for EPDG 5G service; current sessions 15 exceeds license 10
Tue Aug 13 14:12:46 2024 Internal trap notification 81 (Congestion) service type epdg-5g
congestion policy none, resource type license
Tue Aug 13 14:15:56 2024 Internal trap notification 94 (LicenseUnderLimit) system under
license limit for EPDG 5G service; current sessions 9 license 10
Tue Aug 13 14:17:36 2024 Internal trap notification 82 (CongestionClear) service type epdg-5g
```

Verify SNMP Trap Statistics for Congestion

Use the **show snmp trap statistics** command to verify the SNMP trap statistics generated for congestion:

```
Trap Name                           #Gen #Disc  Disable Last Generated
----------------------------------- ----- -----  ------- --------------------
Congestion                             2     0       0  2024:08:12:14:36:19
CongestionClear                        2     0       0  2024:08:12:14:37:09
LicenseExceeded                        3     0       0  2024:08:26:21:14:05
LicenseUnderLimit                      3     0       0  2024:08:26:21:15:15
```

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 4: 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.

Field	Description
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.
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.

Field	Description
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.
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.

Field	Description
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.
5G Sessions – Counter for sessions with access to 5G core not restricted and exceptions as specified in the Limitation section	
Acive	The total number of 5G Active sessions.
PDN-Type IPv4	The total number of 5G Active sessions of PDN type IPv4.
PDN-Type IPv6	The total number of 5G Active sessions of PDN type IPv6.
PDN-Type IPv4 v6	The total number of 5G Active sessions of PDN type Dual.

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.
iwk5g-pdn-active	The total number 5G Active sessions.
iwk5g-pdn-ipv4-active	The total number of 5G active sessions of PDN type IPv4.
iwk5g-pdn-ipv6-active	The total number of 5G active sessions of PDN type IPv6.
iwk5g-pdn-ipv4v6-active	The total number of 5G Active sessions of PDN type Dual.
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.
iwk5g-concurrent-idle-sess	The number of 5G sessions that remain idle longer than the CLI-configured timeout.
uut-iwk5g-smf-preferred	Total number of SMF preferred based on the ue-usage-type during 5G ePDG sessions for the case where 5GSIWK flag is not set.
uut-iwk5g-smf-preferred-dns	Total number of DNS provided SMF selected based on the ue-usage-type during 5G ePDG sessions.
uut-iwk5g-smf-preferred-local	Total number of locally configured SMF selected based on the ue-usage-type during 5G ePDG sessions.
uut-iwk5g-smf-preferred-aaa	Total number of AAA provided SMF selected during 5G ePDG sessions.

uut-iwk5g-smf-only	Total number of SMF selected based on the ue-usage-type during 5G ePDG sessions for the case where 5GSIWK flag is set and PDUSessionID gets forwarded to SMF.
uut-iwk5g-smf-only-dns	Total number of DNS provided SMF selected based on the ue-usage-type during 5G ePDG sessions.
uut-iwk5g-smf-only-local	Total number of locally configured SMF selected based on the ue-usage-type duringS 5G ePDG sessions.
uut-iwk5g-smf-only-aaa	Total number of AAA provided SMF selected for 5G ePDG sessions.
uut-iwk5g-pgw-only	Total number of P-GW selected based on the ue-usage-type during 5G ePDG sessions.
uut-iwk5g-pgw-only-dns	Total number of DNS provided P-GW selected based on the ue-usage-type during 5G ePDG sessions.
uut-iwk5g-pgw-only-local	Total number of locally configured P-GW selected based on the ue-usage-type during 5G ePDG sessions
uut-iwk5g-pgw-only-aaa	Total number of AAA provided P-GW selected during 5G ePDG sessions.
PGW/SMF not available reasons - Provide counters on how many times ue-usage-type based PGW/SMF selection is failed due to no matching ue-usage-type with locally configured PGW/SMF.	
uut-iwk5g-no-local-pgw	Total number of gateway selection failure due to no matching ue-usage-type with locally configured P-GW during 5G ePDG sessions.
uut-iwk5g-no-local-smf	Total number of gateway selection failure due to no matching ue-usage-type with locally configured SMF during 5G ePDG sessions.
Total Number of SMF Fallback: Fallback related counters (Attempted/Success/Failure) for total number of SMF provided by AAA, DNS, and local configuration for the associated ue-usage-type. In general, an attempt for next SMF, if the previously selected SMF for the associated ue-usage-type is failed, then it will be considered as fallback. That is, when a create session request sent for the selected SMF is failed due to some reason, ePDG attempts a fallback and sends create session request to the next available SMF for the associated ue-usage-type.	
uut-iwk5g-smf-fallback-attempted	Total number of ue-usage-type based SMF fallback attempted during 5G ePDG sessions.
uut-iwk5g-smf-fallback-success	Total number of ue-usage-type based SMF fallback succeeded during 5G ePDG sessions.
uut-iwk5g-smf-fallback-failed	Total number of ue-usage-type based SMF fallback failed during ePDG 5G sessions.

uut-iwk5g-smf-fallback-noalt-smf	Total number of alternate ue-usage-type based SMF not available in either AAA or DNS, when the call is dropped for a 5G ePDG session.
SMF Fallback Support Statistics 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: Fallback related counters for the total number of SMF based on ue-usage-type provided by local configuration. These counters gets incremented when the previous attempt of SMF is failed and the next fallback attempt of SMF for the associated ue-usage-type is based on the local configuration.	
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.
uut-iwk5g-local-smf-fallback-attempted	Total number of local ue-usage-type based SMF fallback attempted during 5G ePDG sessions
uut-iwk5g-local-smf-fallback-success	Total number of local ue-usage-type based SMF fallback succeeded during 5G ePDG sessions.
uut-iwk5g-local-smf-fallback-failed	Total number of local ue-usage-type based SMF fallback failed during 5G ePDG sessions.

uut-iwk5g-local-smf-fallback-noalt-smf	Total number of alternate local ue-usage-type based SMF not available to further fallback for a 5G session to get connected.
P-GW Fallback Support Statistics 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.
Total Number of P-GW Fallback: Fallback related counters (Attempted/Success/Failure) for total number of P-GW provided by AAA, DNS, and local configuration for the associated ue-usage-type. An attempt for next P-GW since the previously selected P-GW for the associated ue-usage-type is failed, will be considered as fallback.	
uut-iwk5g-pgw-fallback-attempted	Total number of ue-usage-type based P-GW fallback attempted during 5G ePDG sessions.
uut-iwk5g-pgw-fallback-success	Total number of ue-usage-type based P-GW fallback succeeded during 5G ePDG sessions.
uut-iwk5g-pgw-fallback-failed	Total number of ue-usage-type based P-GW fallback failed during ePDG 5G sessions.
uut-iwk5g-pgw-fallback-noalt-pgw	Total number of alternate ue-usage-type based P-GW not available in either AAA or DNS, when the call is dropped for a 5G ePDG session.
Local P-GW Resolution: Fallback related counters for the total number of P-GW based on ue-usage-type provided by the local configuration. These counters gets incremented when the previous attempt of P-GW is failed and the next fallback attempt to local PGW for the associated ue-usage-type.	
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.
uut-iwk5g-local-pgw-fallback-attempted	Total number of local ue-usage-type based P-GW fallback attempted during 5G ePDG sessions.
uut-iwk5g-local-pgw-fallback-success	Total number of local ue-usage-type based P-GW fallback succeeded during 5G ePDG sessions.
uut-iwk5g-local-pgw-fallback-failed	Total number of local ue-usage-type based P-GW fallback failed during 5G ePDG sessions.
uut-iwk5g-local-pgw-fallback-noalt-pgw	Total number of alternate local ue-usage-type based PGW not available to further fallback for a 5G session to get connected.
DNS-related Failures:	
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.
uut-iwk5g-dns-server-notreachable	Total number of failures due to DNS server not reachable during 5G ePDG sessions for the associated ue-usage-type.
uut-iwk5g-dns-no-resourcerecords	Total number of failures due to no DNS resource records during 5G ePDG sessions for the associated ue-usage-type.
uut-iwk5g-dns-no-matching-pgw-service	Total number of P-GW received without matching the ue-usage-type during 5G ePDG sessions.

uut-iwk5g-dns-no-matching-smf-service	Total number of SMF received without matching the ue-usage-type during 5G ePDG sessions.
uut-iwk5g-dns-pgw-list-exhausted	Total number of ue-usage-type based P-GW list provided in DNS response, has failed to connect and exhausted during 5G ePDG sessions.
uut-iwk5g-dns-smf-list-exhausted	Total number of ue-usage-type based SMF list provided in DNS response, has failed to connect and exhausted during 5G ePDG sessions.