VoNR Support

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Multiple PDU Sessions for VoNR: Enabled – Always-on Emergency Services: Enabled – Always-on PDN Creation, Modification, and Release: Enabled – Configuration required to disable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Introduced the emergency services.	2022.01.0
First introduced.	2021.04.0

Feature Description

The Voice over New Radio (VoNR) feature supports the following functionalities:

- Creating multiple Protocol Data Unit (PDU) sessions
- Emergency services
- Creation, modification, and release of the Packet Data Network

Voice over New Radio (VoNR) Support

Feature Description

The AMF provides the IP Multimedia Subsystem (IMS) voice services over the Packet Switched (PS) or VoNR to the subscribers who are connected over the 3GPP Radio Access Network (RAN).

AMF receives the local configuration and capability parameters from UE or gNB. Based on this information, the AMF determines if the UE can support the IMS voice over PS sessions in the specified area. The AMF communicates the IMS support to the UE during the UE registration process.

With this feature, the AMF extends support for the following:

- PDU support for same or different SMF instances
- Discovery of the SMF instances using Tracking Area Identity (TAI as the query parameter
- Reuse of the discovered SMF instances within the cache expiry timeout period
- If used within the cache expiry time out period, the PDU release and update procedure can utilize the SMF instance discovered for the PDU creation procedure.

Note The NO_SUITABLE_CELLS_IN_TRACKING_AREA is used for rejecting the voice-centric cause.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Initial or Mobility Registration—IMS VoNR Support Procedure Call Flow

This section describes the Initial or Mobility Registration—IMS VoNR Support Procedure call flow.

Figure 1: Initial or Mobility Registration—IMS VoNR Support Procedure Call Flow

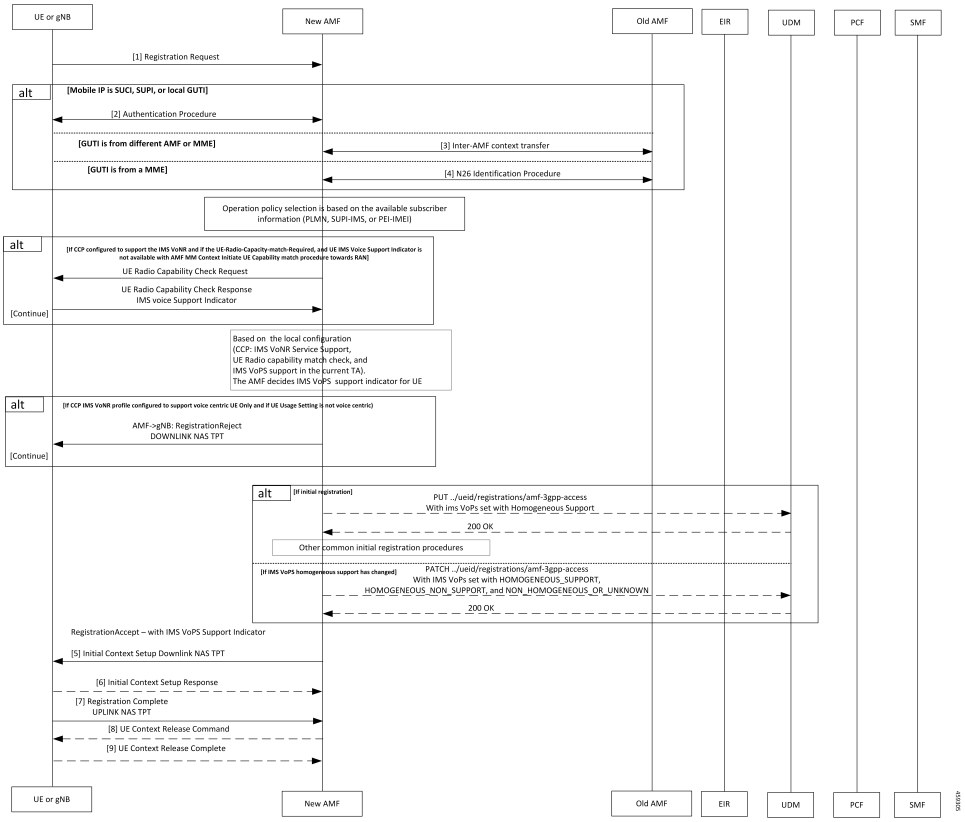

Table 3: Initial or Mobility Registration—IMS VoNR Support Procedure Call Flow Description

Step	Description
1	The UE or gNB sends a Registration Request message to the new AMF instance. During the UE registration (initial, mobility update, and AMF change or EPC to 5GC handover) procedure, after the operator policy and Call Control Profiles are associated with the subscriber context, the AMF checks the following: • The IMS VoPS service for 3GPP access is supported under CCP. • The UE Radio capability match is required or not.
2	The UE or the gNB and the AMF completes the authentication procedure.
3	The new AMF and the old AMF process the inter-AMF Context Transfer procedure.

Step	Description
4	The new AMF and the old AMF complete the N26 identification procedure. If the UE Radio Capability matching is required and the AMF has not received or discovered it yet, the AMF starts the UE Radio Capability check procedure towards gNB. The gNB provides the IMS VoPS capability information to AMF and confirms if it is supported or matching. The AMF considers the UE to provide the IMS VoPS services indicator as supported. AMF checks if the IMS VoPS service is configured to be supported or enabled under the current TA of the subscriber and its support in TAI's list object under TAI DB. If the criteria is matched, AMF considers the IMS VoPS support for the subscriber to be supported for current TA. The AMF informs UDM about the IMS VoPS support for the subscriber in all the TAs that AMF serves or in the 3GPP Access Registration procedure to UDM. Based on CCP configuration, if the subscriber is eligible or capable of the IMS VoPS support, AMF provides the imsVoPS parameter to UDM in 3GPP Access Registration message as HOMOGENEOUS_SUPPORT. This parameter indicates the subscriber about the AMF level support of IMS VoPS service and the TA level support. After UDM receives this information, if the IMS service sent to the subscriber (For example, local configuration change) is modified, the AMF updates UDM using the 3GPP Access Registration Modification procedure.
5	The AMF indicates IMS VoPS service support for the subscriber for current registration area (TA) in Registration Accept message in IMSVoPS-3GPP indicator under 5GS network feature support information element. The UE or the gNB and new AMF processes the Initial Context Setup Downlink NAS TPT.
6	The gNB sends the Initial Context Setup Response to the new AMF.
7	The UE or gNB sends the Registration Complete Uplink NAS TPT to the new AMF.
8	The new AMF sends the UE Context Release Command to the gNB.
9	The gNB sends the UE Context Release Complete to the new AMF.

Provide UE Information for Terminating Domain Selection Call Flow

This section describes the Provide UE Information for Terminating Domain Selection call flow.

Figure 2: Provide UE Information for Terminating Domain Selection Call Flow

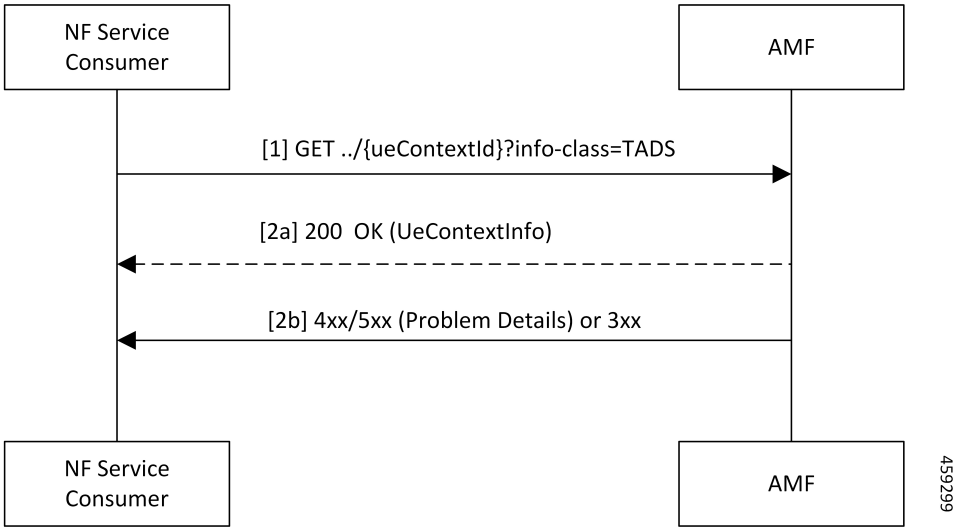

Table 4: Provide UE Information for Terminating Domain Selection Call Flow Description

Step	Description
1	The NF Service Consumer sends a GET request to the URI of the UeContext resource on the AMF with the info-class query parameter set to value to TADS.
2a	On success, the AMF returns the 200 OK status code with the payload containing the UeContextInfo data structure that includes the UE information for terminating the domain selection for IMS voice.
2b	On failure, the AMF returns one of the HTTP status codes listed in *3GPP TS 29.518 Table 6.3.3.3.3.1-3*. The message body contains a ProblemDetails object with the detail set to application errors in *TS 29.518* and *Table 6.3.3.3.3.1-3*.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.501, "System architecture for the 5G System (5GS)"*
- *3GPP TS 23.502, "Procedures for the 5G System (5GS)"*
- *3GPP TS 29.518, "5G System; Access and Mobility Management Services; Stage 3"*
- *3GPP TS 38.143, "5G; NG-RAN;NG Application Protocol (NGAP)"*

Limitations

This feature has the following limitations in this release:

- The AMF doesn’t support IMS services over non-3GPP access.
- The IMS VoPS support indication is applicable only for the voice-centric UE usage setting type.

Feature Configuration

Configuring this feature involves the following steps:

1. Enable AMF to indicate if the UE is capable to handle IMS Voice over Packet-Switched (VoPS) sessions. For more information, refer to Configuring Support to Indicate IMS VoPS Support, on page 6.
2. Configure IMS VoPS service for the configured TALs. For more information, refer to Configuring the TAL-level IMS VoPS, on page 6.

Configuring Support to Indicate IMS VoPS Support

To configure the support that allows AMF to flag if UE supports the IMS VoPS, use the following configuration:

```
config
   amf-global
     call-control-policy policy_name
       feature-support-ie
         ims-vops-service-3gpp
            supported { false | true }
               ue-capability-match-required { false | true }
               reject-voice-centric-ue  { false | true }
               end
```

NOTES:

- **feature-support-ie**—Configure the AMF or 5GC features that are supported or unsupported.
- **ims-vops-service-3gpp**—Configure the UE support for the IMS VoPS service over 3GPP access.
- **supported { false | true }**—Enable the 5G VoPS 3GPP. If the UE capability is supported, the UE is configured with the UE Radio capability.
- **ue-capability-match-required { false | true }**—Configure the UE Radio capability based on the requirement match criteria.
- **reject-voice-centric-ue { false | true }**—Configure the UE capability to reject the “voice centric” UEs when the IMS VoPS service is not supported.

  Any change to the **reject-voice-centric-ue** CLI takes an effect only on the new subscriber (new Registration Requests) or when ueUssageSetting is changed from Data Centric to Voice Centric or conversely. Modifications to **reject-voice-centric-ue** do not have an impact on the ongoing calls.

Configuring the TAL-level IMS VoPS

A TAI group consists of multiple Tracking Area Lists (TALs). Each TAL can contain one or more TAIs.

To configure TAL-level IMS VoPS, use the following configuration:

```
config
   amf-global
     call-control-policy policy_name
        tai-group tai_group_name
          tais tai_value
            ims-voice-over-ps-supported { false | true }
            end
```

NOTES:

- **call-control-policy** *policy_name*—Configure the Call Control Policy.
- **tai-group** *tai_group_name*—Specify the TAI group name.
- **tais** *tai_value*—Specify the TAL element name.
- **ims-voice-over-ps-supported { false | true }**—Configure support for the IMS VoPS service in the configured TAI list.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Statistics

The following statistic and counter are supported for the Multiple PDU Sessions for VoNR feature.

- The ims-vops-support counter captures the reject cause counter.
- amf_ngap_message_total—Captures the total number of inbound or outbound messages sent towards AMF. This metric supports the following message types:
  - N2UeRadioCapabilityCheckRsp
  - N2UeRadioCapabilityCheckReq

Emergency Services

Feature Description

When the 5GC supports the emergency services, the UE is enabled to handle the emergency through the Registration Accept message on per-TA and per-RAT basis.

This feature allows the UE to fall back to EUTRAN connected to 5GC (4G radio, 5G core) or EUTRAN connected to EPC (4G radio, 4G core). UE switches to the EUTRAN type based on the network capabilities and if the 5G Radio is not NR capable.

How it Works

This section describes how this feature works.

In the first occurrence, the UE registers with AMF through the initial registration or the mobility update registration procedure with a new AMF instance. In response to the registration request, the AMF sends the emergency service parameters to the UE.

When the emergency profile is modified, the UE is notified through the procedures defined in UE Context Update. To communicate the emergency services configuration, the UE reregisters with the AMF. The reregistration request has the Registration Required indicator in the Update Configuration message.

During the registration procedure, the AMF searches for an emergency profile in the call control policy configured for the UE. If the AMF detects the profile, it sets the following parameters in the Registration Accept message:

- Emergency Services Support in the 5GC network feature
- Emergency Number List in the Registration Accept message
- Additional Emergency Number List in the Registration Accept message

When the UE does not have a valid subscription in a specific area, it can continue to register for the emergency services. This is driven based on the emergency services profile configuration on the AMF.

Call Flows

This section describes the key call flows for this feature.

Node-level Call Flow

This section describes the Node-level call flow.

Figure 3: Node-level Call Flow

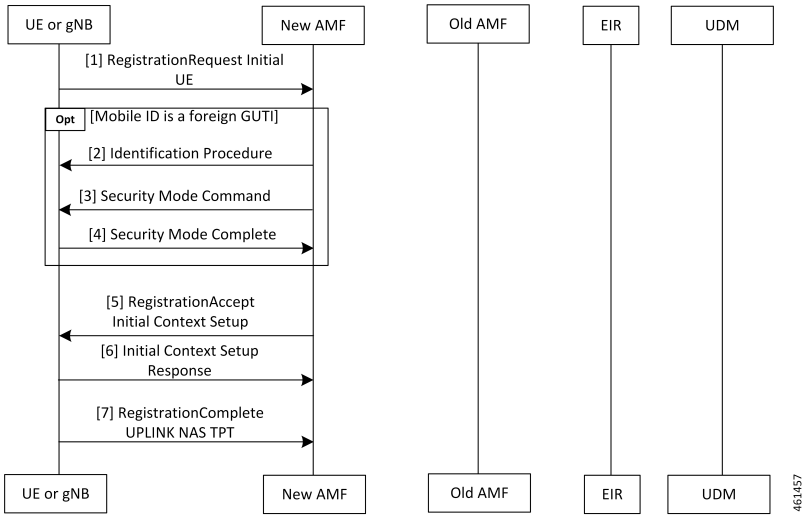

Table 5: Node-level Call Flow Description

Step	Description
1	If the UE wants to register for the emergency services, it sets the registration type to Emergency. When the UE inherits a Globally Unique Temporary ID (GUTI) from the previous 5G registration, it uses GUTI in the Registration Request.
2	If the UE provides a foreign GUTI, the AMF sends the Identity Check Procedure to retrieve the SUCI of the UE. If the AMF fails and authentication is optional, it retrieves Permanent Equipment Identifier (PEI) of the UE.
3	The AMF sends the Security Mode Command message to the UE.
4	The UE responds to the AMF with the Security Mode Complete message.

Step	Description
5	In the Initial Context Setup Request, if the Emergency Services Profile does not require authentication, the AMF signals support only EIA0 and EEA0 based on the integrity protection and encryption algorithms. This algorithm forces the gNB to process the INITIAL_CONTEXT_SETUP procedure without a specific security algorithm from the UE on the RRC interface.
6	The gNB responds with INITIAL_CONTEXT_SETUP response to the AMF.
7	The UE responds with the Registration Complete message to the gNB.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.501 "System Architecture for the 5G System—Emergency Services"*
- *3GPP TS 24.501 "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3—Registration procedure for initial registration"*
- *3GPP TS 23.502 "Procedures for the 5G System (5GS)—Registration procedures"*
- *3GPP TS 33.501 "Security architecture and procedures for 5G System—Security aspects of IMS emergency session handling"*

Limitations

This feature has the following limitations in this release:

- The AMF does not support the N26-based IDLE mode handover procedure, and the N14-based UE Context Transfer scenarios with the emergency PDU and Emergency Registered Subscriber requests.
- For the N26-based handover, AMF supports only the IMSI-based emergency registered handover procedures. However, the AMF does not support IMEI-based handover as the MME requires both IMSI and IMEI information.
- The AMF does not support the emergency services in the following scenarios:
  - E-call interactions
  - Emergency service fallback
  - Congestion interactions
  - Identification, authentication, EIR and UDM interaction
  - Configuration change in emergency profile communication to UE
  - Security procedure failure scenario for normal registration
  - Support for EPS type of service request is not available

Feature Configuration

Configuring this feature involves the following steps:

- Configure the emergency services to enable the UE to handle the emergency requests through the Registration Accept message on per-TA and per-RAT basis. For more information, refer to Associating the Emergency Profile with the AMF Services or Global Configuration, on page 11.
- Configure the emergency profile to define the emergency parameters of the NF. For more information, refer to Configuring Emergency Profile, on page 10.

Configuring Emergency Profile

To configure this feature, use the following configuration:

```
config
   profile
      emergency-profile emergency_profile_name
         dnn dnn_name
         extended-emergency-num extended_emergency_number
         local-emergency-num local_emergency_number
         slice { slice_name | sst sst | sdt  sdt }
         ue-validation-level [ auth-only | full | none | supi-only ]
         end
```

NOTES:

- **extended-emergency-num** *extended_emergency_number*—Specify the extended emergency number. Accepted value is string in the range of 1–10.
- **local-emergency-num** *local_emergency_number*—Specify the local emergency number. Accepted value is string in the range of 1–10.
- **ue-validation-level [auth-only | full | none | supi-only]**—Specify the UE validation level. This parameter provides the following options:

Note For the emergency services, only **none** and **supi-only** options are supported.

  - **auth-only**—Specify to allow only authenticated UEs. When **auth-only** is specified the subscription is bypassed.
  - **full**—Specify to allow only authenticated UEs with subscription and location validated. When **full** is specified, UEs with normal registration are allowed.
  - **none**—Specify to allow any type of UE. The UE without SUPI is attached using the IMEI or PEI. Authentication is optional.
  - **supi-only**—Specify to allow UEs with SUPI. The UE without SUPI is rejected. Authentication is optional.

Associating the Emergency Profile with the AMF Services or Global Configuration

To configure this feature, use the following configuration:

```
config
  amf-global
     operator-policy local
     ccp-name ccp_value
     emergency-profile-name profile_name
     network-element-profile-list [ amf | ausf | nssf | pcf | udm | smf
]
     nf-profile-name network_function_profile
     paging-map-name paging_map_name
     end
  amf-services amf_service_name
     emergency-profile-name em1 amf_service_name
     amf-name amf_name
     guamis [  mcc | mnc | region-id | set-id | pointer ]
     local-cause-code-map local_cause_code_type
     locality locality
     operator-policy-name policy_name
     peer-mme [ gummei [ mcc | mnc | group-id | mme-code | address ] |
tai-match [ priority | mcc | mnc | tac | address ] ]
     pgw fqdn fqdn
     relative-amf-capacity capacity
     slices { slice_name | range }
     tai-groups tai_group-name
     validate-Tais [ false | true ]
     end
```

NOTES:

- You can associate the emergency profile with the emergency services through the **amf-global** or the **amf-services** configuration.
- **network-element-profile-list [amf | ausf | nssf | pcf | udm | smf]**—Specify the selected NF's network element profile name.
- **paging-map-name** *paging_map_name*—Specify the 5G paging map name. Accepted value must be in string within the range of 1–64.
- **local-cause-code-map** *local_cause_code_type*—Specify the local cause code condition type. Accepted value is string in the range of 1–64.
- **locality** *locality*—Specify the locality for geo support.
- **pgw fqdn** *fqdn*—Specify the peer for SMF and PGW-C configurations.
- **relative-amf-capacity** *capacity*—Specify the AMF capacity within the range of 0–255. The default range is 127.

Configuration Verification

To verify the configuration:

show full-configuration profile emergency-profile [e911 | e912]

Sample Output

```
profile emergency-profile e911
  dnn starent1.com
  slice name emergency sst 2 sdt 000003
  ue-validation-level none
  local-emergency-num 100 police
  exit
amf-global
amf-name cisco-amf
dnn-policy starent.com
  network-element-profile-list smf smf1
exit
dnn-policy starent1.com
  network-element-profile-list smf smf1
exit
operator-policy local
  ccp-name local
  network-element-profile-list ausf ausf1
  network-element-profile-list smf smf1
  network-element-profile-list pcf pcf1
  network-element-profile-list udm udm1
  network-element-profile-list nssf nssf1
  emergency-profile-name e911
exit
exit
 amf-services am1
amf-name AMF
emergency-profile-name e911
exit
```

PDN Creation, Modification, and Release

Feature Description

The Packet Data Network (PDN) creation, modification, and release feature enable AMF to implement the following UDM services:

- Initiates the P-CSCF restoration procedure
- Sends a network-triggered PDU Session Update for IMS PDU sessions with the reactivation indication. Based on the indication, SMF takes the appropriate action on the PDU.

  During the UDM registration, the AMF sends the callback URL for the P-CSCF restoration and service name. The AMF handles the notification triggered for the Nudm_UECM_PCscfRestoration service operation received on the URI. This notification contains information about the restoration status as a failure or success.
- Selects a combined instance of SMF and PGW-C, if the UE sends a request to establish a PDU Session with a DNN and S-NSSAI when the following conditions are true:
  - The UE MM Core Network Capability indicates that the UE supports EPC NAS.
  - (Optional) The UE subscription symbolizes support for interworking with EPS for the specified DNN and S-NSSAI of the HPLMN.

Note If the conditions are not met, the AMF selects a standalone instance of SMF.

How it Works

This section describes how this feature works.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 29.503 "5G System; Unified Data Management Services; Stage 3"*
- *3GPP TS 29.502 "5G System; Session Management Services; Stage 3"*
- *3GPP TS 23.502 "Procedures for the 5G System (5GS)"*

Call Flows

This section describes the key call flows for this feature.

SM Context Update Call Flow

This section describes the SM Context Update call flow.

Figure 4: SM Context Update Call Flow

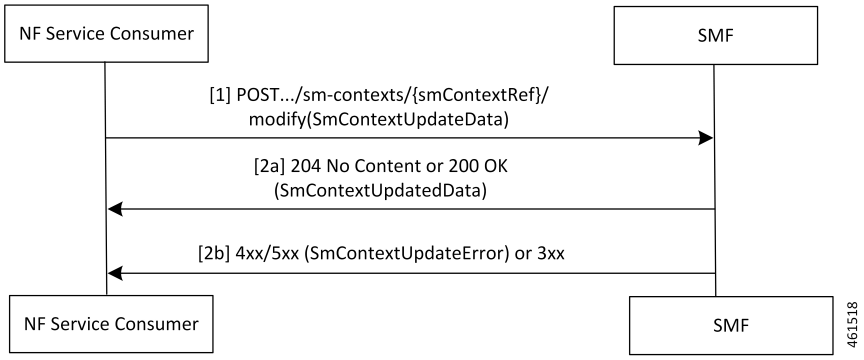

Table 6: SM Context Update Call Flow Description

Step	Description
1	The AMF service consumer performs both or one of the following: • Updates a particular SM context • Provides N1 or N2 SM information to the SMF through the HTTP POST method (modify custom operation). The POST request contains the following information: • The release IE is set to true. • The cause IE is set to REL_DUE_TO_REACTIVATION.
2a	The SMF responds with the SmContextUpdatedData data type that contains the following response codes: • 204 No Content—The SM context is successfully updated when the SMF does not return information in the response. • 200 OK—The SM context is successfully updated when the SMF returns information in the response.
2b	When the SM Context Update fails, the SMF reports an error. For a 4xx or 5xx response, the message body contains an SmContextUpdateError structure.

Feature Configuration

Configuring this feature involves the following steps:

1. Configure the UDM initiated PCSF restoration procedure at AMF. For more information, refer to Configuring the PCSF Restoration Feature, on page 14.
2. Configure the IMS for identifying the PDU session with DNN name. For more information, refer to Configuring the IMS for DNN, on page 15.
3. Configure the query selection parameter to select the SMF instance that supports SMF and PGW-C. For more information, refer to Configuring the Query Selection Parameter, on page 15.

Configuring the PCSF Restoration Feature

To configure the PCSF restoration feature, use the following configuration:

```
config
   amf-global
      call-control-policy call_control_policy_name
         feature-support-ie
            pcsf-restoration-supported { true | false }
            end
```

NOTES:

- **call-control-policy** *call_control_policy_name*—Specify the Call Control Policy name.
- **feature-support-ie**—Configure AMF or 5GC features that are supported.
- **pcsf-restoration-supported { true | false }**—Configure the PCSF restoration capability. After enabling this feature, the capability supports only the new calls that are established.

Configuring the IMS for DNN

To configure the IMS for the DNN, use the following configuration:

```
config
   amf-global
      amf-name amf_name
         dnn-policy policy_name
            network-element-profile-list smf
               ims-enabled { true | false }
               end
```

NOTES:

- **amf-name** *amf_name*—Specify AMF name.
- **dnn-policy** *policy_name*—Specify the DNN policy name.
- **ims-enabled { true | false }**—Enable or disable IMS for the configured DNN.

Configuring the Query Selection Parameter

To configure the query parameter, use the following configuration:

```
config
   profile
      network-element smf smf_instance
         query-params [ pgwind ]
         end
```

NOTES:

- **network-element smf** *smf_instance*—Specify the NF instance name to establish the peer configuration.
- **query-params [pgwind]**—Configure the query parameter that selects the specified SMF instance for SMF and PGW-C support.