Ultra Cloud Core 5G Session Management Function, Release 2020.02 - Configuration and Administration Guide

First Published: 2020-04-30

Last Modified: 2020-07-10

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

CONTENTS

About this Guide

This preface describes the *5G Session Management Function Guide*, how it is organized and its document conventions.

This guide describes the Cisco Session Management Function (SMF) and includes infrastructure and interfaces, feature descriptions, specification compliance, session flows, configuration instructions, and CLI commands for monitoring and troubleshooting the system.

• Conventions Used, on page xxxvii

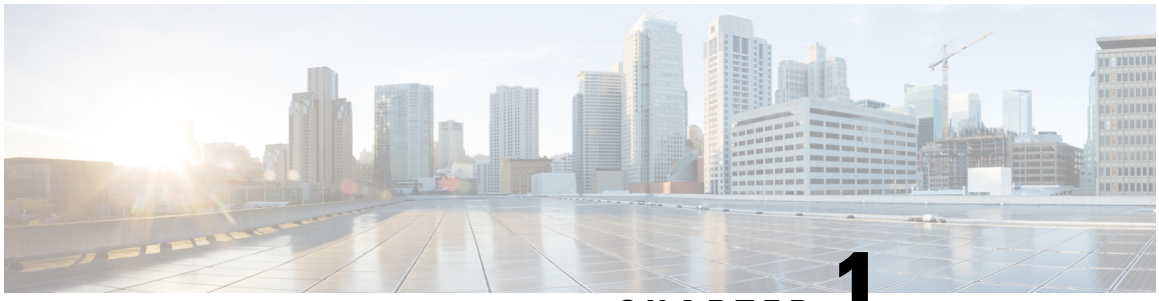
Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.

Typeface Conventions	Description
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**



CHAPTER 1

5G Architecture

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Overview

The Ultra Cloud Core is Cisco's solution supporting 3GPP's standards for 5G new radio (NR) standalone (SA) mode. These standards define various network functions (NFs) based on the separation of control plane (CP) and user plane (UP) (e.g. CUPS) functionality for increased network performance and capabilities.

Control Plane NFs

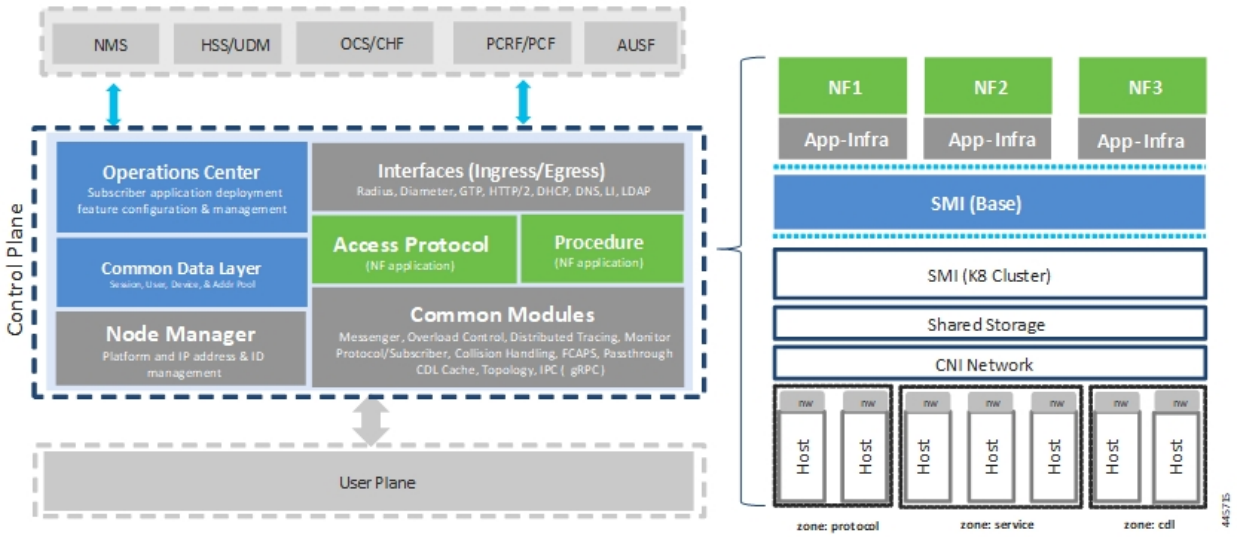
The CP-related NFs that comprise the Ultra Cloud Core are based on a common architecture designed around the following tenants:

- Cloud-scale — Fully virtualized for simplicity, speed, and flexibility
- Automation and orchestration — Optimized operations, service creation, and infrastructure
- Security — Multiple layers of security across the deployment stack from the infrastructure through the NF applications
- API exposure — Open and extensive for greater visibility, control, and service enablement
- Access agnostic — Support for heterogeneous network types (e.g. 5G, 4G, 3G, Wi-Fi, etc.)

These CP NFs are each designed as containerized applications (e.g. microservices) for deployment via the Subscriber Microservices Infrastructure (SMI).

The SMI defines the common application layers for functional aspects of the NF such as life cycle management (LCM), operations and management (OAM), and packaging.

Figure 1: Ultra Cloud Core CP Architectural Components



User Plane NF

The 5G UP NF within the Ultra Cloud Core is the User Plane Function. Unlike the CP-related NFs, the 5G UPF is leverages the same Vector Packet Processing (VPP) technology currently in use by the user plane component within Cisco's 4G CUPS architecture. This commonality ensures the delivery of a consistent set of capabilities between 4G and 5G such as:

- Ultra-fast packet forwarding
- Extensive integrated IP services such as Subscriber Firewall, Tethering, Deep-Packet Inspection (DPI), Internet Content Adaption Protocol (ICAP), Application Detection and Control (ADC), and header enrichment (HE)
- Integrated third-party applications for traffic and TCP optimization

Refer to the Ultra Cloud Core 5G UPF Configuration and Administration Guide for more information.

Subscriber Microservices Infrastructure Architecture

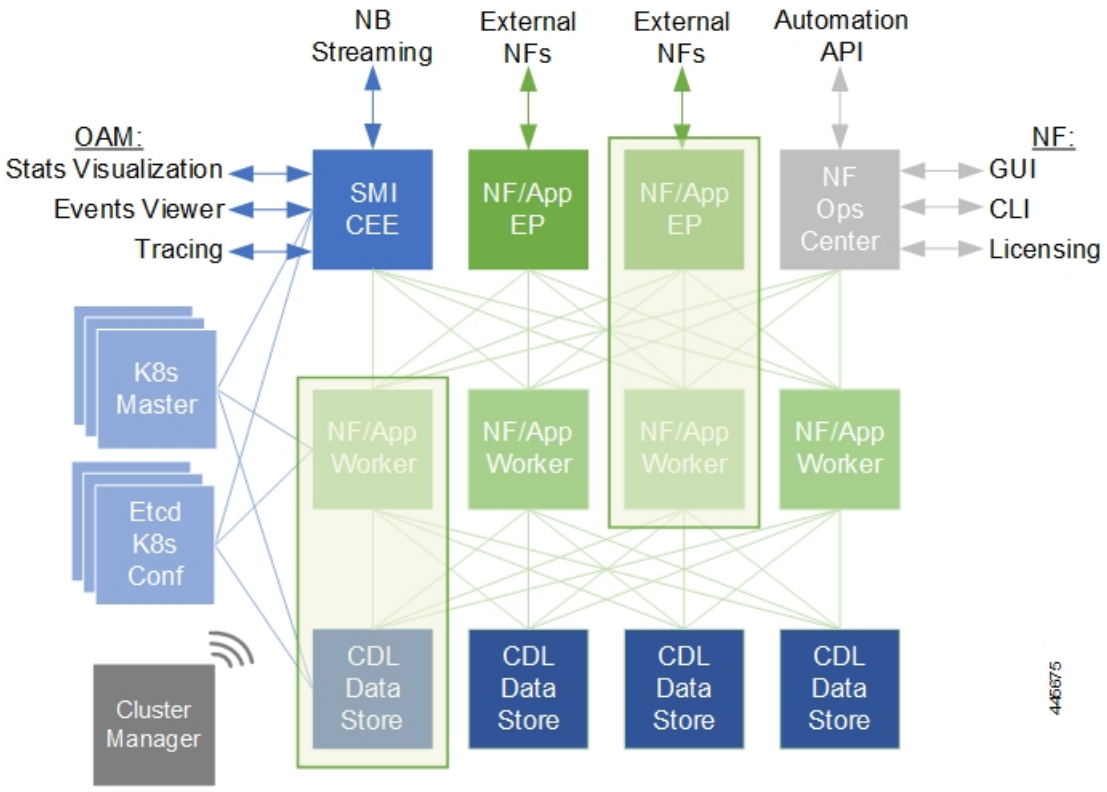
The Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) is a layered stack of cloud technologies that enable the rapid deployment of, and seamless life cycle operations for microservices-based applications.

The SMI stack consists of the following:

- SMI Cluster Manager — Creates the Kubernetes (K8s) cluster, creates the software repository, and provides ongoing LCM for the cluster including deployment, upgrades, and expansion.
- Kubernetes Management — Includes the K8s master and etcd functions, which provide LCM for the NF applications deployed in the cluster. This component also provides cluster health monitoring and resources scheduling.
- Common Execution Environment (CEE) — Provides common utilities and OAM functionalities for Cisco cloud native NFs and applications, including licensing and entitlement functions, configuration management, telemetry and alarm visualization, logging management, and troubleshooting utilities. Additionally, it provides consistent interaction and experience for all customer touch points and integration points in relation to these tools and deployed applications.
- Common Data Layer (CDL) — Provides a high performance, low latency, stateful data store, designed specifically for 5G and subscriber applications. This next generation data store offers HA in local or geo-redundant deployments.
- Service Mesh — Provides sophisticated message routing between application containers, enabling managed interconnectivity, additional security, and the ability to deploy new code and new configurations in low risk manner.
- NF/Application Worker nodes — The containers that comprise an NF application pod.
- NF/Application Endpoints (EPs) – The NF's/application's interfaces to other entities on the network.
- Application Programming Interfaces (APIs) — SMI provides various APIs for deployment, configuration, and management automation.

The following figure depicts how these components interconnect to comprise a microservice-based NF/application.

Figure 2: SMI Components



See the *Overview* chapter in the *Ultra Cloud Core Subscriber Microservices Infrastructure* documentation for more information.

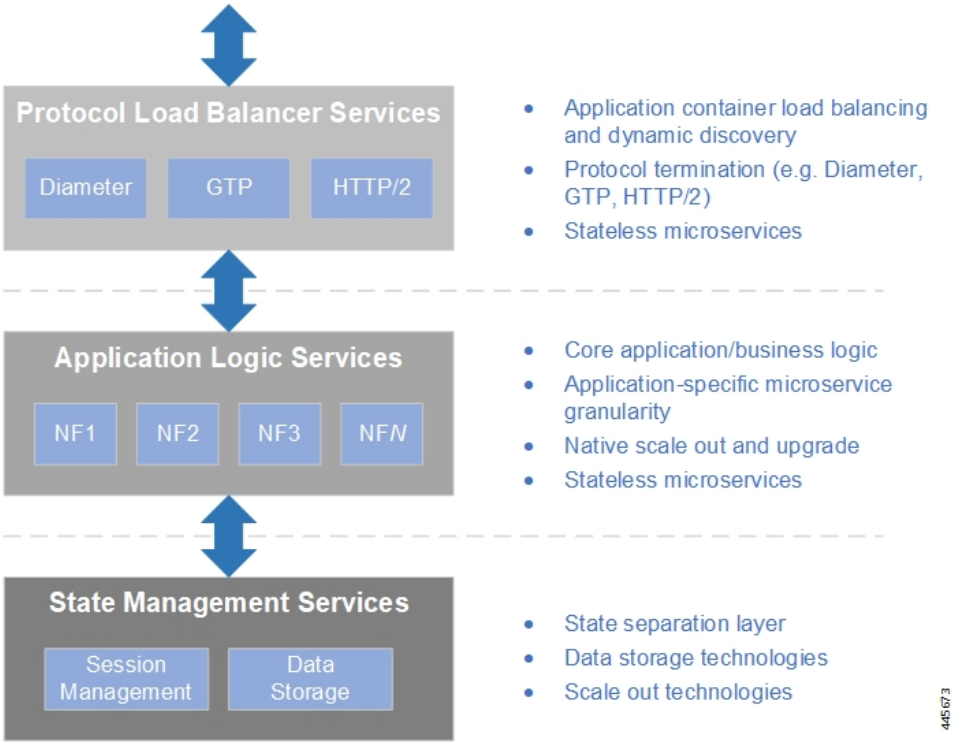
Control Plane Network Function Architecture

CP NFs are designed around a three-tiered architecture that take advantage of the stateful/stateless capabilities afforded within cloud native environments.

The architectural tiers are as follows:

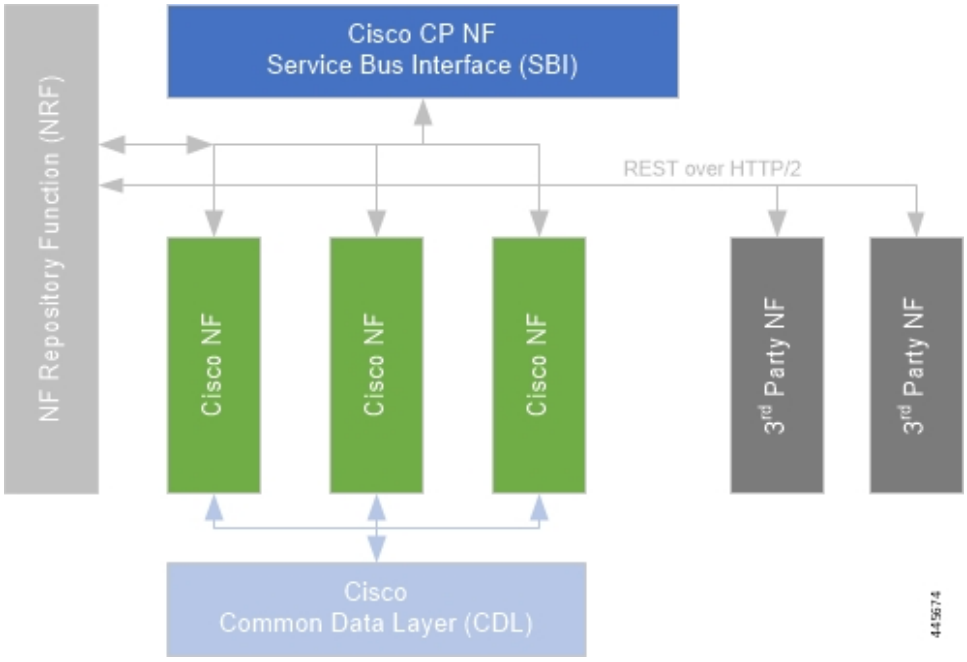
- Protocol Load Balancer Services — These are stateless microservices that are primarily responsible for dynamic discovery of application containers as well as for protocol proxy and/or termination. These include traditional 3GPP protocols and new protocols introduced with 5G.
- Applications Services — Responsible for implementing the core application/business logic, these are the stateless services that render the actual application based on the received information. This layer may contain varying degrees of microservice granularity. Application services are stateless.
- State management services — Enable stateless application services by providing a common data layer (CDL) to store/cache state information (e.g. session and subscriber data). This layer supports various data storage technologies from in-memory caches to full-fledge databases.

Figure 3: Control Plan Network Function Tiered Architecture

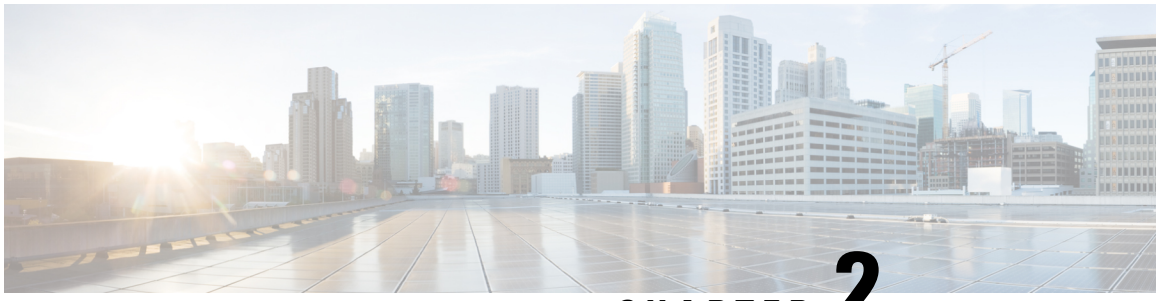


The three-tiered architecture on which Cisco's CP NFs are designed full support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

Figure 4: Cisco CP NF Service-based Architecture Support



Refer to the *Overview* Chapter for more information on the respective Cisco NF.



CHAPTER 2

5G SMF Overview

Feature Summary and Revision History

Summary Data

Table 3: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 4: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Product Description

The Cisco Session Management Function (SMF) is one of the Control Plane Network Functions (NF) of the 5G core network (5GC). The SMF is responsible for the session management with the supported individual functions on a per-session basis.

A single instance of SMF can support some or all the functionalities of the SMF. As specified in 3GPP TS 23.501, the SMF supports the following functionalities:

- Handles session management. For example, session establishment, modification and release, including the tunnel between the User Plane function (UPF) and the access network (AN).
- Handles user element (UE) IP address allocation and management, which includes an optional authorization.
- Performs Dynamic Host Configuration Protocol for IPv4 (DHCPv4) and DHCPv6 functions, both as server and client.
- Performs Allocation and Retention Priority (ARP) proxying and IPv6 Neighbor Solicitation Proxying functionality for the Ethernet PDUs. The SMF communicates with the ARP and the IPv6 Neighbor Solicitation Request by providing the MAC address. This address corresponds to the IP address that exists in the request.
- Selects and controls the UPF for the Ethernet PDU sessions. The UP function includes controlling the UPF to proxy ARP or IPv6 Neighbor Discovery, and forwarding all ARP or IPv6 Neighbor Solicitation traffic to the SMF.
- Configures Traffic Steering at the UPF to route traffic to the corresponding Data Network (DN).
- Terminates interfaces toward the Policy Control Function (PCF).
- Handles the Lawful Intercept (LI) for Session Manager (SM) events and interface to the LI system.
- Controls and synchronizes the charging data collection at the UPF.
- Terminates the SM parts of Non-Access-Stratum (NAS) messages.
- Routes packets and ensures the delivery of information through the Downlink Data Notification (DDN).
- Initiates the AN-specific SM information that is sent through the Access and Mobility Management Function (AMF) to AN over the N2 interface.
- Determines the session and service continuity (SSC) mode of a session.
- Provides the following roaming functionalities:
    - Manages the local enforcement to apply Quality of Service (QoS) SLAs (VPLMN).
    - Collects charging data and supports the charging interfaces.
    - Supports communication with the external Data Network (DN). The communication is for the transport of signaling for the PDU Session authorization or authentication by an external DN.

Use Cases and Features

This section describes the use cases that SMF supports in this release.

Base SMF Configuration

The SMF base configuration provides a detailed view of the configurations that are required for making the SMF operational. This includes setting up the infrastructure to deploy the SMF, deploying the SMF through SMI, and configuring the Ops Center for exploiting the SMF capabilities over time.

For more information on SMI, see the *Ultra Cloud Core SMI Cluster Deployer Operations Guide*.

The following feature is related to this use case:

- Deploying and Configuring SMF through Ops Center, on page 23

4G Session Support with 5GS SBI Interfaces

SMF leverages the 3GPP provision for the UEs that can support both 5G and 4G NAS to connect to both 4G and 5G core networks. With this provision, the SMF includes the EPS interworking support and acts as a PGW-C+SMF. The interfaces, such as the Gx, Gy, or Gz, which are used for a 4G session creation are replaced with the corresponding 5G core SBI interfaces, such as the Npcf and Nchf.

The following feature is related to this use case:

- 4G to 5G Data Session Handover Support, on page 89.

5G Session Support

The Session and Service Continuity (SSC) support in 5G system architecture addresses the continuous requirements of different applications and services for a User Equipment (UE). The 5G system supports the SSC modes such that the network maintains the connectivity service to the UE. The SMF manages the UE IP address and ID allocation for establishing sessions. The SMF also maintains session connectivity on interfaces, such as N40, N4, N7, and N10, to facilitate charging.

The SMF uses the Xn interface to handover a UE from a source NG-RAN to the target NG-RAN when the AMF is unchanged, and without relocating the UPF. The SMF includes the N3 tunnel profile configuration to enable the notifications on the Control Plane (CP) and enable buffering on the UPF. The SMF supports activation and deactivation of the User Plane (UP) connection of a PDU session. The SMF also includes the DNS proxy feature to configure proxy servers for resolving the host names and their IP addresses.

The following features are related to this use case:

- Inter gNodeB Handover, on page 295
- DNS Proxy Integration, on page 193
- IP Pool Allocation per DNN, on page 354
- Load-based Selection of UPF, on page 339
- Protocol Data Unit RAN Tunnel Endpoint Identifier Session, on page 441

- Resource Management, on page 521
- Session and Service Continuity Mode, on page 529

5GS-EPS Interworking

The SMF supports interworking with EPS using the N26 interface (which is an inter-CN interface between the MME and the 5GS AMF) to enable interworking between the Evolved Packet Core (EPC) and the NG core networks. Support of the N26 interface in the network is optional for interworking. The N26 interface supports a subset of the functionalities over S10 interface to enable interworking. The UE uses the EPC NAS or 5GC NAS procedures that are based on the core network. The SMF supports QoS flow failures for access and mobility procedures.

The following features are related to this use case:

- 4G to 5G Data Session Handover Support, on page 89
- Timers Support, on page 581
- EPS Interworking, on page 201
- Flow Failure Handling for Access and Mobility Procedures, on page 271

Access and Mobility Support

The SMF supports the access and mobility through session management procedures for PDU session establishment, modification, and release. The SMF supports N2-based handovers for intra- or inter-AMF when a UE moves from one NG-RAN to another NG-RAN for Data Forwarding Tunnel (DFT) and Indirect Data Forwarding Tunnel (IDFT) cases. With the multi-DNN support, SMF has multiple PDN connections for providing various services including Internet and Voice over New Radio (VoNR) services. The SMF supports network-initiated messages when a UE is either in the CM-Idle state or in the CM-Connected state.

Access and mobility support includes the intra-5G handover use case, which has the following handover support:

- Xn Handover
- Intra-AMF N2 Handover
- Inter-AMF N2 Handover

The following features are related to this use case:

- CHF and PCF Integration for Access and Mobility Procedures, on page 167
- Inter gNodeB Handover, on page 295
- Multiple and Virtual DNN Support, on page 347
- Network-initiated Messages Support, on page 357
- Policy and User Plane Management, on page 453
- Voice over New Radio, on page 599

Charging Integration

The SMF supports converged charging and uses the Nchf or N40 interface to generate charging events. The SMF supports offline failover for charging when a charging (CHF) server fails. Based on the charging data information that SMF receives, it provides reporting level support for online and offline charging.

The following feature is related to this use case:

- SMF Charging, on page 533

Cloud Native Infrastructure

The SMF services includes the configuration to process PDU Session Management API calls. The IP Address Management (IPAM) technique is integrated with the SMF in the Application Services layer for tracking and managing the IP address space of a network. The SMF uses the Operations Center interface, which is a system-level infrastructure, to initiate the deployment of micro-services, to push application specific configuration to one or more micro-services, and to run application-specific commands to invoke APIs in application-specific pods.

The following features are related to this use case:

- NRF Discovery, on page 377
- Policy and User Plane Management, on page 453
- Router Solicit and Router Advertisement, on page 525
- Static IP Support, on page 324

High Availability Support

The SMF supports high availability with the new "smf-udp-proxy" Kubernetes pod. This pod performs the following functions:

- Acts as a proxy for all types of UDP messages.
- Sends the UDP payload out after it receives the payload from the protocol pods.
- Opens the UDP sockets on a virtual IP (VIP) instead of a physical IP to enable node-level high availability for the UDP proxy.

The following feature is related to this use case:

- UDP Proxy for SMF, on page 587

IPAM Support

IP Address Management (IPAM) is a technique for tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. The IPAM provides all the functionalities necessary for working with the cloud-native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions such as the Session Management Function (SMF), Policy Control Function (PCF), and so on.

The following feature is related to this use case:

- IP Address Management, on page 309

Lawful Intercept

The Lawful Intercept (LI) feature enables law enforcement agencies (LEAs) to intercept subscriber communications. The LI functionality provides the network operator the capability to intercept and control data messages of targeted mobile users. The SMF that handles the Control Plane actions for the PDU sessions includes an IRI-POI that has the LI capability to generate the related xIRI.

For more details, contact your Cisco account representative.

NRF Discovery Support

Based on the 3GPP-defined architecture model for 5G systems for data connectivity, SMF discovers the set of NF instances and their associate NF service instances. These instances, which are based on the NF profiles, are registered in the Network Repository Function (NRF) and meet the various input query parameters.

The following feature is related to this use case:

- NRF Discovery, on page 377

Policy Integration

The SMF communicates with the Unified Data Management (UDM) and Policy Control Function (PCF) to do the following:

- Procure the subscribed and authorized QoS parameters for the Guaranteed Bit Rate (GBR) and non-GBR flows
- Pass the relevant information to the UE (NAS), gNB (NGAP), and UPF (PFCP)

This ensures that all nodes on the network provide the desired QoS to the PDU session

The SMF uses the service-based N7 interface with the PCF to retrieve the session management policy information corresponding to the PDU session of the UE. The SMF selects the PCF during the PDU Session Establishment procedure. It also acts as a consumer of the PCF-provided session management policy service.

The following feature is related to this use case:

- Policy and User Plane Management, on page 453

RADIUS Support

In the 5G architecture, the serving network authenticates the Subscription Permanent Identifier (SUPI) during authentication and the key agreement between the UE and the network. In addition, the serving network can perform a secondary authentication for data networks outside the mobile operator domain. For this purpose, various EAP-based authentication methods and associated credentials are used among which the RADIUS protocol is one of the widely used authentication protocols.

The following feature is related to this use case:

- RADIUS Client, on page 499

SMF Emergency Support

The Emergency SoS Support feature enables the co-located cloud-native SMF and PGW-C to support the following:

- SoS emergency over LTE for subscribers camped on the 4G network
- SoS emergency service fallback to LTE for subscribers camped on the 5G network

The following feature is related to this use case:

- Emergency SoS Support, on page 101

SMF Inline Services

The SMF uses the Inline Services feature such as the Enhanced Charging Service (ECS) that enables operators to reduce billing-related costs and gives the ability to offer tiered, detailed, and itemized billing to their subscribers. Using shallow and deep packet inspection (DPI), the ECS [also known as Active Charging Service (ACS)] allows operators to charge subscribers based on the actual usage, number of bytes, premium services, location, and so on. The ECS also generates charging records for postpaid and prepaid billing systems.

The following features are related to this use case:

- Policy and User Plane Management, on page 453
- Content Filtering, Event Detail Records, and X-Header Enrichment Support, on page 179

SMF Specification Compliance

The SMF supports different 3GPP specification versions for the SMF interfaces. It processes the messages from the interfaces as per the compliance profile configured for the corresponding services.

The following feature is related to this use case:

- 3GPP Specification Compliance for SMF Interfaces, on page 83

UPF Integration

The SMF uses the available StarOS-based UPF node to meet the non-standard requirements on the UPF node to interwork with this UPF. To comply with the IPv6 Stateless Auto-configuration, the SMF supports ICMPv6 Router Solicit and Advertisement.

The following features are related to this use case:

- Customization of StarOS-based UPF on N4 Interface, on page 189
- Router Solicit and Router Advertisement, on page 525

VoLTE Support

The SMF supports Voice over Long-Term Evolution or LTE (VoLTE). The VoLTE technology utilizes the IP Multimedia Subsystem (IMS) to support cellular calls over the LTE access network.

The following feature is related to this use case:

- VoLTE Support, on page 623

VoNR Support

The SMF supports the Voice over New Radio (VoNR) solution for the voice and video communication for 5G networks. The voice services in 5GS over NG-RAN continues to be based on the IP Multimedia Subsystem (IMS), such as Voice over LTE (VoLTE).

The following feature is related to this use case:

- Voice over New Radio, on page 599

WiFi Support

The SMF supports Voice over Wi-Fi (VoWiFi). The VoWiFi technology provides the telephony services using Voice over IP (VoIP) from the mobile devices that are connected across a Wi-Fi network.

The following feature is related to this use case:

- VoWiFi Support, on page 635
- Wi-Fi Handovers, on page 643

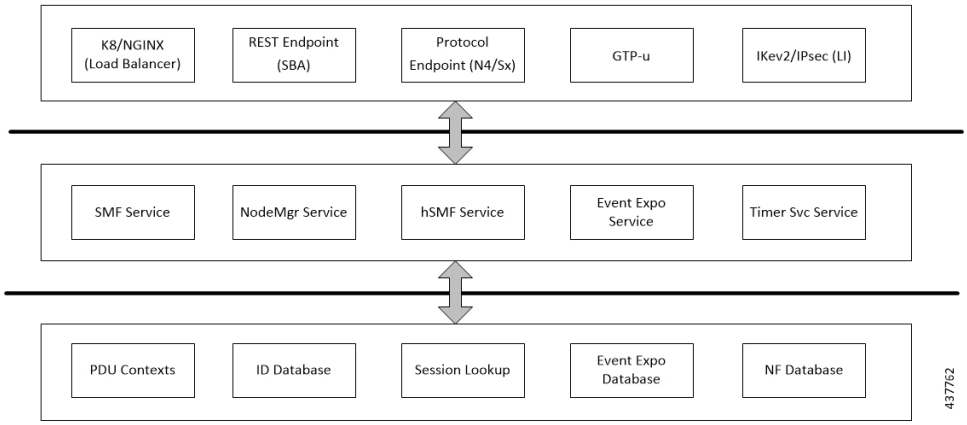
Deployment Architecture and Interfaces

The Cisco SMF is a part of the 5G core network functions portfolio with a common mobile core platform architecture. The core network functions include Access and Mobility Management Function (AMF), Network Repository Function (NRF), Policy Control Function (PCF), Network Slice Selection Function (NSSF), and User Plane Function (UPF).

SMF Architecture

The SMF network function consists of loosely coupled microservices together. The microservice decomposition is based on a three-layered architecture as illustrated in the following figure.

Figure 5: SMF 3-Layered Micro Services Architecture



Following are the three layers of the SMF architecture:

- Layer 1—Protocol and Load Balancer services (Stateless)
- Layer 2—Application services (Stateless)
- Layer 3—Database services (Stateful)

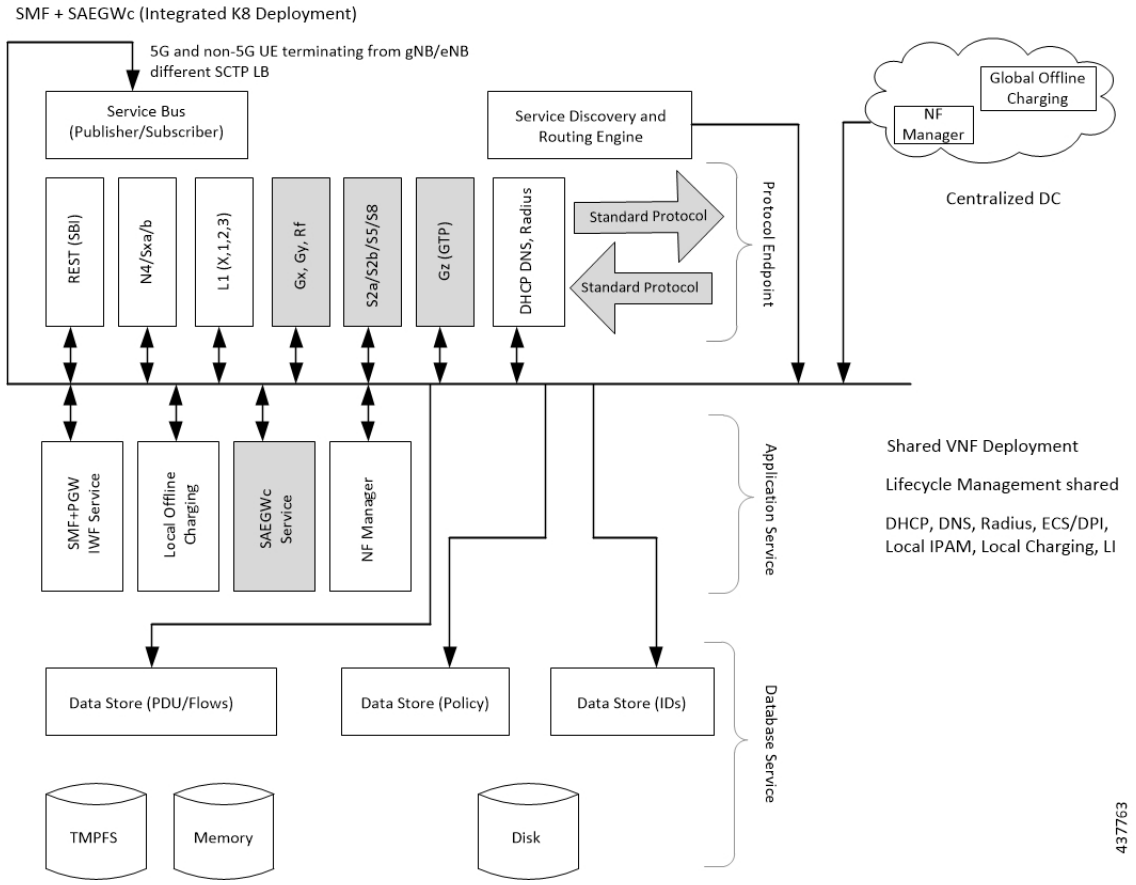
SMF Deployment

The 5G Mobility NFs deployment supports the following modes:

- Standalone mode: In this mode, each NF together with the required microservices is deployed in a separate name space in Kubernetes.
- Converged mode: In this mode, several NFs are deployed together in a single name space and micro-service common to NFs render the service to all the deployed NFs.

The following figure illustrates the SMF and SAEGW service that is deployed in the converged mode.

Figure 6: SMF and SAEGW Service Deployment in Converged Mode



Supported Interfaces

This section describes the interfaces supported between the SMF and other network functions in the 5GC.

- N4—Reference point between the SMF and UPF.
- N7—Reference point between the SMF and PCF.
- N10—Reference point between the UDM and SMF.
- N11—Reference point between the AMF and SMF.
- N40—Reference point between the SMF and CHF.
- S5—Interface between the PGW-C and S-GW.
- S2b—Interface between the PGW-C and ePDG.

Life Cycle of Data Packet

The following call flow depicts the life cycle of a data packet traversing through various pods of the SMF for a successful PDU session establishment.

The SMF application includes the following pods:

- REST-EP
- Cache
- Service
- Nodemgr
- Protocol
- UDP-Proxy
- CDL

Figure 7: End-to-End PDU Session Establishment Call Flow for Data Packets

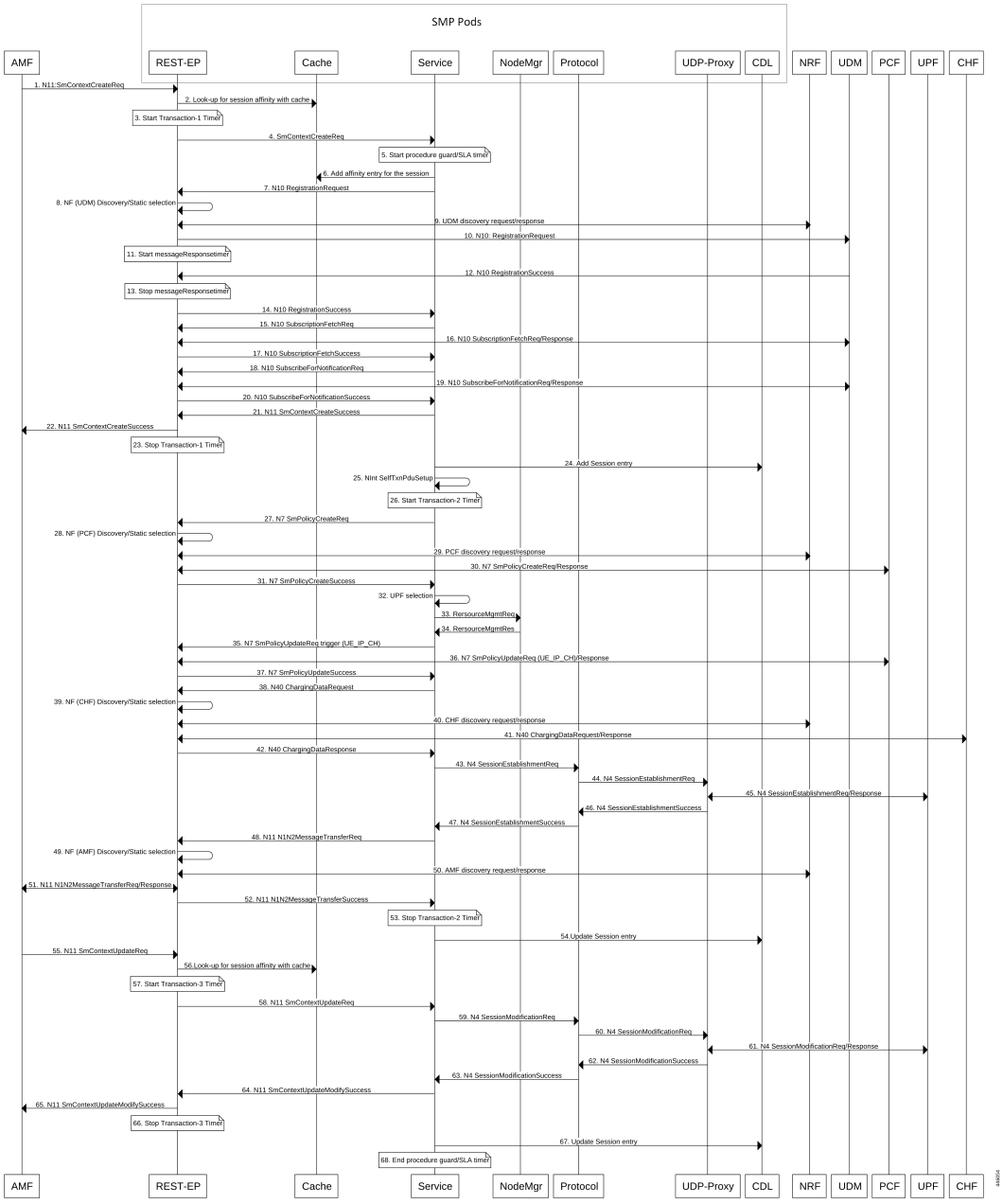


Table 5: End-to-End PDU Session Establishment Call Flow Description

Step	Description
1	The AMF sends N11:SMContextCreateRequest to the SMF, which terminates on the VIP-IP/external IP of REST-EP pod.

Step	Description
2	The REST-EP pod performs look-up for session affinity with cache pod. The SMF does not have the entry for the user session. The cache output does not result in any SMF-service affinity for the user session. Kubernetes service/ISTIO load balancer selects one SMF-service pod from multiple SMF-service pods that are configured.
3	The REST-EP starts the timer associated with transaction-1. The PDU session establishment procedure involves using three transactions which are started at different stages of the call flow. The default transaction timer on SMF is 10 seconds. The transaction timers are configurable through Service Level Agreement (SLA) feature.
4	The REST-EP forwards the N11:SMContextCreateRequest to the selected SMF-service.
5	The SMF-service starts procedure timer (guard timer/SLA timer). The SLA timers are configurable.
6	The SMF-service adds affinity entry with cache pod for the session. The SMF continues to use the same selected SMF-service in the subsequent stages of the call flow until the cache is expired.
7	The SMF-service instructs the REST-EP pod to trigger N10: Registration Request.
8	The REST-EP decides whether to perform NF discovery or static NF selection of UDM based on the configuration.
9	The REST-EP encodes and sends UDM discovery request to the NRF and receives a successful response with the list of UDMs.
10	The REST-EP encodes and sends N10:RegistrationRequest to the selected UDM.
11	The REST-EP starts messageResponseTimer. The default value of the configurable messageResponseTimeout is 2 seconds. The messageResponseTimer is applicable for all outbound HTTP2 messages initiated by SMF. They are not explicitly called out in the subsequent stages of the call flow.
12	The REST-EP receives successful N10:RegistrationResponse from the UDM.
13	The REST-EP stops messageResponseTimer.
14	The REST-EP forwards the N10:RegistrationResponse to the SMF-service.
15	The SMF-service instructs the REST-EP pod to trigger N10:SubscriptionFetchRequest.
16	The REST-EP encodes and sends N10: SubscriptionFetchRequest to the UDM. The REST-EP receives a response from the UDM.
17	The REST-EP forwards the N10:SubscriptionFetchResponse to the SMF-service.
18	The SMF-service instructs the REST-EP pod to trigger N10:SubscribeNotificationRequest.
19	The REST-EP encodes and sends N10:SubscribeNotificationRequest to UDM. The REST-EP receives a response from the UDM.
20	The REST-EP forwards the N10:SubscribeNotificationRequest to the SMF-service.

Step	Description
21	The SMF-service sends N11:SMContextCreateResponse to the REST-EP.
22	The REST-EP forwards the N11:SMContextCreateResponse to the AMF.
23	The REST-EP stops the transaction-1 timer started in step 3.
24	The SMF-service adds the session entry information in the CDL.
25	The SMF-service starts an internal transaction by sending NIntSelfTxnPduSetup message.
26	The SMF-service starts the timer associated with transaction-2.
27	The SMF-service instructs the REST-EP pod to trigger N7:SMPolicyCreateReq.
28	The REST-EP decides whether to perform NF discovery or static NF selection of PCF based on the configuration.
29	The REST-EP encodes and sends the PCF discovery request to the NRF and receives a successful response with the list of PCFs.
30	The REST-EP encodes and sends N7:SMPolicyCreateReq to the selected PCF. The REST-EP receives a response from the PCF.
31	The REST-EP forwards N7:SmPolicyCreateSuccess to the SMF-service.
32	The SMF-service performs the UPF selection.
33	The SMF-service sends ResourceMgmtReq to IPAM module of Nodemgr to request the IP address for the UE.
34	The SMF-service receives ResourceMgmtResp from the IPAM module of the Nodemgr with the IP address to the UE.
35	The SMF-service instructs the REST-EP pod to trigger N7:SMPolicyUpdateReq with trigger "UE_IP_CH".
36	The REST-EP encodes and sends N7:SMPolicyUpdateReq with UE_IP_CH trigger to the selected PCF. The REST-EP receives a response from the PCF.
37	The REST-EP sends N7:SMPolicyUpdateSuccess to the SMF-service.
38	The SMF-service instructs the REST-EP pod to trigger N40:ChargingDataRequest.
39	The REST-EP decides whether to perform the NF discovery or static NF selection of CHF based on the configuration.
40	The REST-EP encodes and sends the CHF discovery request to the NRF. The REST-EP receives a successful response with the list of CHFs.
41	The REST-EP encodes and sends N40:ChargingDataRequest to the selected CHF. The REST-EP receives a response from the CHF.
42	The REST-EP forwards N40:ChargingDataResponse to the SMF-service.
43	The SMF-service instructs the SMF-Protocol pod to trigger N4:SessionEstablishmentRequest.
44	The SMF-Protocol encodes and sends the N4:SessionEstablishmentRequest to the UDP-Proxy pod.

Step	Description
45	The UDP-Proxy pod sends the N4:SessionEstablishmentRequest to the UPF. The UDP-Proxy receives a response from the UPF.
46	The UDP-Proxy forwards the N4:SessionEstablishmentResponse to the SMF-Protocol pod.
47	The SMF-protocol forwards the N4:SessionEstablishmentResponse to the SMF-service.
48	The SMF-service instructs the REST-EP to trigger N11:N1N2MessageTransferReq.
49	The REST-EP decides whether to perform NF discovery or static NF selection of AMF based on the configuration.
50	The REST-EP encodes and sends the AMF discovery request to the NRF. The REST-EP receives a successful response with the list of AMFs.
51	The REST-EP encodes and sends N11:N1N2MessageTransferReq to the selected AMF. The REST-EP receives a successful response from the AMF.
52	The REST-EP forwards the N11:N1N2MessageTransferSuccess to the SMF-service.
53	The REST-EP stops the transaction-2 timer started in step 26.
54	The SMF-service updates the session entry in the CDL.
55	The REST-EP receives N11:SMContextUpdate from the AMF.
56	The REST-EP looks-up for session affinity in the cache pod and identifies the SMF-service handling the session.
57	The REST-EP starts the timer associated with transaction-3.
58	The REST-EP forwards the N11:SMContextUpdate to the SMF-service pod learnt in step 56.
59	The SMF-service instructs the SMF-Protocol pod to trigger N4:SessionModificationRequest.
60	The SMF-Protocol encodes and sends the N4:SessionModificationRequest to the UDP-Proxy pod.
61	The UDP-Proxy pod sends the N4:SessionModificationRequest to the UPF. The UDP-Proxy receives a response from the UPF.
62	The UDP-Proxy forwards the N4:SessionModificationResponse to the SMF-Protocol pod.
63	The SMF-protocol forwards the N4:SessionModificationResponse to the SMF-service.
64	The SMF-service forwards the N11:SMContextUpdateSuccess to the REST-EP.
65	The REST-EP forwards the N11:SMContextUpdateSuccess to the AMF.
66	The REST-EP stops the transaction-3 timer started in step 57.
67	The SMF-service updates the session entry in the CDL.
68	The SMF-service stops the procedure timer (guard timer/SLA timer).

License Information

The SMF supports Cisco Smart Licensing. For more information, see the Smart Licensing, on page 47 chapter in this document.

Standards Compliance

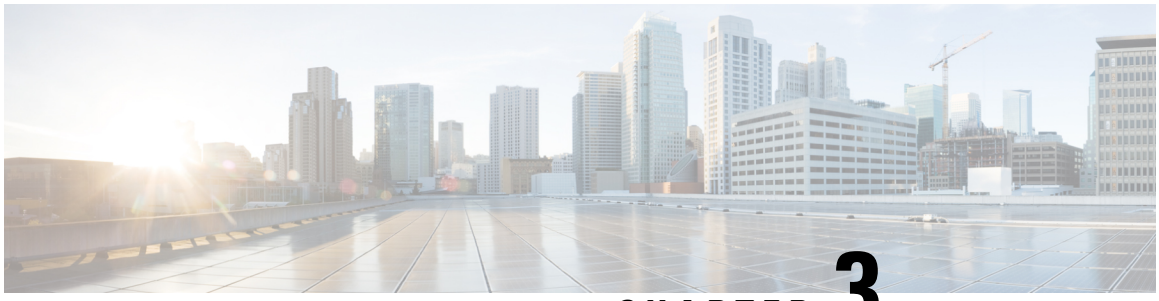
Cisco SMF complies with the following 3GPP standards as per Release 15 Dec 2018:

- 3GPP TS 23.501
- 3GPP TS 23.502
- 3GPP TS 23.503
- 3GPP TS 23.510
- 3GPP TS 24.008
- 3GPP TS 24.501
- 3GPP TS 29.244
- 3GPP TS 29.501
- 3GPP TS 29.502
- 3GPP TS 29.503
- 3GPP TS 29.510
- 3GPP TS 29.512
- 3GPP TS 29.518
- 3GPP TS 32.255
- 3GPP TS 32.290
- 3GPP TS 32.291, Release 15 June 2019
- 3GPP TS 38.413

Limitations

The SMF has the following limitation:

- QoS flow modifications and errors are not supported.



CHAPTER 3

Deploying and Configuring SMF through Ops Center

Feature Summary and Revision History

Summary Data

Table 6: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 7: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF deployment and configuration procedure involves deploying the SMF through the Subscriber Microservices Infrastructure (SMI) Cluster Deployer and configuring the settings or customizations through the SMF Operations (Ops) Center. The Ops Center is based on the ConfD CLI. The SMF configuration includes the NRF profile data configuration and the externally visible IP addresses and ports.

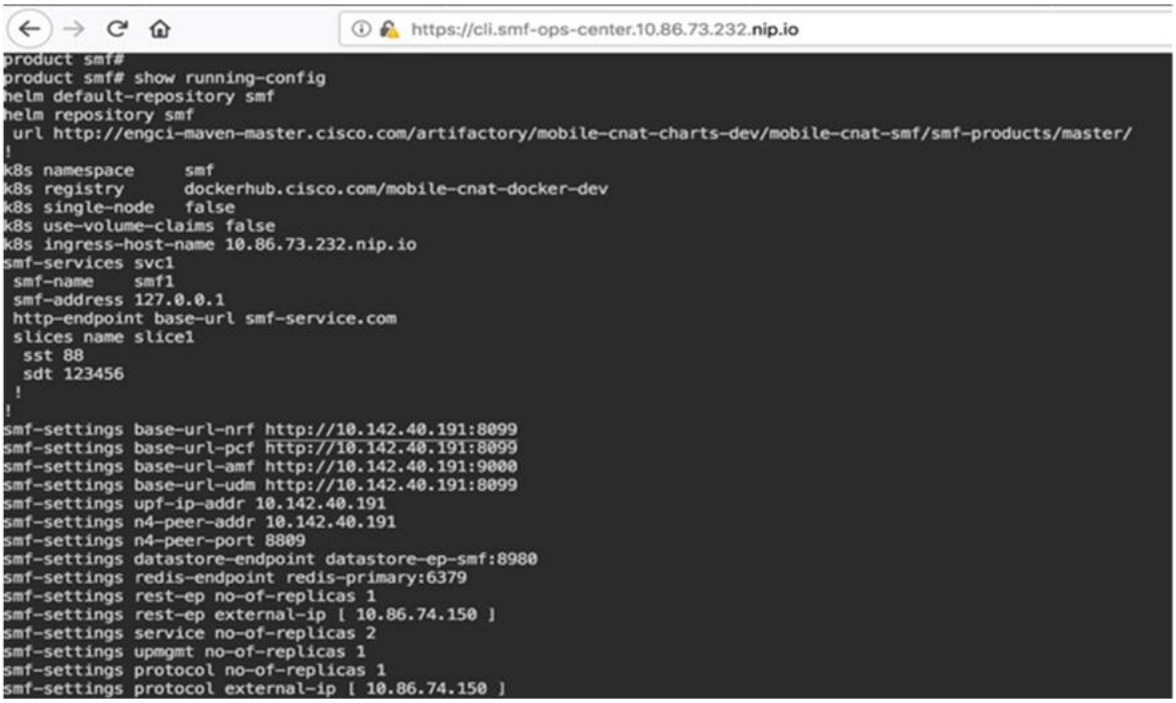
SMF Ops Center

The Ops Center is a system-level infrastructure that provides the following functionality:

- A user interface to trigger a deployment of microservices with the flexibility of providing variable helm chart parameters to control the scale and properties of Kubernetes objects (deployment, pod, services, and so on) associated with the deployment.
- A user interface to push application-specific configuration to one or more microservices through Kubernetes configuration maps.
- A user interface to issue application-specific execution commands (such as show and clear commands). These commands:
  - Invoke some APIs in application-specific pods
  - Display the information returned on the user interface application

The following screenshot is a sample of the web-based command line interface presented to the user.

Figure 8: Web-based CLI of Ops Center



The SMF Ops Center allows you to configure the features such as licensing, SMF engine, REST Endpoint, and CDL.

Prerequisites

Before deploying SMF on the SMI layer:

- Ensure that all the virtual network functions (VNFs) are deployed.
- Run the SMI synchronization operation for the SMF Ops Center and Cloud Native Common Execution Environment (CN-CEE)

Deploying and Accessing SMF

This section describes how to deploy SMF and access the SMF Ops Center.

Deploying SMF

The SMI platform is responsible for deploying and managing the Cloud Native 5G SMF application and other network functions.

For deploying SMF Ops Center on a vCenter environment, see *Deploying and Upgrading the Product* section in the *UCC SMI Cluster Deployer Operations Guide*.

For deploying SMF Ops Center on a OpenStack environment, see *UAME-based VNF Deployment* section in the *UAME-based 4G and 5G VNF Deployment Automation Guide, Release 6.9*

Accessing the SMF Ops Center

You can connect to the SMF Ops Center through SSH or the web-based CLI console.

- SSH:

  ssh admin*@ops_center_pod_ip* **-p 2024**

- Web-based console:

  1. Log in to the Kubernetes master node.
  2. Run the following command:

     kubectl get ingress <*namespace*>

     The available ingress connections get listed.
  3. Select the appropriate ingress and access the SMF Ops Center.
  4. Access the following URL from your web browser:

     cli.<*namespace*>**-ops-center**.<*ip_address*>.**nip.io**

By default, the Day 0 configuration is loaded into the SMF.

Day 0 Configuration

To view the Day 0 configuration, run the following command.

show running-config

The following is a sample Day 0 configuration:

```
root@smf-cluster# ssh -p 2024 admin@$(kubectl get svc -n smf-smf --no-headers | grep
smf-ops-center| grep 2024 |awk '{print $3}')
admin@1.1.1.1's password:
Welcome to the CLI
admin connected from 2.2.2.2 using ssh on ops-center-smf-smf-ops-center-76bbc7f4df-rkrff
product smf# show running-config
helm default-repository base-repos
helm repository base-repos
url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-smf/smf-products/master/
exit
k8s namespace smf-smf
k8s registry dockerhub.cisco.com/smi-fuse-docker-internal
k8s single-node false
k8s use-volume-claims false
k8s ingress-host-name 1.1.1.2.nip.io
aaa authentication users user admin
 uid        117
 gid        117
 password   $1$fvlWGa/b$GW6OyeqG77lQ.Xu/qcbgu.
 ssh_keydir /tmp/admin/.ssh
 homedir    /tmp/admin
exit
aaa ios level 0
 prompt "\h> "
exit
aaa ios level 15
 prompt "\h# "
exit
aaa ios privilege exec
 level 0
  command action
  exit
  command autowizard
  exit
  command enable
  exit
  command exit
  exit
  command help
  exit
  command startup
  exit
 exit
 level 15
  command configure
  exit
 exit
exit
nacm write-default deny
nacm groups group LI
 user-name [ liadmin ]
exit
nacm groups group admin
 user-name [ admin ]
exit
```

```
nacm rule-list admin
 group [ admin ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
 rule any-access
  action permit
 exit
exit
nacm rule-list confd-api-manager
 group [ confd-api-manager ]
 rule any-access
  action permit
 exit
exit
nacm rule-list lawful-intercept
 group [ LI ]
 rule li-accept-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            permit
 exit
 rule li-accept-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            permit
 exit
exit
nacm rule-list any-group
 group [ * ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
exit
```

SMF Service Configuration

The SMF service requires the basic configuration to process PDU Session Management API calls.

Configuring SMF

The SMF configuration is provided using the Ops Center infrastructure.

The following is a sample SMF configuration:

```
smf-settings base-url-nrf http://10.81.71.223:8082/NRF
 smf-settings base-url-amf http://10.81.71.223:8090
 smf-settings base-url-udm http://10.81.71.224:8099
 smf-settings upf-ip-addr 10.81.71.224
 smf-settings n4-peer-addr 10.81.71.224
 smf-settings n4-peer-port 8809
 smf-settings datastore-endpoint datastore-ep-smf:8980
 smf-settings redis-endpoint redis-primary:6379
 smf-settings rest-ep no-of-replicas 1
 smf-settings rest-ep external-ip [ 10.81.71.224 ]
 smf-settings service no-of-replicas 1
 smf-settings upmgmt no-of-replicas 1
 smf-settings protocol no-of-replicas 1
 smf-settings protocol external-ip [ 10.81.71.228 ]
```

The following table describes the supported SMF commands:

Table 8: Supported SMF Commands

No.	Configuration	Description
1	**smf-services** *service_name*	Configures a new SMF service. Entering this command results in a sub command mode. *service_name* is the name of the SMF service.
2	**smf-name** *node_name*	Specifies the NF name that is sent to the NRF during the SMF registration. This is a command in the smf-services mode.
3	**http-endpoint base-url** *url*	Configures the base endpoint URL to be sent in the NRF registration of the SMF. This is a command in the smf-services mode.
4	**dnn** *dnn_name*	Specifies the SMF-served DNN name. This is sent to the NRF during the SMF registration. This is a command in the smf-services mode.
5	**slices name** *slice_name* **sdt** *sdt_value* **sst** *sst_value*	Specifies the slice information to which the SMF belongs. This includes the slice type (sst) and slice descriptor (sdt). This is sent to the NRF during the SMF registration. This is a command in the smf-services mode.

No.	Configuration	Description
6	**smf-settings base-url-nrf** *nrf_url* **smf-settings base-url-amf** *amf_url* **smf-settings base-url-pcf** *pcf_url* **smf-settings base-url-udm** *udm_url* **smf-settings rest-ep no-of-replicas** *num_replicas*	Specifies the URL for the SBI interface towards the NRF, UDM, AMF, and PCF. These configurations are used when the nodes are not discovered through the NRF discovery procedure. Specifies the number of replicas for the different microservices of the SMF.
7	**smf-settings upf-ip-addr** *upf_ip_address* **smf-settings n4-peer-addr** *upf_ip_address* **smf-settings n4-peer-port** *upf_port*	Specifies the peer UPF IP address and port configuration.
8	**smf-settings n4-addr** *pfcp_intf_address*	Specifies the N4 interface IP address of the SMF towards the peer UPF.
9	**smf-settings datastore-endpoint** *datastore_endpoint* **smf-settings redis-endpoint** *redis_store_endpoint*	Specifies the endpoints for the mongodb and redis data stores.
10	**smf-settings rest-ep no-of-replicas** *num_replicas* **smf-settings service no-of-replicas** *num_replicas* **smf-settings upmgmt no-of-replicas** *num_replicas* **smf-settings protocol no-of-replicas** *num_replicas*	Specifies the number of replicas for the different microservices of the SMF.
11	**smf-settings rest-ep external-ip [** *restep_external_ip* **]** **smf-settings protocol external-ip [** *smfprot_external_IP* **]**	Specifies the service IP to be exposed for the rest-ep and smf-protocol services.
12	**ue-pool** *ipv4_address*	Specifies the IP pool to assign the IPv4 address in the CIDR notation to the UE session.

Contact your Cisco Account representative for the corresponding yang and render.yaml files.

Loading Day 1 Configuration

To load the Day 1 configuration for SMF, run the following command:

```
ssh admin@ops_center_pod_ip -p 2024 < Day1config.cli
```

Note The Day1config.cli file contains the necessary parameters required for the Day 1 configuration.

Alternatively, you can copy the configuration and paste it in the SMF Ops Center CLI to load the Day 1 configuration.

```
configure
  <Paste the Day 1 configuration here>
  commit
  exit
```

A sample *Day1config.cli* file, which contains the Day 1 configuration for SMF is shown below.

Day1config.cli

The following is a sample Day1config.cli file, which contains the Day 1 configuration for the SMF.

```
config
ipam
 source local
 address-pool ipv6
  vrf-name ISP
  tags
   dnn intershat
  exit
  ipv6
   prefix-ranges
    prefix-range 2001:4870:e00b:1500:: length 56
   exit
  exit
 exit
 address-pool poolv4
  vrf-name ISP
  tags
   dnn intershat
  exit
  ipv4
   split-size
    per-cache 1024
    per-dp    256
   exit
   address-range 0.0.0.1 0.0.0.254
  exit
 exit
exit
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
group nrf discovery udmdiscovery
 service type nrf nnrf-disc
  endpoint-profile epprof
   capacity   10
   priority   1
   uri-scheme http
   version
    uri-version v1
     full-version 1.1.1.[1]
    exit
   exit
```

```
   endpoint-name endpointName
    priority 1
    capacity 100
    primary ip-address ipv4 3.3.3.3
    primary ip-address port 8082
   exit
  exit
 exit
exit
group nrf mgmt MGMT
 service type nrf nnrf-nfm
  endpoint-profile mgmt-1
   priority   1
   uri-scheme http
   endpoint-name mgmt-1
    primary ip-address ipv4 3.3.3.3
    primary ip-address port 8082
    secondary ip-address ipv4 3.3.3.3
    secondary ip-address port 8083
    tertiary ip-address ipv4 3.3.3.3
    tertiary ip-address port 8084
   exit
  exit
 exit
exit
cdl node-type smf-cdl
cdl zookeeper replica 2
cdl kafka replica 2
etcd replicas 1
endpoint nodemgr
exit
endpoint gtp
 replicas 1
 vip-ip 4.4.4.4
exit
endpoint pfcp
 replicas 1
 nodes    2
exit
endpoint service
 replicas 1
 nodes    1
exit
endpoint protocol
 replicas 1
 nodes    2
 vip-ip 4.4.4.4
exit
endpoint sbi
 replicas 1
 nodes    2
 vip-ip 4.4.4.4
 interface nrf
  loopbackPort 7005
  vip-ip 20.20.20.5 vip-port 9005
 exit
 interface n7
  loopbackPort 7001
  vip-ip 20.20.20.1 vip-port 9001
 exit
 interface n10
  loopbackPort 7004
  vip-ip 20.20.20.4 vip-port 9004
 exit
```

```
 interface n40
  loopbackPort 7003
  vip-ip 20.20.20.3 vip-port 9003
 exit
exit
logging level application trace
logging level transaction trace
logging level tracing off
logging name infra.config.core level application debug
logging name infra.config.core level transaction warn
logging name infra.config.core level tracing warn
logging name infra.resource_monitor.core level application warn
logging name infra.resource_monitor.core level transaction warn
deployment
 app-name     SMF
 cluster-name Local
 dc-name      DC
 model        small
exit
k8 label protocol-layer key smi.cisco.com/node-type value smf-proto
exit
k8 label service-layer key vm-type value smf-svc
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit
helm default-repository smf
helm repository smf
 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-smf/smf-products/master/
exit
helm repository smf-stage
 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-smf/smf-products/dev-smf-stage/
exit
k8s namespace     smf
k8s registry      dockerhub.cisco.com/smi-fuse-docker-internal
k8s single-node   false
k8s use-volume-claims false
k8s ingress-host-name 1.1.1.1.nip.io
profile dnn intershat
 dns primary ipv4 11.11.1.1
 dns primary ipv6 66:66:1::aa
 dns secondary ipv4 22.22.2.2
 dns secondary ipv6 66:66:2::bb
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 dnn starent.com network-function-list [ upf ]
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 pcscf-profile    pcscf1
 ssc-mode 1
 session type IPV4 allowed [ IPV4V6 ]
 upf apn cisco.com
exit
profile dnn profDnn1
 dnn cisco.com network-function-list [ chf pcf udm upf ]
 charging-profile chgprf1
 ssc-mode 1
 session type IPV4
exit
```

```
profile dnn profDnn2
 dnn cisco.com network-function-list [ chf pcf rmgr udm upf ]
 charging-profile chgprf1
 ssc-mode 1
 session type IPV4
exit
profile charging chgprf1
 method                  [ offline ]
 limit volume 20
 limit duration 60
 tight-interworking-mode true
 reporting-level online rating-group
 reporting-level offline service-id
exit
profile pcscf pcscf1
 v4-list
  precedence 3
   primrary 3.3.3.1
   secondary 3.3.3.2
  exit
  precedence 5
   primrary 5.5.5.1
   secondary 5.5.5.2
  exit
  precedence 7
   primrary 7.7.7.1
   secondary 7.7.7.2
  exit
 exit
 v6-list
  precedence 3
   primrary 33:33::1
   secondary 33:33::2
  exit
  precedence 5
   primrary 55:55::1
   secondary 55:55::2
  exit
 exit
 v4v6-list
  precedence 3
   primrary ipv4 46.46.33.1
   primrary ipv6 46:46:33::1
   secondary ipv4 46.46.33.2
   secondary ipv6 46:46:33::2
  exit
  precedence 5
   primrary ipv4 46.46.55.1
   primrary ipv6 46:46:55::1
   secondary ipv4 46.46.55.2
   secondary ipv6 46:46:55::2
  exit
  precedence 7
   primrary ipv4 46.46.77.1
   primrary ipv6 46:46:77::1
   secondary ipv4 46.46.77.2
   secondary ipv6 46:46:77::2
  exit
 exit
exit
profile charging-characteristics 1
 charging-profile chgprf1
exit
profile icmpv6 icmpprf1
```

```
 options virtual-mac b6:6d:57:45:45:45
exit
profile smf smf1
 locality      LOC1
 bind-address ipv4 4.4.4.4
 bind-port     8090
 fqdn          5.5.5.5
 allowed-nssai [ slice1 slice2 ]
 plmn-id mcc 123
 plmn-id mnc 456
 service name nsmf-pdu
  type               pdu-session
  schema             http
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile dec18
  access-profile     access1
  policy subscriber polSub
 exit
exit
profile compliance dec18
 service nsmf-pdusession
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service namf-comm
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service n1
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service n2
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service nudm-sdm
  version uri v1
  version full 1.0.0
  version spec 15.2.1
 exit
 service nudm-uecm
  version uri v1
  version full 1.0.0
  version spec 15.2.1
 exit
 service nnrf-disc
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service nnrf-nfm
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service npcf-smpolicycontrol
  version uri v1
```

```
  version full 1.0.0
  version spec 15.2.0
 exit
 service nchf-convergedcharging
  version uri v2
  version full 1.0.0
  version spec 15.2.1
 exit
exit
profile network-element amf amf1
 nf-client-profile        amfP1
 failure-handling-profile FH3
 query-params [ dnn ]
exit
profile network-element pcf pcf1
 nf-client-profile        pcfP1
 failure-handling-profile FH1
 rulebase-prefix          cbn#
 predefined-rule-prefix   crn#
exit
profile network-element udm udm1
 nf-client-profile        udmP1
 failure-handling-profile FH1
exit
profile network-element upf upf1
 n4-peer-address ipv4 6.6.6.6
 n4-peer-port 8805
 keepalive    60
 dnn-list     [ dnn1 intershat starent ]
exit
profile network-element chf chf1
 nf-client-profile                chfP1
 failure-handling-profile         FH2
 nf-client-profile-offline        CP2
 failure-handling-profile-offline FH2
exit
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
 dscp-map qi5 2 arp-priority-level 3 uplink user-datagram dscp-marking 0x1c
 dscp-map qi5 2 arp-priority-level 3 downlink user-datagram dscp-marking 0x1a encsp-header
 dscp-marking 0x1b
 dscp-map qi5 3 arp-priority-level 3 uplink user-datagram dscp-marking 0x4
 dscp-map qi5 3 arp-priority-level 3 downlink user-datagram dscp-marking 0x3 encsp-header
copy-inner
exit
profile access access1
 eps-fallback cbr delay 500 max-retry 10 timeout 3
 n26 idft enable timeout 15
 n2 idft enable timeout 15
exit
profile nf-client nf-type udm
 udm-profile udmP1
  locality LOC1
   priority 30
   service name type nudm-sdm
    endpoint-profile EP1
     capacity   30
```

```
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9007
     exit
    exit
   exit
   service name type nudm-uecm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9001
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type pcf
 pcf-profile pcfP1
  locality LOC1
   priority 30
   service name type npcf-am-policy-control
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 50
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9003
     exit
    exit
   exit
   service name type npcf-smpolicycontrol
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 5
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9003
     exit
     endpoint-name realPCF
      priority 10
      primary ip-address ipv4 7.7.7.7
      primary ip-address port 9082
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type amf
 amf-profile amfP1
  locality LOC1
   priority 10
   service name type namf-comm
    endpoint-profile EP1
     capacity   20
     uri-scheme http
     endpoint-name EP1
      priority 30
```

```
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9002
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type chf
 chf-profile CP2
  locality LOC1
   priority 31
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9906
     exit
    exit
   exit
  exit
 exit
 chf-profile chfP1
  locality LOC1
   priority 10
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 50
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9904
     exit
     endpoint-name EP2
      priority 80
      primary ip-address ipv4 3.3.3.3
      primary ip-address port 9905
     exit
    exit
   exit
  exit
 exit
exit
profile nf-pair nf-type UDM
 locality client LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type AMF
 locality client LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type PCF
```

```
 locality client LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type UPF
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type CHF
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-client-failure nf-type chf
 profile failure-handling FH2
  service name type nchf-convergedcharging
   message type ChfConvergedchargingCreate
    status-code httpv2 0
     action continue
    exit
   exit
   message type ChfConvergedchargingUpdate
    status-code httpv2 0
     action continue
    exit
   exit
  exit
 exit
exit
policy subscriber polSub
 precedence 1
  sst              01
  sdt              ABcd01
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range 100000000000001
  supi-stop-range  999999999999999
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  operator-policy  opPol1
 exit
exit
policy operator opPol1
 policy dnn opPolDnn1
exit
policy dnn dnnPol1
 profile default
 dnn starent profile abc.com
exit
policy dnn opPolDnn1
 dnn intershat profile intershat
 dnn intershat1 profile profDnn1
exit
policy dnn polDnn
 profile default
 dnn intershat profile intershat
 dnn intershat1 profile profDnn1
 dnn intershat2 profile profDnn2
exit
nssai name slice1
 sst 01
 sdt ABcd01
 dnn [ intershat ]
```

```
exit
nssai name slice2
 sst 02
 sdt 000003
 dnn [ cisco.com ]
exit
active-charging service acs1
 packet-filter pkt1
  ip local-port range 2 to 23
  ip protocol = 23
  ip remote-address = 10.10.10.0/24
  ip remote-port range 12 to 34
  ip tos-traffic-class = 23 mask = 23
  priority 23
 exit
 packet-filter pkt2
  direction uplink
  ip local-port = 100
  ip protocol = 100
  ip remote-address = 1.1.1.1/32
  ip remote-port = 140
  priority  100
 exit
 packet-filter pkt3
  direction downlink
  ip local-port = 111
  ip protocol = 111
  ip remote-address = 2.2.2.2/31
  ip remote-port = 111
  priority  111
 exit
 charging-action ca1
  allocation-retention-priority 12 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard committedDataRate 2000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 3
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
 exit
 charging-action ca10
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000000 peak-burst-size 100
 violate-action discard
  tos af11
 exit
 charging-action ca11
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000000 peak-burst-size 100
 violate-action discard
 exit
 charging-action ca12
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca13
```

```
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca2
  allocation-retention-priority 13 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000000 peak-burst-size 100
violate-action discard committedDataRate 3000000000 committed-burst-size 100 exceed-action
 discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000000 peak-burst-size 100
 violate-action discard committedDataRate 4000000000 committed-burst-size 100 exceed-action
 discard
  qos-class-identifier 2
  tft-notify-ue
  tos af11
  tft packet-filter pkt2
 exit
 charging-action ca20
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca21
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca22
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca23
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca3
  allocation-retention-priority 14 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 1000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 1
  tft-notify-ue
  tos af11
  tft packet-filter pkt3
 exit
 charging-action ca4
  allocation-retention-priority 11 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 4000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 4
```

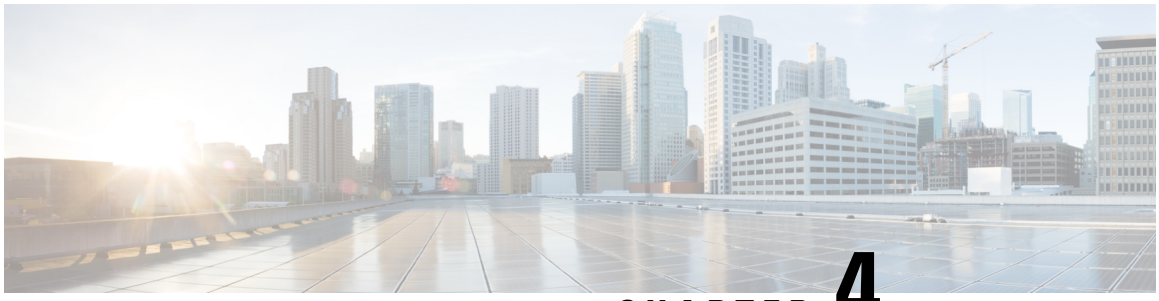
```
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
 exit
 charging-action ca5
  allocation-retention-priority 11 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 4000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 4
  tft-notify-ue
  tos af11
  tft packet-filter pkt2
 exit
 charging-action ca6
  allocation-retention-priority 11 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 4000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 4
  tft-notify-ue
  tos af11
  tft packet-filter pkt3
 exit
 charging-action ca7
  allocation-retention-priority 1 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 400000 peak-burst-size 100
violate-action discard
  qos-class-identifier 7
  tft-notify-ue
  tos af11
 exit
 charging-action caGyGz
  billing-action egcdr
  cca charging credit rating-group 102
  content-id         102
  service-identifier 202
 exit
 charging-action caOffline
  billing-action egcdr
  content-id         100
  service-identifier 200
 exit
 charging-action caOffline1
  billing-action egcdr
  content-id         11
  service-identifier 21
 exit
 charging-action caOffline2
  billing-action egcdr
  content-id         12
  service-identifier 22
 exit
 charging-action caOffline3
  billing-action egcdr
  content-id         13
```

```
 service-identifier 23
exit
charging-action caOffline4
 billing-action egcdr
 content-id 40
exit
charging-action caOfflineOnline
 billing-action egcdr
 cca charging credit
 content-id         30
 service-identifier 60
exit
charging-action caOfflineOnline1
 billing-action egcdr
 cca charging credit
 content-id         31
 service-identifier 61
exit
charging-action caOnline
 cca charging credit rating-group 100
 content-id         100
 service-identifier 200
exit
charging-action caOnline1
 cca charging credit rating-group 101
 content-id         101
 service-identifier 201
exit
charging-action caOnline2
 cca charging credit
 content-id         102
 service-identifier 202
exit
charging-action caOnline3
 cca charging credit
 content-id         103
 service-identifier 203
exit
charging-action caOnline4
 cca charging credit
 content-id 110
exit
charging-action nocharging
exit
rulebase cbn#spp-tmobile
 action priority 1 ruledef crn#test_1 charging-action ca1
 action priority 2 ruledef crn#test_2 charging-action ca2
exit
rulebase rba1
 action priority 1 dynamic-only ruledef rda1 charging-action ca1 description myrule1
 action priority 2 dynamic-only ruledef rda2 charging-action ca2 description myrule2
 action priority 3 dynamic-only ruledef rda3 charging-action ca3 description myrule3
exit
rulebase rba2
 action priority 10 ruledef rda10 charging-action ca10 description myrule10
 action priority 11 ruledef rda11 charging-action ca11 description myrule11
 action priority 12 dynamic-only ruledef rda12 charging-action ca12 description myrule12
 action priority 13 dynamic-only ruledef rda13 charging-action ca13 description myrule13
exit
rulebase rba3
 action priority 20 ruledef rda20 charging-action ca20 description myrule20
 action priority 21 ruledef rda21 charging-action ca21 description myrule21
 action priority 22 dynamic-only ruledef rda22 charging-action ca22 description myrule22
 action priority 23 dynamic-only ruledef rda23 charging-action ca23 description myrule23
```

```
exit
rulebase rba4
 action priority 30 ruledef rda3 charging-action ca3 description myrule3
 action priority 31 dynamic-only ruledef rda3 charging-action ca3 description myrule3
exit
rulebase rba5
 action priority 50 dynamic-only ruledef rda50 charging-action ca4 description myrule50
 action priority 51 dynamic-only ruledef rda51 charging-action ca5 description myrule51
 action priority 52 dynamic-only ruledef rda52 charging-action ca6 description myrule52
exit
rulebase rba6
 action priority 60 dynamic-only ruledef rda60 charging-action ca1 description myrule60
 action priority 61 dynamic-only ruledef rda61 charging-action ca1 description myrule61
 action priority 62 dynamic-only ruledef rda62 charging-action ca1 description myrule62
exit
rulebase rba7
 action priority 50 ruledef rda50 charging-action ca4 description myrule50
 action priority 51 ruledef rda51 charging-action ca5 description myrule51
 action priority 52 ruledef rda52 charging-action ca6 description myrule52
exit
rulebase rba8
 action priority 60 ruledef rda60 charging-action ca1 description myrule60
 action priority 61 ruledef rda61 charging-action ca1 description myrule61
 action priority 62 ruledef rda62 charging-action ca1 description myrule62
exit
rulebase rbaStatic
 action priority 10 ruledef rda20 charging-action caOffline
exit
rulebase rbaStatic-Online
 action priority 20 ruledef rdaStatic charging-action caOnline
exit
rulebase rbaStatic1
 action priority 10 ruledef rda20 charging-action caOffline
exit
rulebase rba_GyGz
 egcdr threshold volume downlink 100000 uplink 100000
 action priority 20 dynamic-only ruledef rdaPredefined charging-action caGyGz
 action priority 30 ruledef rda20 charging-action caGyGz
exit
rulebase rba_charging_StaticDynamic_Offline_Online_mix
 cca diameter requested-service-unit sub-avp volume cc-input-octets 11000 cc-output-octets
12000 cc-total-octets 23000
 credit-control-group onlineoffline
 egcdr threshold interval 100
 egcdr threshold volume downlink 150000 uplink 150000 total 300000
 action priority 20 dynamic-only ruledef rdaPredefined charging-action caOffline1
 action priority 21 dynamic-only ruledef rdaPredefined1 charging-action caOnline1
 action priority 31 ruledef rdaStatic charging-action caOfflineOnline
exit
rulebase rba_charging_StaticDynamic_offline
 egcdr threshold volume downlink 100000 uplink 100000
 action priority 20 dynamic-only ruledef rdaPredefined charging-action caOffline1
 action priority 30 ruledef rda20 charging-action caOffline
exit
rulebase rba_charging_StaticDynamic_online
 action priority 20 ruledef rda20 charging-action caOnline
 action priority 30 dynamic-only ruledef rdaPredefined charging-action caOnline1
exit
rulebase rbs1
 action priority 1 ruledef rds1 charging-action ca1 description myrules1
 action priority 2 ruledef rds2 charging-action ca2 description myrules2
exit
urr-list urr_smf
 rating-group 10 service-identifier 20 urr-id 1
```

```
 rating-group 11 service-identifier 21 urr-id 2
 rating-group 12 service-identifier 22 urr-id 3
 rating-group 13 service-identifier 23 urr-id 4
 rating-group 30 service-identifier 60 urr-id 20
 rating-group 31 service-identifier 61 urr-id 21
 rating-group 100 service-identifier 200 urr-id 5
 rating-group 101 service-identifier 201 urr-id 6
 rating-group 102 service-identifier 202 urr-id 7
 rating-group 103 service-identifier 203 urr-id 8
exit
ruledef rda1
 ip server-ip-address = 10.10.10.10
exit
ruledef rda10
 ip any-match = TRUE
exit
ruledef rda11
 ip any-match = TRUE
exit
ruledef rda12
 ip any-match = TRUE
exit
ruledef rda13
 ip any-match = TRUE
exit
ruledef rda2
 ip server-ip-address = 10.165.161.77/32
exit
ruledef rda20
 ip any-match = TRUE
exit
ruledef rda21
 ip any-match = TRUE
exit
ruledef rda22
 ip any-match = TRUE
exit
ruledef rda23
 ip any-match = TRUE
exit
ruledef rda3
 ip server-ip-address = 8.8.8.8/28
exit
ruledef rda40
 ip any-match = TRUE
exit
ruledef rda50
 ip server-ip-address = 50.50.50.50
exit
ruledef rda51
 ip server-ip-address = 51.51.51.51
exit
ruledef rda52
 ip server-ip-address = 52.52.52.52
exit
ruledef rda60
 ip dst-address = 60.60.60.60
exit
ruledef rda61
 ip dst-address = 61.61.61.61
exit
ruledef rda62
 ip dst-address = 62.62.62.62
exit
```

```
 ruledef rdaPredefined
  ip any-match = TRUE
 exit
 ruledef rdaStatic
  ip any-match = TRUE
 exit
 ruledef rdaStatic1
  ip any-match = TRUE
 exit
 ruledef rdaStatic2
  ip any-match = TRUE
 exit
 ruledef rds1
  ip any-match = TRUE
 exit
 ruledef rds2
  ip any-match = TRUE
 exit
 credit-control group onlineoffline
  diameter ignore-service-id true
 exit
exit
apn intershat
 gtpp group group1
 active-charging rulebase rba1
exit
gtpp group group1
 gtpp egcdr service-data-flow threshold interval 60
 gtpp egcdr service-data-flow threshold volume downlink 100000 uplink 100000 total 200000
apn intershat
gtpp group group1
exit
smiuser add-user username liadmin password Cisco@123
smiuser change-password username liadmin current_password Cisco@123 new_password Mitg_123
confirm_password Mitg_123
smiuser add-group groupname LI
smiuser assign-user-group username liadmin group LI
smiuser add-user username liadmin2 password Cisco@123
smiuser change-password username liadmin2 current_password Cisco@123 new_password Mitg_123
 confirm_password Mitg_123
smiuser add-group groupname LI2
smiuser assign-user-group username liadmin2 group LI2
smiuser add-user username liadmin3 password Cisco@123
smiuser change-password username liadmin3 current_password Cisco@123 new_password Mitg_123
 confirm_password Mitg_123
smiuser add-group groupname LI3
smiuser assign-user-group username liadmin3 group LI3
nacm groups group LI2
user-name [ liadmin2 ]
exit
nacm groups group LI3
user-name [ liadmin3 ]
exit
nacm rule-list lawful-intercept
group [ LI LI2 LI3 ]
commit
end
config
system mode running
commit
end
exit
```



CHAPTER 4

Smart Licensing

Feature Summary and Revision History

Summary Data

Table 9: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 10: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Smart Software Licensing

Smart Licensing is a cloud-based approach to licensing that simplifies the purchase, deployment, and management of Cisco software assets. Entitlements are purchased through your Cisco account via Cisco

Commerce Workspace (CCW) and immediately deposited into your Virtual Account for usage. This eliminates the need to install license files on every device. Products that are smart enabled communicate directly to Cisco to report consumption. A single location is available to customers to manage Cisco software licenses — the Cisco Software Central (CSC). License ownership and consumption are readily available to help make better purchase decision based on consumption or business need. See https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html for more information about Cisco Smart Licensing.

Comparison Between Legacy Licensing and Smart Licensing

Cisco employs two types of license models - Legacy Licensing and Smart Software Licensing. Legacy Licensing consists of software activation by installing Product Activation Keys (PAK) on to the Cisco product. A Product Activation Key is a purchasable item, ordered in the same manner as other Cisco equipment and used to obtain license files for feature set on Cisco Products. Smart Software Licensing is a cloud-based licensing of the end-to-end platform through the use of a few tools that authorize and deliver license reporting. Smart Software Licensing functionality incorporated into the NFs complete the product registration and authorization.

Cisco Software Central

Cisco Software Central (CSC) enables the management of software licenses and Smart Account from a single portal. The interface allows you to activate your product, manage entitlements, and renew and upgrade software. A functioning Smart Account is required to complete the registration process. To access the Cisco Software Central, see https://software.cisco.com.

Smart Accounts/Virtual Accounts

A Smart Account provides a single location for all Smart-enabled products and entitlements. It helps speed procurement, deployment, and maintenance of Cisco Software. When creating a Smart Account, you must have the authority to represent the requesting organization. After submitting, the request goes through a brief approval process.

A Virtual Account exists as a sub-account within the Smart Account. Virtual Accounts are a customer-defined structure based on organizational layout, business function, geography or any defined hierarchy. They are created and maintained by the Smart Account administrator.

See https://software.cisco.com to learn about the set up or manage the Smart Accounts.

Request a Cisco Smart Account

A Cisco Smart Account is an account where all products enabled for Smart Licensing are deposited. A Cisco Smart Account allows you to manage and activate your licenses to devices, monitor license use, and track Cisco license purchases. Through transparent access, you have a real-time view into your Smart Licensing products. IT administrators can manage licenses and account users within your organization's Smart Account through the Software Central.

Step 1 In a browser window, enter the following URL:

```
https://software.cisco.com
```

Step 2 Log in using your credentials, and then click **Request a Smart Account** in the **Administration** area.

The **Smart Account Request** window is displayed.

Step 3 Under **Create Account**, select one of the following options:

- **Yes, I have authority to represent my company and want to create the Smart Account** – If you select this option, you agree to authorization to create and manage product and service entitlements, users, and roles on behalf of your organization.
- **No, the person specified below will create the account** – If you select this option, you must enter the email address of the person who will create the Smart Account.

Step 4 Under **Account Information**:

a) Click **Edit** beside **Account Domain Identifier**.
b) In the **Edit Account Identifier** dialog box, enter the domain, and click **OK**. By default, the domain is based on the email address of the person creating the account and must belong to the company that will own this account.
c) Enter the **Account Name** (typically, the company name).

Step 5 Click **Continue**.

The Smart Account request will be in pending status until it has been approved by the Account Domain Identifier. After approval, you will receive an email confirmation with instructions for completing the setup process.

SMF Smart Licensing

At present, the Smart Licensing feature supports application entitlement for online and offline licensing for all 5G applications (PCF, SMF and NRF). The application usage is unrestricted during all stages of licensing including Out of Compliance (OOC) and expired stages.

Note A 90 day evaluation period is granted for all licenses in use. Currently, the functionality and operation of the 5G applications is unrestricted even after the end of the evaluation period.

Software Tags and Entitlement Tags

Tags for the following software and entitlements have been created to identify, report, and enforce licenses.

Software Tags

Software tags uniquely identify each licenseable software product or product suite on a device. The following software tags exist for the SMF.

Product Type / Description	Software Tag
Ultra Cloud Core - Session Management Function (SMF), Base Minimum	regid.2020-04.com.cisco.SMF,1.0_37ffdc21-3e95-4192-bcda-d3225b6590ce

Entitlement Tags

The following entitlement tags identify licenses in use:

Product Type / Description	Entitlement Tag
Ultra Cloud Core - Session Management Function (SMF), Base Minimum	regid.2020-04.com.cisco.SMF_BASE,1.0_b49f5997-21aa-4d15-9606-0cff88729f69

Note The license information is retained during software upgrades and rollback.

Configuring Smart Licensing

You can configure Smart Licensing after a new SMF deployment.

Users with Access to CSC

This section describes how to configure Smart Licensing if you have access to CSC portal from your environment.

Setting Up the Product and Entitlement in CSC

Before you begin, you need to setup your product and entitlement in the CSC. To setup your product and entitlement:

1. Log in to your CSC account.
2. Click **Add Product** and enter the following details.
   - **Product name** – Specify the name of the deployed product. For example, SMF.
   - **Primary PM CEC ID** – Specify the primary Project Manager's CEC ID for the deployed product.
   - **Dev Manager CEC ID** – Specify the Development Manager's CEC ID for the deployed product.
   - **Description** (Optional) – Specify a brief description of the deployed product.
   - **Product Type** – Specify the product type.
   - **Software ID Tag** – Specify the software ID Tag provided by the Cisco Accounts team.
3. Click **Create**.
4. Select your product from the **Product/Entitlement Setup** grid.
5. Click **Entitlement** drop-down and select **Create New Entitlement**.
6. Select **New Entitlement** in **Add Entitlement** and enter the following details.

- **Entitlement Name** – Specify the license entitlement name. For example, SMF_BASE.
- **Description** (Optional) – Specify a breif description about the license entitlement.
- **Entitlement Tag** – Specify the entitlement tag provided by the Cisco Accounts team.
- **Entitlement Type** – Specify the type of license entitlement.
- **Vendor String** – Specify the vendor name.

7. Click **Entitlement Allocation**.
8. Click **Add Entitlement Allocation**.
9. In **New License Allocation**, provide the following details:
   - **Product** – Select your product from the drop-down list.
   - **Entitlement** – Select your entitlement from the drop-down list.
10. Click **Continue**.
11. In **New License Allocation** window, provide the following details:
    - **Quantity** – Specify the number of licenses.
    - **License Type** – Specify the type of license.
    - **Expiring Date** – Specify the date of expiry for the license purchased.
12. Click **Create**.
13. Verify the status of Smart Licensing using the following command.

    `show license all`

    Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec
  Last Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME
```

```
Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

Registering Smart Licensing

You must register the product entitled to the license with CSC. In order to register, you must generate an ID token from CSC.

1. Log in to your CSC account.
2. Click **General > New Token** and enter the following details:
   - **Description** – Specify a brief description about the ID token.
   - **Expires After** – Specify the number of days for the token to expire.
   - **Max. Number Users** – Specify the maximum number of users.
3. Click **Create Token**.
4. Select **new ID token** in **Product Instance Registration Token**.
5. Click **Actions > Copy**.
6. Log in to SMF Ops Center CLI and paste the **ID token** using the following command.

   `license smart register` *`idtoken`*

   Example:

   ```
   SMF# license smart register
   Value for 'idtoken' (<string>): MTI2Y2FlNTAtOThkMi00YTAxLWE4M2QtOTNhNzNjNjY4ZmFiLTE2MTc4N
   Tky%0AMTA5MDh8ck1jUHNwc3k1ZC9nWFFCSnVEcUp4QU1jTFoxOGxDTU5kQ3lpa25E%0Ab04wST0%3D%0A
   SMF#
   ```

7. Verify the Smart Licensing status using the following command.

   `show license all`

Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems, Inc.
  Virtual Account: SMF-SMF
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Last Renewal Attempt: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Next Renewal Attempt: Oct 12 05:45:07 2020 GMT
  Registration Expires: Apr 15 05:40:31 2021 GMT

License Authorization:
  Status: AUTHORIZED on Apr 15 05:45:12 2020 GMT
  Last Communication Attempt: SUCCEEDED on Apr 15 05:45:12 2020 GMT
  Next Communication Attempt: May 15 05:45:12 2020 GMT
  Communication Deadline: Jul 14 05:40:40 2020 GMT

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=============
License Authorization Status: AUTHORIZED as of Apr 15 05:45:12 2020 GMT

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED_ALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

NOTES:

- **license smart register** – Registers Smart Licensing with CSC.
- *idtoken* – Specifies the ID token generated from CSC.

Deregistring Smart Licensing

To deregister Smart Licensing:

1. Log in to SMF Ops Center CLI and use the following command.

   `license smart deregister`

2. Verify the Smart Licensing status using the following command.

   `show license all`

   Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec
  Last Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

```
SMF#
```

NOTES:

- **license smart deregister** – Deregisters Smart Licensing from CSC.

Users without Access to CSC

The Smart License Reservation feature – Perpetual Reservation – is reserved for customers without access to CSC from their internal environments. With this feature, Cisco allows customers to reserve licenses from their virtual account and tie them to their devices Unique Device Identifier (UDI). This enables customers to use their devices with reserved licenses in a disconnected mode.

The subsequent sections describe the procedure involved in reserving Smart License for users without access to CSC from their internal environment.

Enabling Smart License Reservation

To enable Smart License reservation through SMF Ops Center CLI:

1. Log in to SMF Ops Center CLI and use the following configuration.

```
configure terminal
  license smart reservation
  commit
  exit
```

NOTES:

- **license smart reservation** – Enables license reservation.

Generating Smart License Reservation Request Code

To generate the Smart License reservation request code:

1. Log in to SMF Ops Center CLI.
2. To enable reservation, use the following configuration.

```
configure terminal
  license smart reservation
  commit
  exit
```

3. To request for a reservation code, use the following command.

```
license smart reservation request
```

Example:

```
SMF# license smart reservation request
reservation-request-code CJ-ZSMF:6GKJ2OA-NMUWA7Y-Ai75GxtBs-3B
SMF#
Message from confd-api-manager at 2020-04-15 05:51:37...
Global license change NotifyReservationInProgress reason code Success - Successful.
SMF#
```

NOTES:

- **license smart reservation** – Enables license reservation request code.
- **license smart reservation request** – Generates the license reservation request code.

Important You must copy the generated license request code from the SMF Ops Center CLI.

Generating an Authorization Code from CSC

To generate an authorization code from CSC using the license reservation request code:

1. Log in to your CSC account.
2. Click **License Reservation**.
3. Enter the Request Code: Paste the license reservation request code copied from the SMF Ops Center CLI in the **Reservation Request Code** text-box.
4. Select the Licenses: Click **Reserve a Specific License** radio-button and select *UCC 5G SMF BASE*.

Note In the **Reserve** text-box enter the value *1*.

5. Review your selection.
6. Click **Generate Authorization Code**.
7. Download the response file: The authorization code is generated and displayed on-screen. Click **Download as File** to download the authorization code.
8. Click **Close**.

Reserving Smart Licensing

To reserve Smart License for the deployed product using the authorization code generated in CSC:

1. Log in to SMF Ops Center CLI and use the following command.

   `license smart reservation install` *`authorization_code`*

   Example:

```
SMF# license smart reservation install
Value for 'key' (<string>):
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>35757dc6-2bdf-4fa1-ba7e-4190f5b6ea22</piid><timestamp>1586929992297</timestamp>
<entitlements><entitlement><tag>regid.2020-04.com.cisco.SMF_BASE,1.0_60b1da6f-3832-4687-90c9-8879dc815a27</tag>
<count>1</count><startDate>2020-Apr-08 UTC</startDate><endDate>2020-Oct-05 UTC</endDate>
<licenseType>TERM</licenseType><displayName>UCC 5G SMF BASE</displayName>
<tagDescription>Ultra Cloud Core - Session Management Function (SMF), Base
Minimum</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
<signature>MEYCIQC/9v5LpgFoEk2l4omIgjjk83g5WXjzs09kQnsO8D0jRgIhAMh+
```

```
D6DRuYmqh1TlfJoZxNte0fPKw6fHEY5CEF3+kPQj</signature>
<udi>P:SMF,S:6GKJ2OA-NMUWA7Y</udi></specificPLR>
SMF#
```

2. Verify the smart licensing status using the following command.

   show license all

   Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Wed Apr 15 05:53:31 GMT 2020
  Last Renewal Attempt: None

License Authorization:
  Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

License Usage
=============
License Authorization Status:
  Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020
  Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF),
Base Minimum
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>
  Reservation:
    Reservation Status: SPECIFIC INSTALLED
    Total Reserved Count: 1
    Term expiration: 2020-Oct-05 GMT

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y
```

```
Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

NOTES:

- **license smart reservation install** *authorization_code* – Installs a Smart License Authorization code.

Returning the Reserved License

You can return the reserved license to CSC if required. Use the following procedure to return the reserved license:

1. When the license reservation authorization code is installed in the SMF Ops Center.
   a. Log in to the SMF Ops Center CLI and use the following command.

      `license smart reservation return`

      Example:

      ```
      SMF# license smart reservation return
      reservation-return-code CJ6m3k-RAvu6b-hMNmwf-mrdcko-NoSwKL-tF7orz-9aNtEu-yVjGAm-D6j
      SMF#
      ```

   b. Copy the license reservation return code generated in SMF Ops Center CLI.
   c. Log in to your CSC account.
   d. Select your product instance from the list.
   e. Click **Actions > Remove**.
   f. Paste the license reservation return code in **Return Code** text-box.

   NOTES:

   - **license smart reservation return** – Returns a reserved Smart License.

2. When the license reservation authorization code is not installed in the SMF Ops Center.
   a. Log in to the SMF Ops Center CLI and use the following command to generate the return code.

      `license smart reservation return`
      `authorization_code`

Important Paste the license reservation authorization code generated in CSC to generate the return code.

   b. Log in to your CSC account.
   c. Select your product instance from the list.
   d. Click **Actions > Remove**.
   e. Paste the license reservation return code in **Return Code** text-box.

3. Verify the smart licensing status using the following command.

show license all

Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
  Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13

SMF#
```

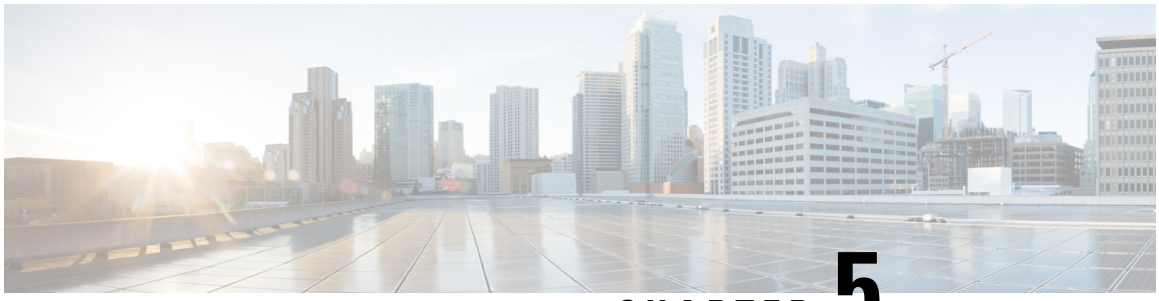
Monitoring and Troubleshooting Smart Licensing

You can use the following show commands to view Smart Licensing related information in the SMF Ops Center.

```
show license [ all | UDI | displaylevel | reservation | smart | status |
 summary | tech-support | usage ]
```

NOTES:

- **all** – Displays an overview of Smart Licensing information that includes license status, usage, product information and Smart Agent version.
- **UDI** – Displays Unique Device Identifiers (UDI) details.
- **displaylevel** – Depth to display information.
- **reservation** – Displays Smart Licensing reservation information.
- **smart** – Displays Smart Licensing information.
- **status** – Displays the overall status of Smart Licensing.
- **summary** – Displays a summary of Smart Licensing.
- **tech-support** – Displays Smart Licensing debugging information.
- **usage** – Displays the license usage information for all the entitlements that are currently in use.



CHAPTER 5

SMF Rolling Software Update

Feature Summary and Revision History

Summary Data

Table 11: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 12: Revision History

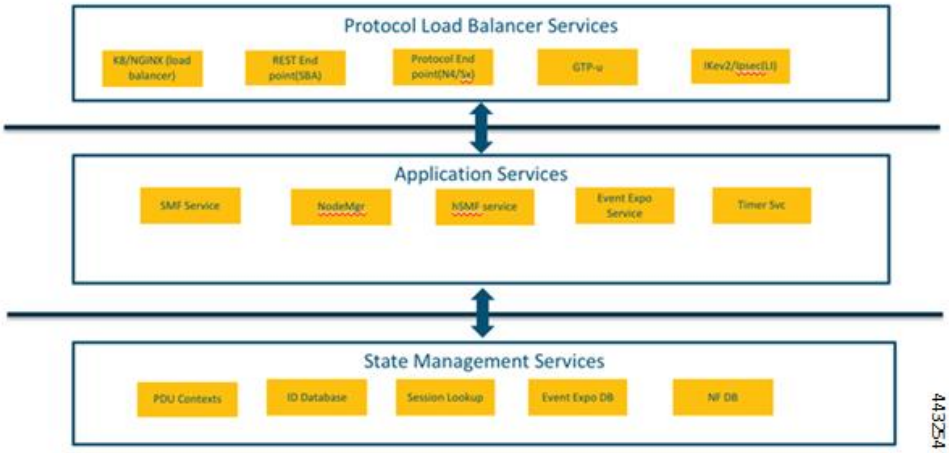
Revision Details	Release
First introduced.	Pre-2020.02.0

Introduction

The Cisco SMF has a three-tier architecture consisting of Protocol, Service, and Session tiers. Each tier includes a set of microservices (pods) for a specific functionality. Within these tiers, there exists a Kubernetes Cluster comprising of Kubernetes (K8s) master, and worker nodes (including Operation and Management nodes).

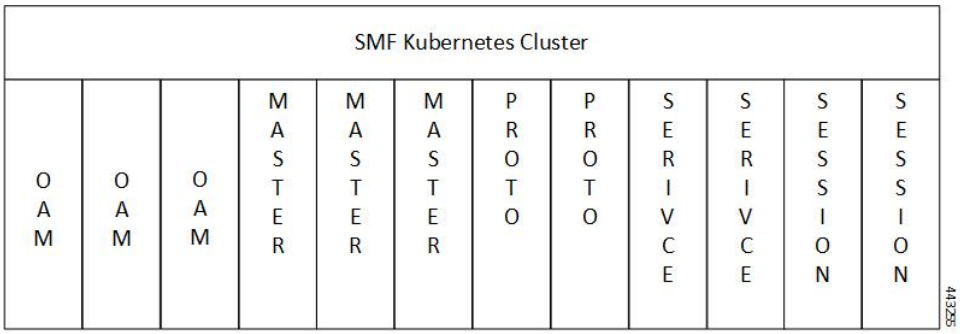
For high availability and fault tolerance, a minimum of two K8s worker nodes are required for each tier. You can have multiple replicas for each worker node. Kubernetes orchestrates the pods using the StatefulSets controller. The pods require a minimum of two replicas for fault tolerance.

Figure 9: SMF Architecture



The following figure depicts an SMF K8s Cluster with 12 nodes – three Master nodes, three Operations and Management (OAM) worker nodes, two Protocol worker nodes, two Service worker nodes, and two Session (data store) worker nodes.

Figure 10: SMF Kubernetes Cluster



Note

- OAM worker nodes: These nodes host the Ops Center pods for configuration management and metrics pods for statistics and Key Performance Indicators (KPIs).
- Protocol worker nodes: These nodes host the SMF protocol-related pods for service-based interfaces (N11, N7, N10, N40, NRF) and UDP-based protocol interfaces (N4, S5/S8).
- Service worker nodes: These nodes host the SMF application-related pods that perform session management processing.
- Session worker nodes: These nodes host the database-related pods that store subscriber session data.

Updating SMF

The following section describes the procedure involved in updating the SMF software.

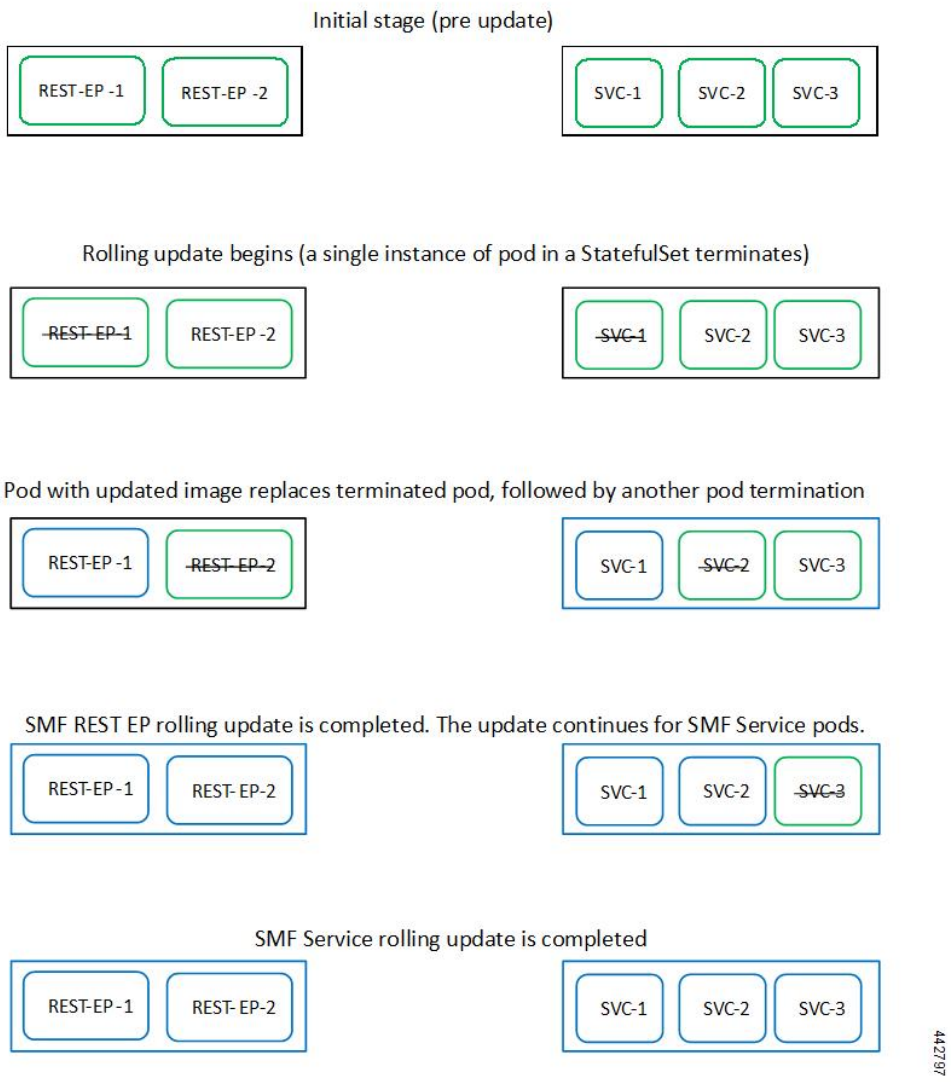
Rolling Software Update Using SMI Cluster Manager

The SMF software update or in-service update procedure utilizes the K8s rolling strategy to update the pod images. In K8s rolling update strategy, the pods of a StatefulSet are updates sequentially to ensure that the ongoing process remains unaffected. Initially, a rolling update on a StatefulSet causes a single pod instance to terminate. A pod with an updated image replaces the terminated pod. This process continues until all the replicas of the StatefulSet are updated. The terminating pods exit gracefully after competing all the ongoing processes. Other in-service pods continue to receive and process the traffic to provide a seamless software update. You can control the software update process through the Ops Center CLI.

Note Each pod needs a minimum of two pods for high availability. In a worst-case scenario, the processing capacity of the pod may briefly reduce to 50% while the software update is in-progress.

The following figure illustrates an SMF rolling update for SMF REST Endpoint pods (two replicas) on Protocol worker nodes along with SMF Service pods (three replicas) on Service worker nodes.

Figure 11: SMF Rolling Update



Prerequisites

The prerequisites for upgrading SMF are:

- All the nodes – including all the pods in the node – are up and running.
- A patch version of the SMF software.

Note Currently, major versions does not support rolling upgrade.

Important Trigger rolling upgrade only when the CPU usage of the nodes is less than 50%.

SMF Health Check

You need to perform an health check to ensure that all the services are running and nodes are in ready state. To perform an health check:

1. Log in to master node and use the following configuration

```
kubectl get pods -n smi
kubectl get nodes
kubectl get pod --all-namespaces -o wide
kubectl get pods -n smf-wsp -o wide
kubectl get pods -n cee-wsp -o wide
kubectl get pods -n smi-vips -o wide
helm list
kubectl get pods -A | wc -l
```

Important Ensure that all the services are running and nodes are in ready state before you proceed further.

Preparing the Upgrade

This section describes the procedure involved creating a backup configuration, logs and deployment files. To backup the files:

1. Log in to the SMI Cluster Manager Node as an **ubuntu** user.
2. Create a new directory for deployment.

   Example:

```
test@smismf-cm01:~$ mkdir -p "temp_$(date +'%m%d%Y_T%H%M')" && cd "$_"
```

3. Move all the working files into the newly created deployment directory.
4. Untar the *smf* deployment file.

   Example:

```
test@smi1smf01-cm01:~/temp_08072019_T1651$ tar -xzvf smf.2020.01.0-1.SPA.tgz
./
./smf_REL_KEY-CCO_RELEASE.cer
./cisco_x509_verify_release.py
./smf.2020.01.0-1.tar
./smf.2020.01.0-1.tar.signature.SPA
./smf.2020.01.0-1.tar.SPA.README
```

5. Verify the downloaded image.

   Example:

```
test@smi1smf01-cm01:~/temp_08072019_T1651$ cat smf.2020.01.0-1.tar.SPA.README
```

Important Follow the procedure mentioned in the *SPA.README* file to verify the build before proceeding to the next step.

Back Up Ops Center Configuration

This section describes the procedure involved in creating a backup of the Ops Center configurations.

To perform a backup of the Ops Center configurations:

1. Log in to SMI Cluster Manager node as an **ubuntu** user.
2. Run the following command to backup the SMI Ops Center configuration to **/home/ubuntu/smiops.backup** file.

   ```
   ssh -p <port_number> admin@$(kubectl get svc -n smi | grep
   '.*netconf.*<port_number>' | awk '{ print $4 }') "show run | nomore"
   > smiops.backup_$(date +'%m%d%Y_T%H%M')
   ```

3. Run the following command to backup the CEE Ops Center configuration to **/home/ubuntu/ceeops.backup** file.

   ```
   ssh admin@<cee-vip> "show run | nomore" > ceeops.backup_$(date
   +'%m%d%Y_T%H%M')
   ```

4. Run the following command to backup the SMF Ops Center configuration to **/home/ubuntu/smfops.backup** file.

   ```
   ssh admin@<smf-vip> "show run | nomore" > smfops.backup_$(date
   +'%m%d%Y_T%H%M')
   ```

Back Up CEE and SMF Ops Center Configuration

This section describes the procedure involved in creating a backup of CEE and Ops Center configuration from the master node. To perform a backup of CEE and Ops Center configuration:

1. Log in to the master node as an **ubuntu** user.
2. Create a directory to backup the configuration files.

   ```
   mkdir backups_$(date +'%m%d%Y_T%H%M') && cd "$_"
   ```

3. Backup the SMF Ops Center configuration and verify the line count of the backup files.

   ```
   ssh -p <port_number> admin@$(kubectl get svc -n $(kubectl get namespaces
    | grep -oP 'smf-(\d+|\w+)') | grep <port_number> | awk '{ print $3
   }') "show run | nomore" > smfops.backup_$(date +'%m%d%Y_T%H%M') && wc
    -l smfops.backup_$(date +'%m%d%Y_T%H%M')
   ```

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p 2024 admin@$(kubectl get svc -n
   $(kubectl get namespaces | grep -oP 'smf-(\d+|\w+)') | grep <port_number> | awk '{ print
    $3 }') "show run | nomore" > smfops.backup_$(date +'%m%d%Y_T%H%M') && wc -l
   smfops.backup_$(date +'%m%d%Y_T%H%M')
   admin@<ipv4address>'s password: smf-OPS-PASSWORD
   334 smfops.backup
   ```

4. Backup the CEE Ops Center configuration and verify the line count of the backup files.

   ssh -p <port_number> admin@$(kubectl get svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep <port_number> | awk '{ print $3 }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M') && wc -l ceeops.backup_$(date +'%m%d%Y_T%H%M')

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p <port_number> admin@$(kubectl get
   svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep <port_number> | awk
   '{ print $3 }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M') && wc -l
   ceeops.backup_$(date +'%m%d%Y_T%H%M')
   admin@<ipv4address>'s password: CEE-OPS-PASSWORD
   233 ceeops.backup
   ```

5. Move the SMI Ops Center backup file (from the SMI Cluster Manager) to the backup directory.

   scp $(grep cm01 /etc/hosts | awk '{ print $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ scp $(grep cm01 /etc/hosts | awk '{ print
   $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .
   ubuntu@<ipv4address>'s password: SMI-CM-PASSWORD
   smiops.backup                                                 100% 9346    22.3MB/s
      00:00
   ```

6. Verify the line count of the backup files.

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ wc -l *
     233 ceeops.backup
     334 smfops.backup
     361 smiops.backup
     928 total
   ```

Staging a New SMF Image

This section describes the procedure involved in staging a new SMF image before initiating the upgrade.

To stage the new SMF image:

1. Download and verify the new SMF image.
2. Log in to the SMI Cluster Manager node as an **ubuntu** user.
3. Copy the images to **Uploads** directory.

   sudo mv <smf_new_image.tar> /data/software/uploads

Note The SMI uses the new image present in the **Uploads** directory to upgrade.

4. Verify whether the image is picked up by the SMI for processing from the **Uploads** directory.

   sleep 30; ls /data/software/uploads

   Example:

```
ubuntu@posmf-cm01:~/temp_08072019_T1651$ sleep 30; ls /data/software/uploads
ubuntu@posmf-cm01:~/temp_08072019_T1651$
```

5. Verify whether the images were successfully picked up and processed.

   Example:

```
auser@unknown:$ sudo du -sh /data/software/packages/*
1.6G /data/software/packages/cee.2019.07
5.3G /data/software/packages/smf.2019.08-04
16K /data/software/packages/sample
```

Note The SMI must unpack the images into the **packages** directory successfully to complete the staging.

Triggering the Rolling Software Upgrade

The SMF utilizes the SMI Cluster Manager to perform a rolling software update. To update SMF using SMI Cluster Manager, use the following configurations:

Important Before you begin, ensure that SMF is up and running with the current version of the software.

1. Log in to SMI Cluster Manager Ops Center.
2. Download the latest TAR ball from the URL.

   `software-packages download` *`url`*

   Example:

```
SMI Cluster Manager# software-packages download <url>
```

3. Verify whether the TAR balls are loaded.

   `software-packages list`

   Example:

```
SMI Cluster Manager# software-packages list
[ smf-2019-08-21 ]
[ sample ]
```

4. Update the product repository URL with the latest version of the product chart.

Note If the repository URL contains multiple versions, the Ops Center automatically selects the latest version.

```
configure
  cluster cluster_name
   ops-centers app_name smf_instance_name
        repository url
         exit
       exit
```

Example:

```
SMI Cluster Manager# config
SMI Cluster Manager(config)# clusters test2
SMI Cluster Manager(config-clusters-test2)# ops-centers smf data
SMI Cluster Manager(config-ops-centers-smf/data)# repository <url>
SMI Cluster Manager(config-ops-centers-smf/data)# exit
SMI Cluster Manager(config-clusters-test2)# exit
```

5. Run the **cluster sync** command to update to the latest version of the product chart.

   clusters *cluster_name* **actions sync run**

   Example:

   ```
   SMI Cluster Manager# clusters test2 actions sync run
   ```

Important

- The cluster synchronization updates the SMF Ops Center, which in turn updates the application pods (through **helm sync** command) one at a time automatically.
- When you trigger rolling upgrade on a specific pod, the SMF avoids routing new calls to that pod.
- The SMF honors in-progress call by waiting for 30 seconds before restarting the pod where rolling upgrade is initiated. Also, the SMF establishes all the in-progress calls completely within 30 seconds during the upgrade period (maximum call-setup time is 10 seconds).

Note

- **software-packages download** *url* – Specifies the software packages to be downloaded through HTTP/HTTPS.
- **software-packages list** – Specifies the list of available software packages.
- **cluster** – Specifies the K8s cluster.
- *cluster_name* – Specifies the name of the cluster.
- **ops-centers** *app_name instance_name* – Specifies the product Ops Center and instance. *app_name* is the application name. *instance_name* is the name of the instance.
- **repository** *url* – Specifies the local registry URL for downloading the charts.
- **actions** – Specifies the actions performed on the cluster.
- **sync run** – Triggers the cluster synchronization.

Monitoring the Upgrade

You can monitor the status of the upgrade through SMI Cluster Manager Ops Center. To monitor the upgrade status, use the following configurations:

```
configure
  clusters cluster_name actions sync run debug true
  clusters cluster_name actions sync logs
  monitor sync-logs cluster_name
```

clusters *cluster_name* **actions sync status**
exit

Example:

```
SMI Cluster Manager# clusters test1 actions sync run
SMI Cluster Manager# clusters test1 actions sync run debug true
SMI Cluster Manager# clusters test1 actions sync logs
SMI Cluster Manager# monitor sync-logs test1
SMI Cluster Manager# clusters test1 actions sync status
```

Important

- **clusters** *cluster_name* – Specifies the information about the nodes to be deployed. *cluster_name* is the name of the cluster.
- **actions** – Specifies the actions performed on the cluster.
- **sync run** – Triggers the cluster synchronization.
- **sync logs** – Shows the current cluster synchronization logs.
- **sync status** – Shows the current status of the cluster synchronization. **debug true** – Enters the debug mode.
- **monitor sync logs** – Monitors the cluster synchronization process.

Important You can view the pod details after the upgrade through CEE Ops Center. For more information on pod details, see Viewing the Pod Details section.

Viewing the Pod Details

You can view the details of the current pods through CEE Ops Center. To view the pod details, use the following command (in CEE Ops Center CLI):

cluster pods *instance_name pod_name* **detail**

Note

- **cluster pods** – Specifies the current pods in the cluster.
- *instance_name* – Specifies the name of the instance.
- *pod_name* – Specifies the name of the pod.
- **detail** – Displays the details of the specified pod.

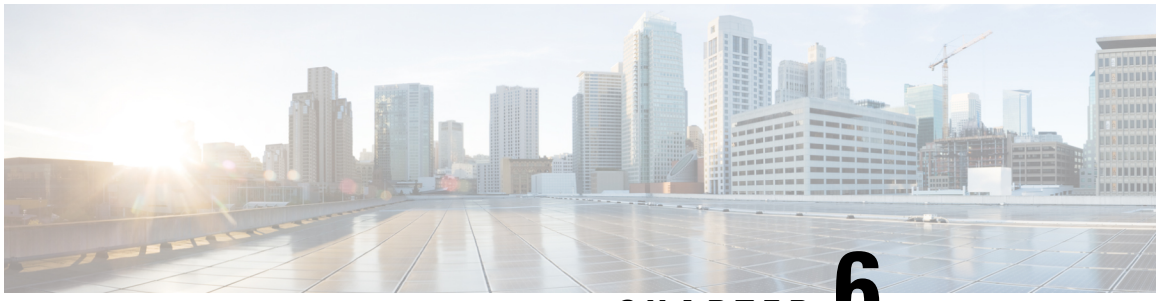
The following example displays the details of the pod named *alertmanager-0* in the *smf-data* instance.

Example:

```
cee# cluster pods smf-data alertmanager-0 detail
details apiVersion: "v1"
kind: "Pod"
metadata:
  annotations:
```

```
    alermanager.io/scrape: "true"
    cni.projectcalico.org/podIP: "<ipv4address/subnet>"
    config-hash: "5532425ef5fd02add051cb759730047390b1bce51da862d13597dbb38dfbde86"
  creationTimestamp: "2020-02-26T06:09:13Z"
  generateName: "alertmanager-"
  labels:
    component: "alertmanager"
    controller-revision-hash: "alertmanager-67cdb95f8b"
    statefulset.kubernetes.io/pod-name: "alertmanager-0"
  name: "alertmanager-0"
  namespace: "smf"
  ownerReferences:
  - apiVersion: "apps/v1"
    kind: "StatefulSet"
    blockOwnerDeletion: true
    controller: true
    name: "alertmanager"
    uid: "82a11da4-585e-11ea-bc06-0050569ca70e"
  resourceVersion: "1654031"
  selfLink: "/api/v1/namespaces/smf/pods/alertmanager-0"
  uid: "82aee5d0-585e-11ea-bc06-0050569ca70e"
spec:
  containers:
  - args:
    - "/alertmanager/alertmanager"
    - "--config.file=/etc/alertmanager/alertmanager.yml"
    - "--storage.path=/alertmanager/data"
    - "--cluster.advertise-address=$(POD_IP):6783"
    env:
    - name: "POD_IP"
      valueFrom:
        fieldRef:
          apiVersion: "v1"
          fieldPath: "status.podIP"
    image: "<path_to_docker_image>"
    imagePullPolicy: "IfNotPresent"
    name: "alertmanager"
    ports:
    - containerPort: 9093
      name: "web"
      protocol: "TCP"
    resources: {}
    terminationMessagePath: "/dev/termination-log"
    terminationMessagePolicy: "File"
    volumeMounts:
    - mountPath: "/etc/alertmanager/"
      name: "alertmanager-config"
    - mountPath: "/alertmanager/data/"
      name: "alertmanager-store"
    - mountPath: "/var/run/secrets/kubernetes.io/serviceaccount"
      name: "default-token-kbjnx"
      readOnly: true
  dnsPolicy: "ClusterFirst"
  enableServiceLinks: true
  hostname: "alertmanager-0"
  nodeName: "for-smi-cdl-1b-worker94d84de255"
  priority: 0
  restartPolicy: "Always"
  schedulerName: "default-scheduler"
  securityContext:
    fsGroup: 0
    runAsUser: 0
  serviceAccount: "default"
  serviceAccountName: "default"
```

```
  subdomain: "alertmanager-service"
  terminationGracePeriodSeconds: 30
  tolerations:
  - effect: "NoExecute"
    key: "node-role.kubernetes.io/oam"
    operator: "Equal"
    value: "true"
  - effect: "NoExecute"
    key: "node.kubernetes.io/not-ready"
    operator: "Exists"
    tolerationSeconds: 300
  - effect: "NoExecute"
    key: "node.kubernetes.io/unreachable"
    operator: "Exists"
    tolerationSeconds: 300
  volumes:
  - configMap:
      defaultMode: 420
      name: "alertmanager"
    name: "alertmanager-config"
  - emptyDir: {}
    name: "alertmanager-store"
  - name: "default-token-kbjnx"
    secret:
      defaultMode: 420
      secretName: "default-token-kbjnx"
status:
  conditions:
  - lastTransitionTime: "2020-02-26T06:09:02Z"
    status: "True"
    type: "Initialized"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "Ready"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "ContainersReady"
  - lastTransitionTime: "2020-02-26T06:09:13Z"
    status: "True"
    type: "PodScheduled"
  containerStatuses:
  - containerID: "docker://821ed1a272d37e3b4c4c9c1ec69b671a3c3fe6eb4b42108edf44709b9c698ccd"

    image: "<path_to_docker_image>"
    imageID: "docker-pullable://<path_to_docker_image>"
    lastState: {}
    name: "alertmanager"
    ready: true
    restartCount: 0
    state:
      running:
        startedAt: "2020-02-26T06:09:05Z"
  hostIP: "<host_ipv4address>"
  phase: "Running"
  podIP: "<pod_ipv4address>"
  qosClass: "BestEffort"
  startTime: "2020-02-26T06:09:02Z"
cee#
```



CHAPTER 6

Pods and Services Reference

Feature Summary and Revision History

Summary Data

Table 13: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 14: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

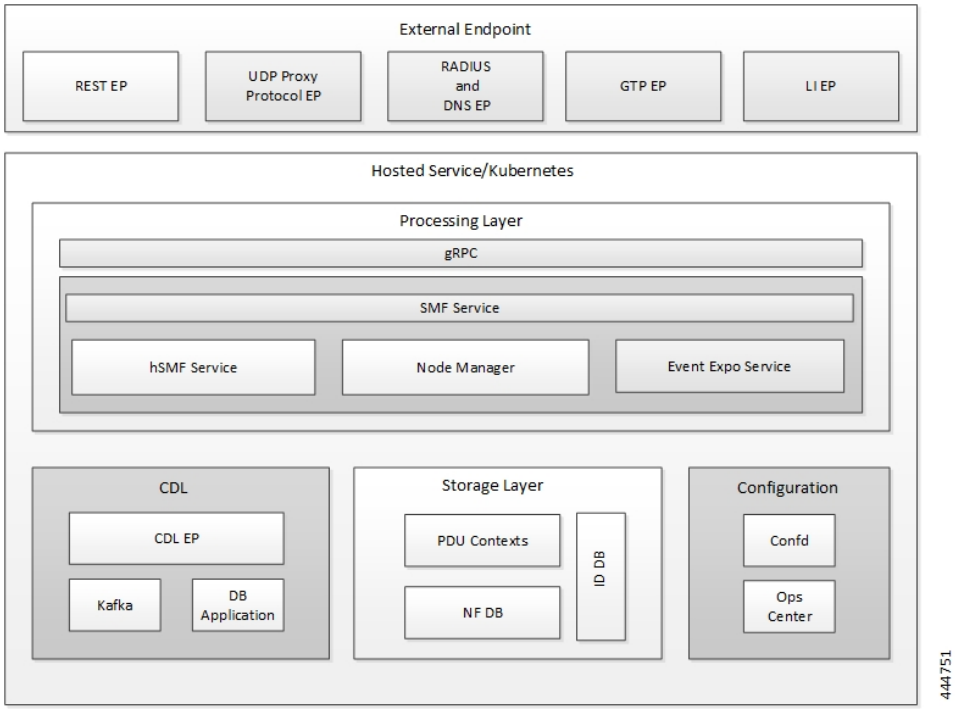
Feature Description

The SMF is built on the Kubernetes cluster strategy, which implies that it has adopted the native concepts of containerization, high availability, scalability, modularity, and ease of deployment. To achieve the benefits offered by Kubernetes, SMF uses the construct that includes the components such as pods and services.

Depending on your deployment environment, the SMF deploys the pods on the virtual machines that you have configured. Pods operate through the services that are responsible for the intrapod communications. If the machine hosting the pods fail or experiences network disruption, the pods are terminated or deleted. However, this situation is transient and SMF spins new pods to replace the invalid pods.

The following workflow provides a high-level visibility into the host machines, and the associated pods and services. It also represents how the pods interact with each other. The representation might defer based on your deployment infrastructure.

Figure 12: Communication Workflow of Pods



Kubernetes deployment includes the kubectl command-line tool to manage the Kubernetes resources in the cluster. You can manage the pods, nodes, and services.

For generic information on the Kubernetes concepts, see the Kubernetes documentation.

For more information on the Kubernetes components in SMF, see the following.

- Pods
- Services

Pods

A pod is a process that runs on your Kubernetes cluster. Pod encapsulates a granular unit known as a container. A pod contains one or multiple containers.

Kubernetes deploys one or multiple pods on a single node which can be a physical or virtual machine. Each pod has a discrete identity with an internal IP address and port space. However, the containers within a pod can share the storage and network resources.

The following tables list the SMF and Common Execution Environment (CEE) pod names and the hosts on which they are deployed depending on the labels that you assign. For information on how to assign the labels, see Associating Pods to the Nodes.

Table 15: SMF Pods

Pod Name	Description	Host Name
api-smf-ops-center	Functions as the *confD* API pod for the SMF Ops Center.	OAM
base-entitlement-smf	Supports Smart Licensing feature.	OAM
cache-pod	Operates as the pod to cache any sort of system information that will be used by other pods as applicable.	Protocol
cdl-ep-session-c1	Provides an interface to the CDL.	Session
cdl-index-session-c1	Preserves the mapping of keys to the session pods.	Session
cdl-slot-session-c1	Operates as the CDL Session pod to store the session data.	Session
documentation	Contains the documentation.	OAM
etcd-smf-etcd-cluster	Hosts the etcd for the SMF application to store information such as pod instances, leader information, NF-UUID, endpoints, and so on.	OAM
grafana-dashboard-app-infra	Contains the default dashboard of app-infra metrics in Grafana.	OAM
grafana-dashboard-cdl	Contains the default dashboard of CDL metrics in Grafana.	OAM
grafana-dashboard-smf	Contains the default dashboard of SMF-service metrics in Grafana.	OAM
gtpc-ep-n0	Operates as GTPC endpoint of SMF.	Protocol
kafka	Hosts the Kafka details for the CDL replication.	Protocol
li-ep-n0	Operates as Lawful Intercept endpoint of SMF.	Protocol

Pod Name	Description	Host Name
oam-pod	Operates as the pod to facilitate Ops Center actions like show commands, configuration commands, monitor protocol monitor subscriber, and so on.	OAM
ops-center-smf-ops-center	Acts as the SMF Ops Center.	OAM
smart-agent-smf-ops-center	Operates as the utility pod for the SMF Ops Center.	OAM
smf-nodemgr-n0	Performs node level interactions such as N4 link establishment, management (heart-beat), and so on. Also, generates unique identifiers such as UE IP address, SEID, CHF-ID, Resource URI, and so on.	Service
smf-protocol-n0	Operates as encoder and decoder of application protocols (PFCP, GTP, RADIUS, and so on) whose underlying transport protocol is UDP.	Protocol
smf-radius-dns-n0	Operates as RADIUS and DNS endpoint of SMF.	Protocol
smf-rest-ep-n0	Operates as REST endpoint of SMF for HTTP2 communication.	Protocol
smf-service-n0	Contains main business logic of SMF.	Service
smf-udp-proxy	Operates as proxy for all UDP messages. Owns UDP client and server functionalities.	Protocol
swift-smf-ops-center	Operates as the utility pod for the SMF Ops Center.	OAM
zookeeper	Assists Kafka for topology management.	OAM

Table 16: CEE Pods

Pod Name	Description	Host Name
alert-logger	Stores the history of active and resolved alerts.	OAM
alertmanager	Duplicates alerts and sends out resolution of alerts when they are resolved in Prometheus.	OAM

Pod Name	Description	Host Name
api-cee-global-ops-center	Functions as the confD API pod for the CEE Ops Center.	OAM
bulk-stats	Assists to retrieve bulkstats saved by Prometheus containers.	OAM
cee-global-product-documentation	Contains the product documentation (API, CLI, and so on).	OAM
core-retriever	Assists in retrieving the core dumps.	All the nodes except ETCD nodes.
documentation	Contains the documentation (metrics and usage).	OAM
grafana-dashboard-metrics	Assists in collating Grafana metrics on the dashboard.	OAM
grafana	Contains the Grafana metrics for CEE.	OAM
kube-state-metrics	Assists in generating metrics about the state of Kubernetes objects: node status, node capacity (CPU and memory), and so on.	OAM
logs-retriever	Assists in retrieving Kernel, Kubelet, and Container level logs through output to JournalD driver.	All the nodes except ETCD nodes.
node-exporter	Exports the node metrics.	All the nodes.
ops-center-cee-global-ops-center	Provides NETCONF and CLI interface to the application.	OAM
path-provisioner	Provisions the local storage volume.	All the nodes except ETCD nodes.
pgpool	*Pgpool* is a middleware that works between *PostgreSQL* servers and a *PostgreSQL* database.	OAM
postgres	Storage of alerts and Grafana dashboards.	OAM
prometheus-hi-res	Stores all metrics and generates alerts by alerting rules.	OAM
prometheus-rules	Contains the default alerting rules and recording rules for Prometheus.	OAM
prometheus-scrapeconfigs-synch	Synchronizes the Prometheus scrape configuration.	OAM
pv-manager	Provisions the local storage volume.	OAM

Pod Name	Description	Host Name
pv-provisioner	Provisions the local storage volume.	OAM
show-tac-manager	Assists in creating and deleting debug package.	OAM
smart-agent-cee-global-ops-center	Operates as the utility pod for the CEE Ops Center.	OAM
snmp-trapper	Sends the SNMP traps based on triggered alerts.	OAM
swift-cee-global-ops-center	Operates as the utility pod for the CEE Ops Center	OAM
thanos-query-hi-res	Implements the Thanos query for Prometheus HA.	OAM
fluentbit	Assists in log forwarding to the external logs collector.	All the nodes except ETCD nodes.

Services

The SMF configuration is composed of several microservices that run on a set of discrete pods. Microservices are deployed during the SMF deployment. SMF uses these services to enable communication between the pods. When interacting with another pod, the service identifies the pod's IP address to initiate the transaction and acts as an endpoint for the pod.

The following table describes the SMF services and the pod on which they run.

Table 17: SMF Services and Pods

Service Name	Pod Name	Description
base-entitlement-smf	base-entitlement-smf	Supports Smart Licensing feature.
datastore-ep-session	cdl-ep-session-c1	Responsible for the CDL session.
datastore-notification-ep	smf-rest-ep	Responsible for sending the notifications from the CDL to the *smf-service* through *smf-rest-ep*.
datastore-tls-ep-session	cdl-ep-session-c1	Responsible for the secure CDL connection.
documentation	documentation	Responsible for the SMF documents.
etcd	etcd-smf-etcd-cluster-0, etcd-smf-etcd-cluster-1, etcd-smf-etcd-cluster-2	Responsible for pod discovery within the namespace.
etcd-smf-etcd-cluster-0	etcd-smf-etcd-cluster-0	Responsible for synchronization of data among the *etcd* cluster.

Service Name	Pod Name	Description
etcd-smf-etcd-cluster-1	etcd-smf-etcd-cluster-1	Responsible for synchronization of data among the *etcd* cluster.
etcd-smf-etcd-cluster-2	etcd-smf-etcd-cluster-2	Responsible for synchronization of data among the *etcd* cluster.
grafana-dashboard-app-infra	grafana-dashboard-app-infra	Responsible for the default dashboard of app-infra metrics in Grafana.
grafana-dashboard-cdl	grafana-dashboard-cdl	Responsible for the default dashboard of CDL metrics in Grafana.
grafana-dashboard-smf	grafana-dashboard-smf	Responsible for the default dashboard of SMF-service metrics in Grafana.
gtpc-ep	gtpc-ep-n0	Responsible for inter-pod communication with GTP-C pod.
helm-api-smf-ops-center	api-smf-ops-center	Manages the Ops Center API.
kafka	kafka	Processes the Kafka messages.
li-ep	li-ep-n0	Responsible for lawful-intercept interactions.
local-ldap-proxy-smf-ops-center	ops-center-smf-ops-center	Responsible for leveraging Ops Center credentials by other applications like Grafana.
oam-pod	oam-pod	Responsible to facilitate Exec commands on the Ops Center.
ops-center-smf-ops-center	ops-center-smf-ops-center	Manages the SMF Ops Center.
ops-center-smf-ops-center-expose-cli	ops-center-smf-ops-center	To access SMF Ops Center with external IP address.
smart-agent-smf-ops-center	smart-agent-smf-ops-center	Responsible for the SMF Ops Center API.
smf-sbi-service	smf-rest-ep	Responsible for routing incoming HTTP2 messages to REST-EP pods.
smf-n10-service	smf-rest-ep	Responsible for routing incoming N10 messages to REST-EP pods.
smf-n11-service	smf-rest-ep	Responsible for routing incoming N11 messages to REST-EP pods.
smf-n40-service	smf-rest-ep	Responsible for routing incoming N40 messages to REST-EP pods.
smf-n7-service	smf-rest-ep	Responsible for routing incoming N7 messages to REST-EP pods.

Service Name	Pod Name	Description
smf-nrf-service	smf-rest-ep	Responsible for routing incoming NRF messages to REST-EP pod.
smf-nodemgr	smf-nodemgr	Responsible for inter-pod communication with *smf-nodemgr* pod.
smf-protocol	smf-protocol	Responsible for inter-pod communication with smf-protocol pod
smf-radius-dns	smf-radius-dns	Responsible for inter-pod communication with smf-radius-dns pod
smf-rest-ep	smf-rest-ep	Responsible for inter-pod communication with smf-rest-ep pod
smf-service	smf-service	Responsible for inter-pod communication with smf-service pod
swift-smf-ops-center	swift	Operates as the utility pod for the SMF Ops Center
zookeeper	zookeeper	Assists Kafka for topology management
zookeeper-service	zookeeper	Assists Kafka for topology management

Associating Pods to the Nodes

This section describes how to associate a pod to the node based on their labels.

After you have configured a cluster, you can associate pods to the nodes through labels. This association enables the pods to get deployed on the appropriate node based on the key-value pair.

Labels are required for the pods to identify the nodes where they must get deployed and to run the services. For example, when you configure the protocol-layer label with the required key-value pair, the pods are deployed on the nodes that match the key-value pair.

1. To associate pods to the nodes through the labels, use the following configuration:

```
configure
  label
    cdl-layer
      key key_value
      value value
    oam-layer
      key key_value
      value value
```

```
protocol-layer
  key key_value
  value value
service-layer
  key key_value
  value value
  end
```

NOTES:

- If you opt not to configure the labels, then SMF assumes the labels with the default key-value pair.
  - **label { cdl-layer { key** *key_value* **| value** *value* **}**: Configures the key value pair for CDL.
  - **oam-layer { key** *key_value* **| value** *value* **}**: Configures the key value pair for OAM layer.
  - **protocol-layer { key** *key_value* **| value** *value* **}**: Configures the key value pair for protocol layer.
  - **service-layer { key** *key_value* **| value** *value* **}**: Configures the key value pair for the service layer.

Viewing the Pod Details and Status

If the service requires additional pods, SMF creates and deploys the pods. You can view the list of pods that are participating in your deployment through the SMF Ops Center.

You can run the kubectl command from the master node to manage the Kubernetes resources.

1. To view the comprehensive pod details, use the following command.

   kubectl get pods -n smf *pod_name* **-o yaml**

The pod details are available in YAML format. The output of this command results in the following information:

- The IP address of the host where the pod is deployed.
- The service and application that is running on the pod.
- The ID and name of the container within the pod.
- The IP address of the pod.
- The current state and phase in which the pod is.
- The start time from which pod is in the current state.

Use the following command to view the summary of the pod details.

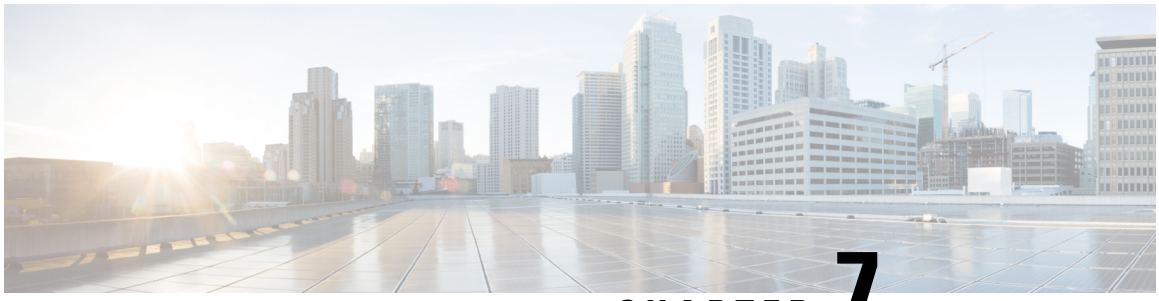
kp get pods -n *smf_namespace* **-o wide**

States

Understanding the pod's state lets you determine the current health and prevent the potential risks. The following table describes the pod's states.

Table 18: Pod States

State	Description
Running	The pod is healthy and deployed on a node. It contains one or more containers.
Pending	The application is in the process of creating the container images for the pod.
Succeeded	Indicates that all the containers in the pod are successfully terminated. These pods cannot be restarted.
Failed	One ore more containers in the pod have failed the termination process. The failure occurred as the container either exited with non zero status or the system terminated the container.
Unknown	The state of the pod could not be determined. Typically, this could be observed because the node where the pod resides was not reachable.



CHAPTER 7

3GPP Specification Compliance for SMF Interfaces

This chapter covers the following topics:

Feature Summary and Revision History

Summary Data

Table 19: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 20: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF currently supports either the December 2018 compliance version of 3GPP specification or the June 2019 compliance version of 3GPP specification for the SMF interfaces such as N1, N2, N4, N7, N10, N11, N40, and Nnrf. The SMF processes the messages from these interfaces as per the compliance profile configured for the corresponding services. For information on the compliance profile configurations, see the Configuring Interfaces, on page 85 section.

Currently, only IE encoding and decoding is supported. The existing features work with the June 2019 specification versions. No additional features in the June 2019 version are supported.

Note The SMF continues to support the older versions of 3GPP specifications and the compliance profile configuration controls the same for the SMF interfaces.

Standards Compliance

The SMF is one of the control plane (CP) NFs of the 5G core network. The SMF uses different interfaces to communicate with the other NFs or nodes. For example, the N4 interface exists between the SMF and User Plane Function (UPF). Each of the SMF interfaces comply to a specific version of the 3GPP specification depending on the compliance version supported.

Use the following table to determine the compliance mapping of each SMF interface and the 3GPP Standards specification versions.

Interface	Relationship	3GPP Specification	Version
N11	Between AMF and SMF	29.518 29.502	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N7	Between PCF and SMF	29.512	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N4	Between UPF and SMF	29.244	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0

Interface	Relationship	3GPP Specification	Version
Nnrf	Between NRF and SMF	29.510	For December 2018 Compliance Support: 15.0.0 For June 2019 Compliance Support: 15.4.0
N10	Between UDM and SMF	29.503	For December 2018 Compliance Support: 15.2.1 For June 2019 Compliance Support: 15.4.0
N40	Between SMF and CHF	32.291	For December 2018 Compliance Support: 15.1.0 For June 2019 Compliance Support: 15.3.0
N1	Between UE and SMF	24.501	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support:15.4.0
N2/NGAP	Between RAN and SMF	38.314	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support:15.4.0

Configuring Interfaces

Use the following commands to configure the SMF interfaces in compliance with the 3GPP specifications.

```
configure
   profile compliance profile_name
      service
        n1 version full version_format spec spec_version uri_version uri_version

        n2 version full version_format spec spec_version uri_version uri_version

         namf-comm version full version_format spec spec_version uri_version
```

```
uri_version
          nchf-convergedcharging version full version_format spec spec_version
 uri_version uri_version
          nnrf-disc version full version_format spec spec_version uri_version
uri_version
          nnrf-nfm version full version_format spec spec_version uri_version
uri_version
          npcf-smpolicycontrol version full version_format spec spec_version
uri_version uri_version
          nsmf-pdusession version full version_format spec spec_version
uri_version uri_version
          nudm-sdm version full version_format spec spec_version uri_version
uri_version
          nudm-uecm version full version_format spec spec_version uri_version
uri_version
          range
          !
          !
```

Important Service selection is based only on the specification version. In future releases, the full API version will be used.

NOTES:

- **version full**: Specifies the API full version for each service in the following format:

  <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]

  The format is specified in 3GPP TS 29.501 V15.2.0, section 4.3.1.1.

- **version spec**: Specifies the 3GPP specification version number. It can be one of the following values:
  - 15.0.0
  - 15.1.0
  - 15.2.0
  - 15.2.1
  - 15.4.0

Important Configuring the 3GPP specification version value depends on the SMF interface. Not all the preceding versions are options for the SMF interfaces. Only a combination of the preceding versions exist as options for the 3GPP version compliance configuration. For details on the compliance version, see the Standards Compliance, on page 84 section.

For example, to support 3GPP June 2019 specification compliance for the N7 (PCF) interface, configure the specification version as 15.4.0.

The default version number depends on the SMF interface. For example, the default version is 15.2.0 for the N7 interface. Similarly, for the N10 interface, the default version is 15.2.1.

- **version uri**: Specifies the API version URI for each service in the following format:

  "v" concatenated with a number

  It can be both v1 and v2, or either v1 or v2.

  For example, for the compliance version 15.4.0 in the NRF configuration for the service type nudm-sdm/nudm-uecm, mandate the configuration of the uri-version in the versions to ‘v2’. For compliance version 15.2.1, this configuration is optional.

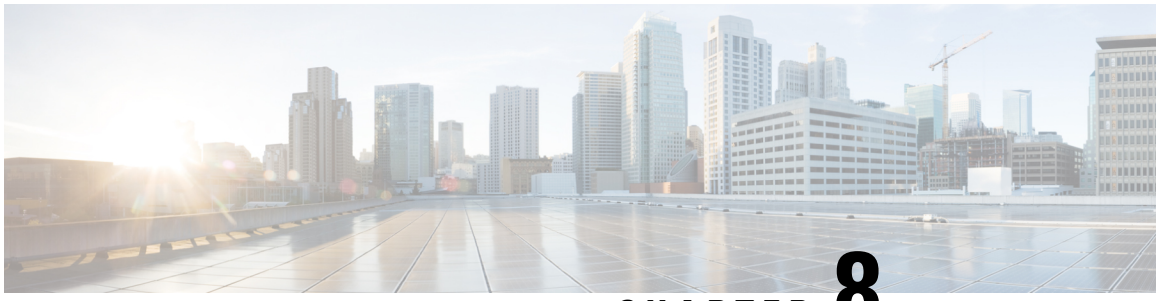
  For example, version v1: (- url: '{apiRoot}/nsmf-pdusession/v1')

- **service**: The service names as specified in 3GPP TS 29.510 V15.2.0, section 6.1.6.3.11.

Sample Configuration

The following is a sample output of the interface configuration:

```
product smf(config-compliance-comp1)# show full
profile compliance comp1
   service nsmf-pdusession
      version uri v1
      version full 1.0.0
      version spec 15.2.0
product smf(config-service-nsmf-pdu)# compliance-profile comp1
product smf(config)# show full-configuration profile smf
profile smf smf1
   service name nsmf-pdu
   ---------------------------------------------------------------------
   compliance-profile comp1
   ---------------------------------------------------------------------
!
!
```



CHAPTER 8

4G to 5G Data Session Handover Support

Feature Summary

Summary Data

Table 21: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 22: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF leverages the 3GPP provision for the UEs that can support both 5G and 4G NAS to connect to E-UTRAN and 5G core network. With this provision, the SMF includes the EPS interworking support and acts as PGW-C+SMF. The SMF uses the S5 or S8 interface to receive the 4G Session Creation Request. The interfaces, such as the Gx, Gy, or Gz, that are used for a 4G session creation are replaced with the corresponding 5G core SBI interfaces, such as the NPCF and NCHF.

After a PDU session is created on PGW-C+SMF through E-UTRAN, MME, and S-GW, the SMF can perform the 4G to 5G data session handover.

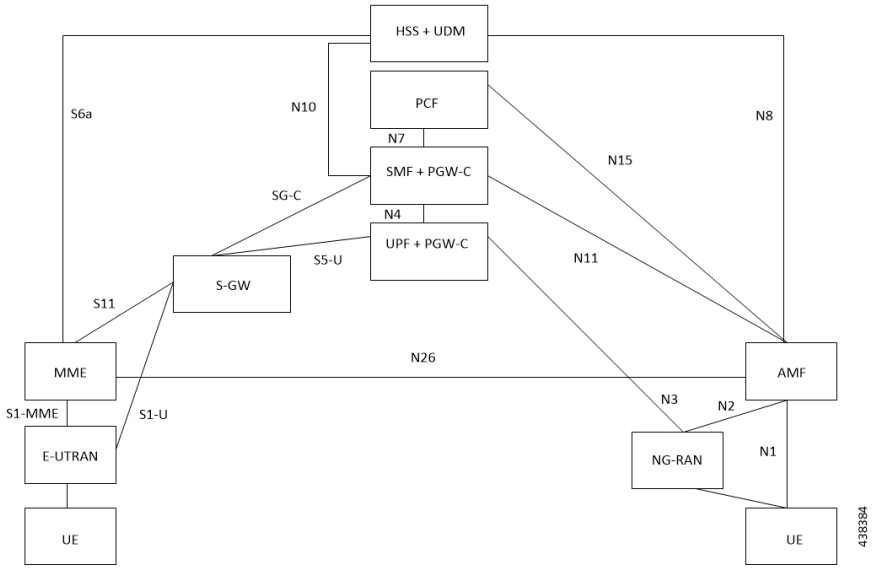
How it Works

To interwork with EPS, a UE that supports both 5GC and EPS NAS works in one of the following modes:

- Single-registration Mode—In this mode, the UE has only one active MM state, which is either the RM state in 5GC or EMM state in EPS. In addition, this state is either in 5GC NAS mode or in EPS NAS mode when connected to 5GC or EPS, respectively.
- Dual-registration Mode—In this mode, the UE handles independent registrations for 5GC and EPS using separate RRC connections. The UE may be registered to 5GC only, EPS only, or to both 5GC and EPS.

Architecture

This section describes the network architecture for the EPS-5G Core interworking.



Call Flows

This section describes the following call flows.

- EPS to 5G Handover with N26 Interface – Preparation Call Flow
- EPS to 5G Handover with N26 Interface – Execution Call Flow
- UE Idle Mode Mobility from EPS to 5GS using N26 Interface – PDU is in Inactive State
- UE Idle Mode Mobility from EPS to 5GS using N26 interface – User Plane Connection Reactivation Request

EPS to 5G Handover with N26 Interface – Preparation Call Flow

This section describes the call flow of the preparation of the EPS to 5G Handover with the N26 interface.

Figure 13: Preparation of the EPS to 5G Hand-over with the N26 Interface Call Flow

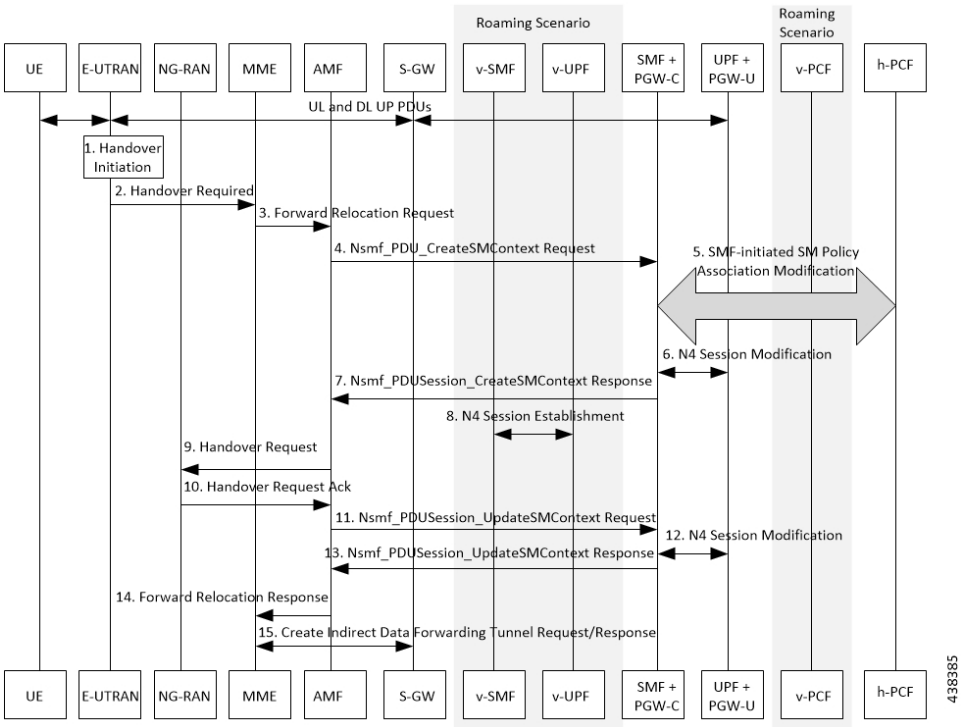


Table 23: Preparation of the EPS to 5G Hand-over with the N26 Interface Call Flow Description

Step	Description
1	Call handover initiation starts from UE and E-UTRAN toward each other, proceeds from E-UTRAN to the S-GW, and then for roaming calls, call handover initiation proceeds from S-GW to the UPF+P-GW-U.
2	The E-UTRAN sends the Handover Call Request to the MME.
3	The MME forwards the Relocation Request to the AMF.

Step	Description
4	The AMF invokes the Nsmf_PDUSession_CreateSMContext service operation on SMF. The PGW-C+SMF address identifies this service operation. The service operations can be UE EPS PDN Connection, AMF ID, or Direct Forwarding Flag. The AMF then indicates the handover preparation to avoid switching the UP path. The SMF searches for the corresponding PDU session that is based on EPS Bearer Contexts. The AMF includes Direct Forwarding Flag to inform the SMF of the applicability of indirect data forwarding.
5	If you have deployed the dynamic PCC, the SMF+ PGW-C initiates the SMF-initiated SM Policy Modification toward the PCF. **Important** Cisco SMF does not support this step in this release.
6	The PGW-C+SMF sends the N4 Session Modification to PGW-U+UPF to establish the CN tunnel for a PDU Session. The PGW-U+UPF receives the uplink packets from NG-RAN. This step involves creating uplink PDRs and FARs for the 5G session along with the QFIs that are mapped from the existing 4G bearers.
7	The PGW-C+SMF sends a Nsmf_PDUSession_CreateSMContext Response to the AMF. This response includes PDU Session ID, S-NSSAI, and N2 SM Information. The N2 SM Information includes PDU Session ID, S-NSSAI, QFIs, QoS Profiles, EPS Bearer Setup List, mapping between EBIs and QFIs, CN Tunnel information, and cause code details. The SMF includes mapping between EBIs and QFIs as the N2 SM Information container. If the P-GW-C+SMF determines that session continuity from EPS to 5GS is not supported for the PDU session, then the P-GW-C+SMF does not provide the Session Manager information for the corresponding PDU session. However, the P-GW-C+SMF includes the cause code details for rejecting the PDU session transfer in the N2 SM information.
8	The V-SMF and V-UPF establish an N4 session with each other.
9	The AMF sends the Handover Request to NG-RAN.
10	The NG-RAN sends the Handoff Request Acknowledgment for the received Handover Request to the AMF.
11	The AMF sends a Nsmf_PDUSession_UpdateSMContext Request, T-RAN SM N3 forwarding information list message to the SMF for updating the N3 tunnel information. The Nsmf_PDUSession_UpdateSMContext request includes a PDU Session ID, S-NSSAI, and N2 SM Information. The tunnel information exists in the NGAP IE DL Forwarding UP TNL Information of the Handoff Request Acknowledgment that is received from NG-RAN.
12	The SMF+PGW-C performs the N4 session modification toward UPF+PGW-U to create the indirect tunnel to forward the DL data from eNodeB to NG-RAN. This step includes creating UL PDRs for the redirected DL data and associating FARs with them to forward the FARs to NG-RAN. The mapping of these PDRs and FARs is based on QFI and the corresponding bearer ID.

Step	Description
13	The PGW-C+SMF sends the Nsmf_PDUSession_UpdateSMContext Response to the AMF. This response includes PDU Session ID, EPS Bearer Setup List, and CN tunnel information for data forwarding. At this point, the indirect tunnels are established for DL data forwarding.
14	The AMF sends the Forward Relocation Response to the MME.
15	The MME sends the creation request for the indirect data forwarding tunnel to the S-GW. The S-GW sends the response for the indirect data forwarding tunnel to the MME.

EPS to 5G Handover with N26 Interface – Execution Call Flow

This section describes the call flow of the execution of the EPS to 5G Handover with the N26 interface.

Figure 14: Execution of the EPS to 5G Hand-over with the N26 Interface Call Flow

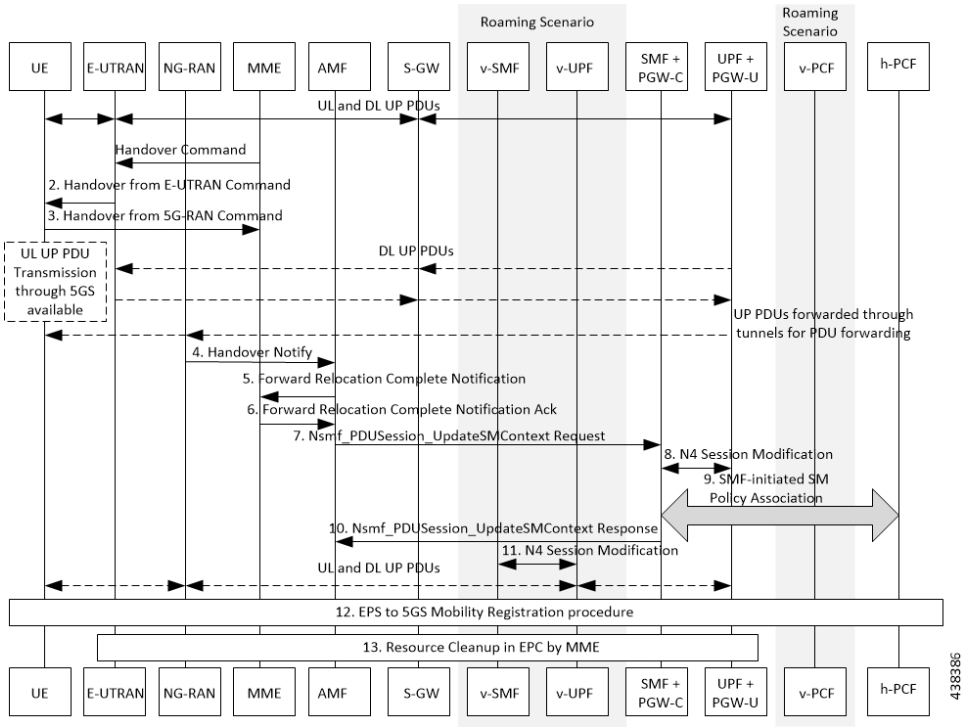


Table 24: Execution of the EPS to 5G Hand-over with the N26 Interface Call Flow Description

Step	Description
1	Call handover initiation starts from the UE and E-UTRAN toward each other, proceeds from E-UTRAN to S-GW, and then for roaming calls, call handover initiation proceeds from S-GW to the UPF+P-GW-U. The MME sends the handover command to E-UTRAN.
2	The E-UTRAN sends the handover command to the UE.

Step	Description
3	The UE sends the confirmation message to NG-RAN for the received handover to 5G-RAN.
4	The NG-RAN sends the Handover Notification message to the AMF.
5	The AMF sends the Forward Relocation Complete Notification to the MME.
6	The MME sends the Acknowledgment Response for the received Forward Relocation Complete Notification.
7	The AMF sends Nsmf_PDUSession_UpdateSMContext Request to SMF +PGW-C. This request includes Handover Complete Indication for PDU Session ID details. For indirect forwarding, a timer in SMF+PGW-C starts to check when resources in UPF are to be released.
8	The SMF performs N4 Modification Request with UPF+PGW-U to update the DL tunnel information for the FARs that are associated with DL PDRs of the 5G session. The DL data path is activated. At this point, the indirect tunnel also exists.
9	The SMF informs PCF of the RAT type change. **Important** Cisco SMF does not support this step in this release.
10	The SMF sends Nsmf_PDUSession_UpdateSMContext Response, with PDU Session ID, to SMF. The SMF confirms the reception of Handover Complete.
11	After the timer that started in Step 7 expires, the SMF sends N4 Modification Request to UPF. This request is to remove the PDRs and FARs that are associated with the indirect data tunnel.
12	The UE starts the EPS to 5GS mobility registration procedure and sends it to H-PCF.
13	The E-UTRAN performs the resource cleanup in EPC by MME.

UE Idle Mode Mobility from EPS to 5GS using N26 Interface

SMF and PGW-C supports EPS to 5GS Idle Mode Mobility procedure. For Idle Mode Mobility from EPS to 5GS, UE performs Mobility Registration Update Procedure with AMF. AMF and SMF retrieves MM and SM context from EPC and moves UE context from EPS to 5GS by interacting with other core NFs.

This feature enables the EPS and 5GS core network elements to support the following use cases during EPS to 5GS Idle Mode Mobility procedure.

- UE idle mode mobility from EPS to 5GS using N26 interface - PDU session in inactive state
- UE idle mode mobility from EPS to 5GS using N26 interface - User Plane connection reactivation request

PDU Session is in Inactive State

The following call flows captures information on UE Idle Mode Mobility from EPS to 5GS using N26 Interface when PDU session is in inactive state.

Figure 15: PDU Session in Inactive State

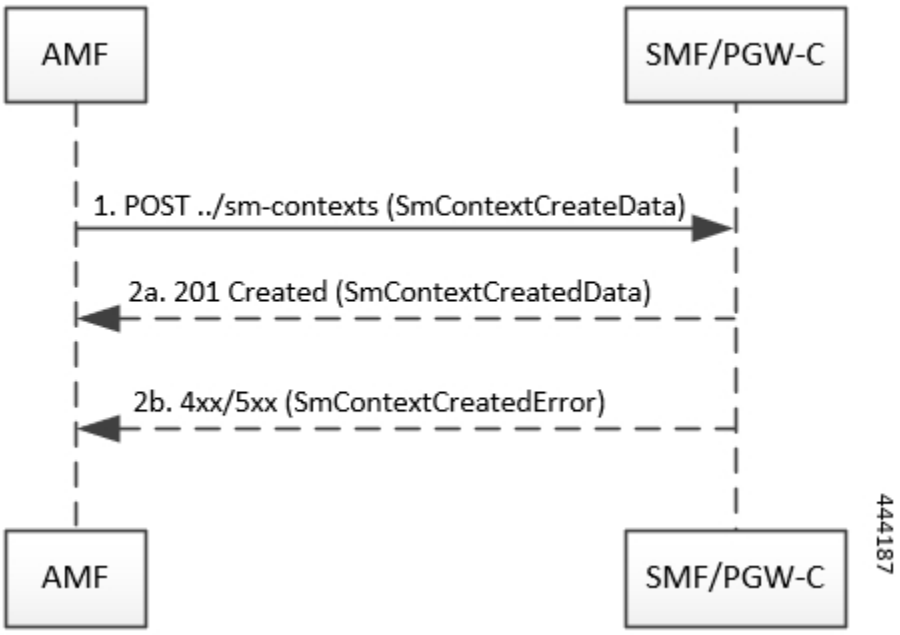


Table 25: PDU Session in Inactive State

Step	Description
1	AMF sends a POST request towards SMF/PGW-C of each UE EPS PDN connection with following information: • UE EPS PDN connection, including the EPS bearer contexts, received from the MME, representing the individual SM context to be created. • EPS Bearer Context Status attribute, indicating the status of all the EPS bearer contexts in the UE, if corresponding information is received in the Registration Request from the UE.
2	Upon receipt of such a request, if: • a corresponding PDU session is found based on the EPS bearer contexts. • the default EPS bearer context of the corresponding PDU session is not reported as inactive by the UE in the EPS Bearer Connection Status attribute, if received; and • it is possible to proceed with moving the PDN connection to 5GS.

Step	Description
2a	SMF returns a 201 Created response including the following information: • PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection. • Allocated EBI List, containing the EBI(s) allocated to the PDU session. The Location header present in the POST response contains the URI of the created SM context resource. AMF stores the association of the PDU Session ID and the SMF ID, and allocated EBI(s) associated to the PDU Session ID. If the EPS Bearer Context Status attribute is received in the request, the SMF checks whether some EPS bearer(s) of the corresponding PDU session have been deleted by the UE but not notified to the EPS. If so, SMF releases these EPS bearers, corresponding QoS rules and QoS flow level parameters locally.
2b	SMF returns 4xx/5xx failure response if: • SMF determines that seamless session continuity from EPS to 5GS is not supported for the PDU session. SMF sets the cause attribute in the Problem Details structure to `NO_EPS_5GS_CONTINUITY`. • The default EPS Bearer Context of the PDU session is reported as inactive by the UE in the EPS Bearer Context Status attribute. SMF sets the cause attribute in the Problem Details structure to `DEFAULT_EPS_BEARER_INACTIVE`.

User Plane Connection Reactivation Request

The following call flows captures information on UE idle mode mobility from EPS to 5GS with UP (User Plane) connection reactivation using N26 interface.

Figure 16: User Plane Connection Reactivation Request

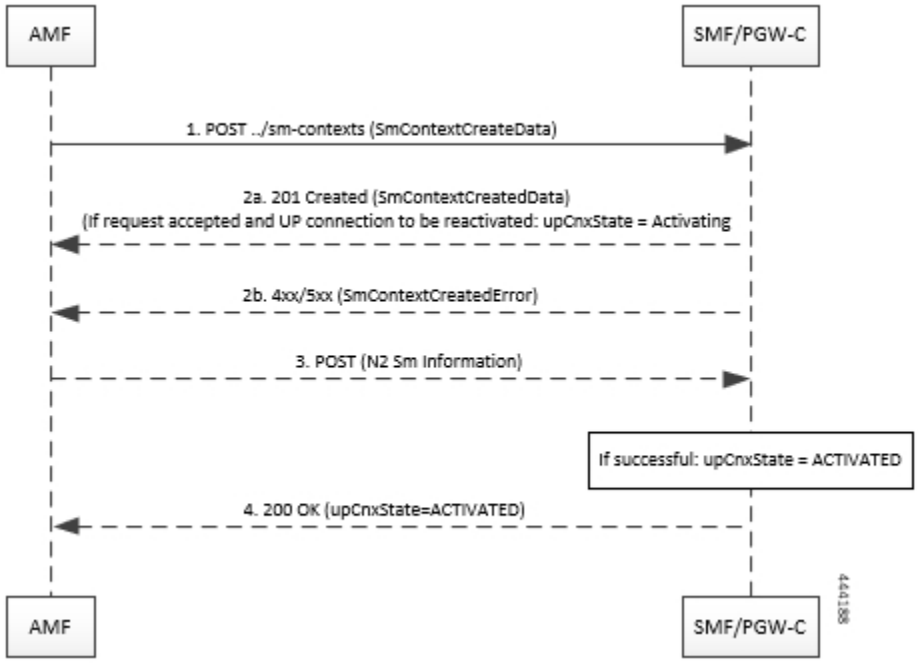


Table 26: User Plane Connection Reactivation Request

Step	Description
1	AMF sends a POST request towards SMF/PGW-C of each UE EPS PDN connection with following information: • UE EPS PDN connection, including the EPS bearer contexts, received from the MME, representing the individual SM context to be created. • the PDU Sessions Activate List attribute, including the PDU Session ID of all the PDU session(s) to be re-activated. • EPS Bearer Context Status attribute, indicating the status of all the EPS bearer contexts in the UE, if corresponding information is received in the Registration Request from the UE.
2	Upon receipt of such a request, if: • a corresponding PDU session is found based on the EPS bearer contexts. • the default EPS bearer context of the corresponding PDU session is not reported as inactive by the UE in the EPS Bearer Context attribute, if received; and • it is possible to proceed with moving the PDN connection to 5GS.

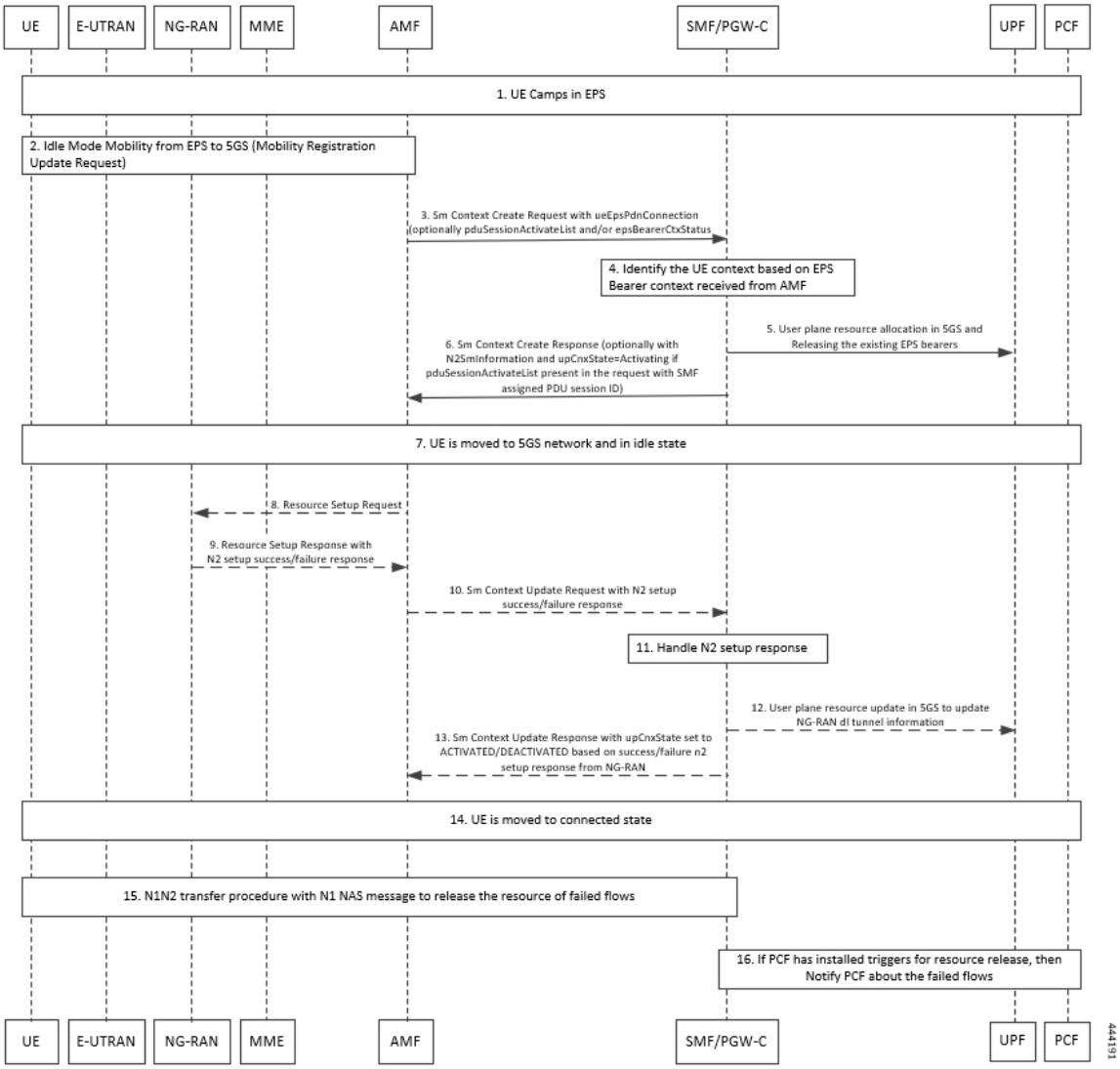
Step	Description
2a	SMF returns a 201 Created response including the following information: • PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection. • Allocated EBI List, containing the EBI(s) allocated to the PDU session. and, if the PDU session that is derived by the SMF based on the EPS bearer contexts was requested to be re-activated, i.e. if the PDU Session ID was present in the PDU Sessions Activate List, • the User Plane Connection State attribute is set to ACTIVATING. • N2 SM information to request the 5G-AN to assign resources to the PDU session (PDU Session Resource Setup Request Transfer), including the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session (i.e. UPF's GTP-U F-TEID for uplink traffic). The Location header present in the POST response contains the URI of the created SM context resource. AMF stores the association of the PDU Session ID and the SMF ID, and allocated EBI(s) associated to the PDU Session ID. If the EPS Bearer Context Status attribute is received in the request, the SMF checks whether some EPS bearer(s) of the corresponding PDU session have been deleted by the UE but not notified to the EPS. If so, SMF releases these EPS bearers, corresponding QoS rules and QoS flow level parameters locally.
2b	SMF returns 4xx/5xx failure response if: • SMF determines that seamless session continuity from EPS to 5GS is not supported for the PDU session. SMF sets the cause attribute in the Problem Details structure to `NO_EPS_5GS_CONTINUITY`. • The default EPS Bearer Context of the PDU session is reported as inactive by the UE in the EPS Bearer Context Status attribute. SMF sets the cause attribute in the Problem Details structure to `DEFAULT_EPS_BEARER_INACTIVE`.

Step	Description
3	If the SMF returns a 200 OK response, the AMF subsequently updates the SM context in the SMF by sending POST request with the following information: • N2 SM information received from the 5G-AN (PDU Session Resource Setup Response Transfer IE), including the transport layer address and tunnel endpoint of one or two downlink termination point(s). It also includes the associated list of QoS flows for this PDU session (i.e. 5G-AN's GTP-U F-TEID(s) for downlink traffic), if the 5G-AN succeeded in establishing resources for the PDU sessions; or • N2 SM information received from the 5G-AN (PDU Session Resource Setup Unsuccessful Transfer IE), including the Cause of the failure, if resources failed to be established for the PDU session. Upon receipt of this request, the SMF: • Updates the UPF with the 5G-AN's F-TEID(s) and sets the User Plane Connection State attribute to ACTIVATED, if the 5G-AN succeeds in establishing resources for the PDU sessions; or • Considers that the activation of the User Plane connection has failed and sets the User Plane Connection State attribute to DEACTIVATED.
4	SMF returns a 200 OK response including the User Plane Connection State attribute representing the final state of the user plane connection.

Message Flows

The following message flow describes the different scenarios of idle mode mobility procedure across 5GS network elements and subscriber.

Figure 17: Message Flow across 5GS NEs and Subscriber



Standards Compliance

The SMF Support for 4G to 5G Data Session Handover feature complies with the following standard:

- 3GPP TS 23.502 V15.2.0 (2018-09)

Limitations

In this release, this feature has the following limitations:

- SMF supports N26 4G to 5G handoff with single UPF, which implies that UPF selection and UPF modification are not supported.
- SMF does not support PCF trigger.

- SMF does not support charging and PCF integration.
- SMF does not support the roaming scenario.

Emergency SoS Support

Feature Description

The Emergency SoS Support feature enables the co-located cloud-native SMF and PGW-C to support SoS emergency over LTE for subscribers camped on the 4G network and SoS emergency service fallback to LTE for subscribers camped on the 5G network.

The Emergency SoS Support feature supports the following functionalities:

- Provides a new configuration to skip UDM interaction.
- Enables an emergency PDN connection creation in 4G (LTE) for PGW-C.
- Supports emergency service fallback to LTE requirement for SMF serving subscriber in NR.
- Supports interworking with an existing charging interface failure handling to ‘continue’ emergency call creation upon failure.
- Supports interworking with an existing secondary authentication using radius to skip radius authentication for emergency calls when not configured.
- Provides inter-RAT handover support (4G to 5G and 5G to 4G) for EPS interworking capable subscribers.

How it Works

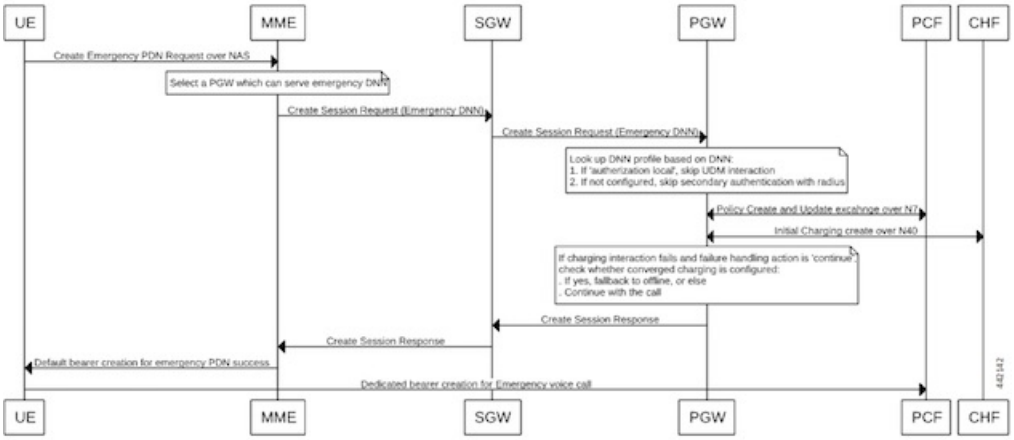
This section provides a brief of how the Emergency SoS Support feature works.

Call Flows

This section includes the following call flows.

Emergency Session Creation in LTE Call Flow

Figure 18: Emergency Session Creation in LTE

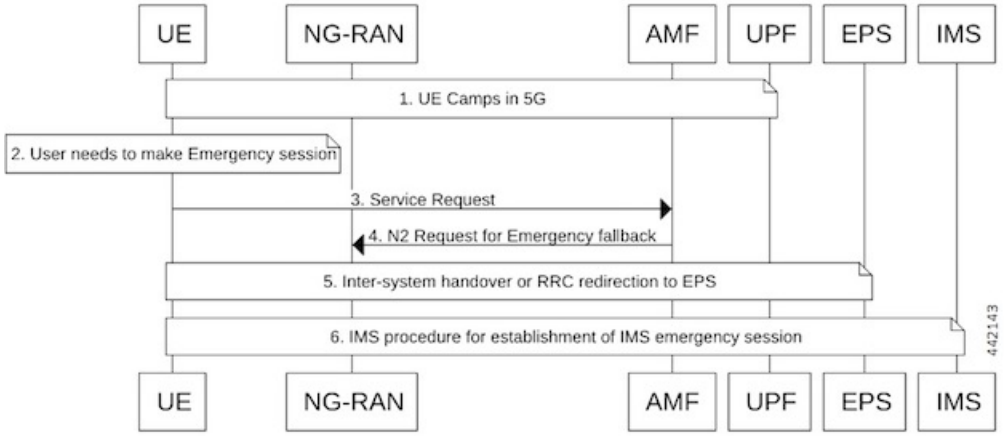


Step	Description
1	When an emergency service is required and an emergency PDU session is not already established, the UE initiates the UE-requested PDU session establishment procedure with a request type indicating, "Emergency Request" in LTE.
2	The MME selects an APN or DNN for the emergency PDN creation, and sends a ‘Create Session Request’ to the P-GW via the S-GW.
3	The DNN profile lookup at P-GW is based on the subscriber policy or DNN policy. These policies are associated in the SMF profile. The subscriber policy has higher precedence over DNN policy when both the configurations are present.
4	The DNN policy can have the DNN profile configuration for each of the UE-requested APN or DNN received in the “Create Session Request” from the MME or S-GW.
5	When a new configuration ‘authorization local’ under the selected DNN profile is present: • P-GW skips the UDM interaction for fetch subscription and uses the values received in the ‘Create Session Request’ message from the MME. • P-GW skips the UDM interaction to ‘Subscribe-for-Notification’ from the UDM.
6	When the ‘Secondary Authentication Radius’ under the selected DNN profile is not present, the PGW-C rejects the RADIUS-based secondary authentication.
7	When ‘failure handling’ for charging interaction is set as ‘action continue’: • P-GW continues the call if converged charging is not configured. • P-GW falls back to offline charging and continues the call.

Step	Description
8	During handover from 4G to 5G using N26, if the emergency PDN gets handed over, the SMF checks the DNN profile and if 'authentication local' is present, it skips the UDM interactions for registration and deregistration.

Emergency Services Fallback to LTE Call Flow

Figure 19: Emergency Services Fallback to LTE



Step	Description
1	UE camps on E-UTRA or NR cell in the 5GS (in either CM_IDLE or CM_CONNECTED state).
2	UE has a pending IMS emergency session request (example, voice) from the upper layers.
3	If the AMF has indicated support for emergency services using fallback via the "Registration Accept" message for the current RAT, the UE sends a "Service Request" message indicating that it requires an emergency services fallback.
4	The 5GC executes an NG-AP procedure in which it indicates to the NG-RAN that this is a fallback for emergency services. This procedure triggers the "Emergency Services Fallback" request. Currently the Cisco SMF and PGW-C supports Emergency Services in the EPC core Network (LTE). The AMF includes the EPC as a target CN to trigger inter-RAT fallback. When the AMF initiates the redirection for UEs that are successfully authenticated, AMF includes the security context in the request to trigger fallback towards the NG-RAN.
5	The NG-RAN initiates the handover or redirection to the E-UTRAN connected to the EPS (N26 interface based handover or redirection procedure). The NG-RAN uses the security context that the AMF to secure the redirection procedure. If the redirection procedure is used, the target CN is also conveyed to the UE to enable it to perform the S1 mode NAS procedures. The UE uses the emergency indication in the RRC message and E-UTRAN provides the emergency indication to the MME during the "Tracking Area Update".

Step	Description
6	After handover to the target cell, the UE establishes a PDU session or PDN connection for IMS emergency services and performs the IMS procedures for establishment of an IMS emergency session (example, voice).

Configuring Emergency SoS Support

This section describes how to configure the Emergency SoS Support feature.

Configuring the Emergency SoS Support involves the following steps:

1. Local authorization configuration under DNN profile
2. Secondary authentication configuration under DNN profile
3. Charging failure handling configuration under Charging profile

Configuring Local Authorization

To configure the local authorization under the DNN profile, use the following commands:

```
configure
  profile dnn pool_name
    [ no ] authorization local
    end
```

NOTES:

no: Disables the local authorization under the DNN profile.

Configuring Secondary Authentication

To configure secondary authentication under the DNN profile, use the following commands:

```
configure
  profile dnn pool_name
    [ no ] secondary authentication radius
    end
```

NOTES:

- **no**: Disables the secondary authentication under the DNN profile.
- **radius**: Specifies RADIUS for secondary authentication.

Configuring Charging Failure Handling

To configure failure handling action for both converged charging and offline charging failure cases under the charging profile, use the following commands:

```
configure
  profile network-element chf charging_profile_name
    nf-client-profile offline_charging_profile_name
    failure-handling-profile failure_handling_profile_name
```

```
exit
exit
```

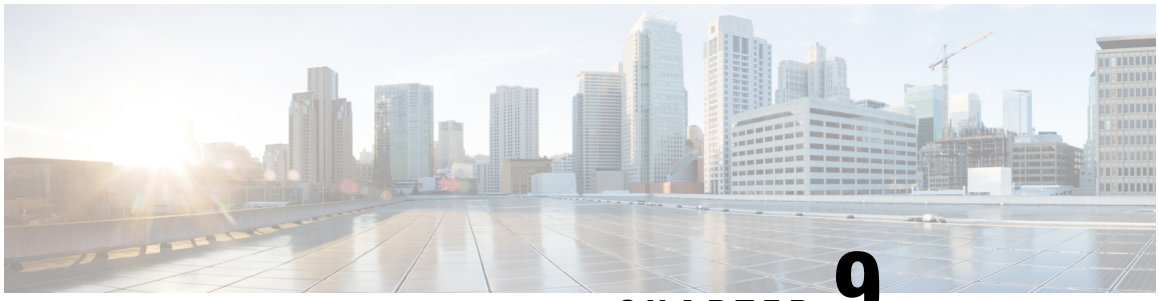
NOTES:

- **profile network-element chf** *charging_profile_name*: Specifies the charging function (CHF) as the network element profile. *charging_profile_name* must an alphanumeric string representing the corresponding network element profile name.
- **nf-client-profile** *offline_charging_profile_name*: Specifies the local NF client profile.*offline_charging_profile_name* must an alphanumeric string representing the corresponding NF client profile name.
- **failure-handling-profile** *failure_handling_profile_name*: Specifies the NRF failure handling network profile for the configured NF type. *failure_handling_profile-name* must an alphanumeric string representing the corresponding NRF failure handling network profile name.

Sample Configuration

The following is a sample configuration of the failure handling action for converged charging:

```
profile nf-client-failure nf-type chf
profile failure-handling [failure_handling_profile_name]
service name type nchf-convergedcharging
message type ChfConvergedchargingCreate
status-code httpv2 0
action continue
exit
```



CHAPTER 9

5GSM Cause Handling

Feature Summary and Revision History

Feature Summary

Feature Summary

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 27: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

The SMF supports 5GSM cause handling for the UE and Network initiated procedures.

The procedures include:

- PDU-Session-Establishment
- PDU-Session-Modification
- PDU-Session-Release

PDU Session Establishment Reject

If the connectivity with the requested DN is rejected by the network, SMF sets the 5GSM cause IE of the PDU Session Establishment Reject message to indicate the reason for rejecting the PDU Session Establishment procedure.

The SMF supports the following causes in the PDU Session Establishment Reject message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #26 – insufficient resources	The SMF includes this cause when it receives N2SmInfoType with "PDU_RES_SETUP_FAIL" along with any of the following N2 causes: • RadioNetwork/Radio_resources_not_available • RadioNetwork/Failure_in_the_radio_interface_procedure • Misc/Not_enough_user_plane_processing_resources
Cause #27 – missing or unknown DNN	The SMF includes this cause when DNN is not present in SmContextCreateData even though it is required and not configured in SMF.
Cause #28 – unknown PDU session type	The SMF includes this cause when the PDU Session Establishment Request message includes a PDU session type that is not supported by SMF.
Cause #29 – user authentication or authorization failed	The SMF includes this cause when DN authentication of the UE was performed and completed unsuccessfully (Radius Authentication Timeout).
Cause #32 – service option not supported	The SMF supports this cause when the validation of received S-NSSAI fails against the allowed list of S-NSSAI.
Cause #33 – requested service option not subscribed	The SMF supports this cause when the UE requests a service option for which it has no subscription.
Cause #38 – network failure	The SMF supports this cause when the requested service was rejected due to an error in the network. This includes any internal failures or no response from any external NF during the PDN-setup procedure.
Cause #54 – PDU session does not exist	The SMF supports this cause when it does not have any information about the PDU session which is requested by the UE to transfer between 3GPP access and non-3GPP access or from the EPS to the 5GS.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #70 – missing or unknown DNN in a slice	The SMF supports this cause when the slice configuration is present but the requested DNN is not configured under the slice in the SMF.
Protocol errors	
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content. **Important** For mandatory parameters (PDU Session Identity and Procedure Transaction Identity) with non-semantical error also, the SMF sends this cause.

PDU Session Modification Reject

If the SMF does not accept the request to modify the PDU session, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification procedure.

The SMF supports the following causes in the PDU Session Modification Reject message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF sends this cause when SMF does not have the session.
Protocol errors	
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content. **Important** For mandatory parameters (PDU Session Identity and Procedure Transaction Identity) with non-semantical error also, the SMF sends this cause.

PDU Session Release Reject

If the SMF does not accept the request to release the PDU session, SMF sets the 5GSM Cause IE of the PDU Session Release Reject message to indicate the reason for rejecting the PDU session release.

The SMF supports the following causes in the PDU Session Release Reject message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF supports this cause when SMF does not have the session.
Protocol errors	

Reject Cause / 5GSM Cause	SMF Behavior
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content. **Important** For mandatory parameters (PDU Session Identity and Procedure Transaction Identity) with non-semantical error also, the SMF sends this cause.

PDU Session Release Request

To initiate the UE-requested PDU Session Release procedure, UE sends the PDU Session Release Request message with the 5GSM Cause IE to indicate the reason for releasing the PDU session.

The SMF supports the following causes in the PDU Session Release Request message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #36 – regular deactivation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #41 – Semantic error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #42 – Syntactical error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #44 – Semantic errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #45 – Syntactical errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.

PDU Session Modification Command Reject

If the UE rejects the PDU-Session-Modification-Command, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification.

The SMF supports the following 5GSM causes.

5GSM Cause	SMF Behavior
Cause #26 – insufficient resources	The SMF retains the statistics based on the cause.
Cause #43 – Invalid PDU session identity	The SMF retains the statistics based on the cause and releases the existing PDU session.
Cause #44 – Semantic error in packet filter(s)	The SMF retains the statistics based on the cause.
Cause #45 – Syntactical error in packet filter(s)	The SMF retains the statistics based on the cause.

5GSM Cause	SMF Behavior
Cause #83 – Semantic error in the QoS operation	The SMF retains the statistics based on the cause.
Cause #85 – Syntactical error in the QoS operation	The SMF retains the statistics based on the cause.

How it Works

The SMF supports 5GSM cause handling for the PDU-Session-Establishment, PDU-Session-Modification and PDU-Session-Release procedures. An appropriate SM cause will be sent over the N1 message to the UE.

Standards Compliance

The 5GSM Cause Handling feature complies with the 3GPP TS 24.501, version 15.4.0, Release 15 (Non-Access-Stratum (NAS) protocol for 5G System (5GS)).

Configuring the 5GSM Cause Handling Feature

5GSM Cause Handling OAM Support

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

Statistics

The 5GSM Cause Handling feature supports the following statistics to track the number of failures based on the 5GSM cause.

SMF N1 Message Stats

PDU-Session-Establishment-Reject:

- NETWORK_FAILURE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "NETWORK_FAILURE".
- UNKNOWN_PDU_SESSION_TYPE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "UNKNOWN_PDU_SESSION_TYPE".
- USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED".
- REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED".
- MISSING_OR_UNKNOWN_DNN: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING_OR_UNKNOWN_DNN".
- SERVICE_OPTION_NOT_SUPPORTED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "SERVICE_OPTION_NOT_SUPPORTED".

- INSUFFICIENT_RESOURCES: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "INSUFFICIENT_RESOURCES".
- MISSING_OR_UNKNOWN_DNN_IN_A_SLICE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING_OR_UNKNOWN_DNN_IN_A_SLICE".
- PDU_SESSION_DOES_NOT_EXIST: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "PDU_SESSION_DOES_NOT_EXIST".

PDU-Session-Modification-Reject:

- INVALID_PDU_SESSION_IDENTITY: The number of PDU-Session-Modification-Reject messages sent from SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".

PDU-Session-Release-Reject:

- INVALID_PDU_SESSION_IDENTITY: The number of PDU-Session-Release-Reject messages sent from SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".

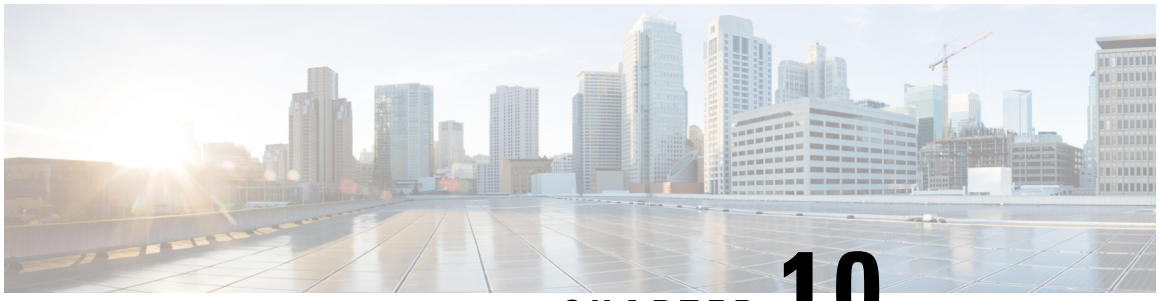
PDU-Session-Release-Request:

- REGULAR_DEACTIVATION: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "REGULAR_DEACTIVATION".
- SEMANTIC_ERRORS_IN_PACKET_FILTER: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC_ERRORS_IN_PACKET_FILTER".
- SYNTACTICAL_ERROR_IN_PACKET_FILTER: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_PACKET_FILTER".
- SEMANTIC_ERROR_IN_THE_TFT_OPERATION: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC_ERROR_IN_THE_TFT_OPERATION".
- SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION".

PDU-Session-Modification-Command-Reject:

- INSUFFICIENT_RESOURCES: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INSUFFICIENT_RESOURCES".
- INVALID_PDU_SESSION_IDENTITY: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".
- SEMANTIC_ERRORS_IN_PACKET_FILTER: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC_ERRORS_IN_PACKET_FILTER".
- SYNTACTICAL_ERROR_IN_PACKET_FILTER: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_PACKET_FILTER".
- SEMANTIC_ERROR_IN_THE_QOS_OPERATION: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC_ERROR_IN_THE_QOS_OPERATION".

- SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION".



CHAPTER 10

AN Modification Call Flow Support

Feature Summary and Revision History

Summary Data

Table 28: Summary Data

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 29: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

This procedure is used to release the logical NG-AP signalling connection for the UE between the (R)AN and the AMF and the associated N3 User Plane connections, and (R)AN signalling connection between the UE and the (R)AN and the associated (R)AN resources.

How it Works

When the NG-AP signalling connection is lost due to (R)AN or AMF failure, the AN release is performed locally by the AMF or the (R)AN as described in the following procedure without using or relying on any of the signalling shown between (R)AN and AMF. The AN release causes all UP connections of the UE to be deactivated.

The initiation of AN release may be due to:

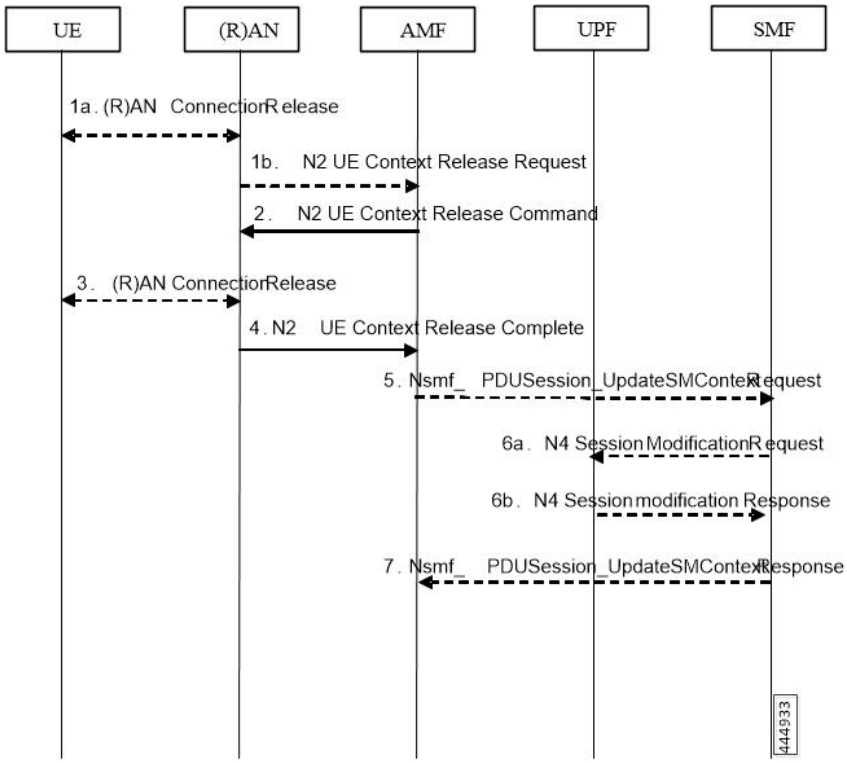
- (R)AN-initiated with cause, for example, O&M Intervention, Unspecified Failure, (R)AN (for example, Radio) Link Failure, User Inactivity, Inter-System Redirection, request for establishment of QoS Flow for IMS voice, Release due to UE-generated signalling connection release, mobility restriction, Release Assistance Information (RAI) from the UE, and so on, or
- AMF-initiated with cause like Unspecified Failure, and so on

Both (R)AN-initiated and AMF-initiated AN Release procedures are shown in the following figure.

If Service Gap Control is applied for the UE and the Service Gap timer is not already running, the Service Gap timer is started in AMF and UE when entering CM-IDLE, unless the connection was initiated after a paging of an MT event, or after a Registration procedure without Uplink data status.

For this procedure, the impacted SMF and UPF are all under control of the PLMN serving the UE, for example, in Home Routed roaming case the SMF and UPF in HPLMN are not involved.

Figure 20: AN Release Procedure



Step	Description
1.	If there is some confirmed (R)AN conditions like Radio Link Failure or for other (R)AN internal reason, the (R)AN may decide to initiate the UE context release in the (R)AN. In this case, the (R)AN sends an N2 UE Context Release Request (Cause, List of PDU Session ID(s) with active N3 user plane) message to the AMF. Cause indicates the reason for the release (for example, AN Link Failure, O&M intervention, unspecified failure, and so on). The List of PDU Session ID(s) indicates that the PDU Sessions served by (R)AN of the UE. If the (R)AN is NG-RAN "UE Context Release Request (NG-RAN node initiated)". If the reason for the release is the NG-RAN received an AS Release Assistance Indicator, NG-RAN does not release the RRC connection but sends an N2 UE Context Release Request message to the AMF. If the AS RAI indicates only a single downlink transmission is expected, then NG-RAN sends only the N2 UE Context Release Request after a single downlink NAS PDU or N3 data PDU has been transferred. If N2 Context Release Request cause indicates the release, then release is requested due to user inactivity or AS RAI. Then, the AMF continues with the AN Release procedure unless the AMF is aware of pending MT traffic or signalling.

Step	Description
2.	If the AMF receives the N2 UE Context Release Request message or due to an internal AMF event, including the reception of Service Request or Registration Request to establish another NAS signalling connection still via (R)AN, the AMF sends an N2 UE Context Release Command (Cause) to the (R)AN. The Cause indicates either the Cause from (R)AN in step 1 or the Cause due to an AMF event. In case the (R)AN is a NG-RAN this step, "UE Context Release (AMF initiated)". In case the (R)AN is an N3IWF/TNGF/W-AGF this step. If the AMF receives Service Request or Registration Request to establish another NAS signalling connection still via (R)AN, after successfully authenticating the UE, the AMF releases the old NAS signalling connection, and then continues the Service Request or Registration Request procedure.
3.	If the (R)AN connection (for example, RRC connection or NWu connection) with the UE is not already released (step 1), either: **1.** The (R)AN requests the UE to release the (R)AN connection. Upon receiving (R)AN connection release confirmation from the UE, the (R)AN deletes the UE's context, or **2.** If the Cause in the N2 UE Context Release Command indicates that the UE has already locally released the RRC connection, the (R)AN locally releases the RRC connection.
4.	The (R)AN confirms the N2 Release by returning an N2 UE Context Release Complete (List of PDU Session ID(s) with active N3 user plane, User Location Information, Age of Location Information) message to the AMF. The List of PDU Session ID(s) indicates that the PDU Sessions served by (R)AN of the UE. The AMF always stores the latest UE Radio Capability information or NB-IoT specific UE Radio Access Capability Information received from the NG-RAN node received. The N2 signalling connection between the AMF and the (R)AN for that UE is released. The (R)AN provides the list of recommended cells / TAs / NG-RAN node identifiers for paging to the AMF. If the PLMN has configured secondary RAT usage reporting, the NG-RAN node provides RAN usage data Report. This step is performed immediately after step 2, for example, in a situation where the UE does not acknowledge the RRC Connection Release. The NG-RAN includes Paging Assistance Data for CE capable UE, if available, in the N2 UE Context Release Complete message. The AMF stores the received Paging Assistance Data for CE capable UE in the UE context for subsequent Paging procedure.

Step	Description
5.	For each of the PDU Sessions in the N2 UE Context Release Complete, the AMF invokes Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID, PDU Session Deactivation, Cause, Operation Type, User Location Information, Age of Location Information, N2 SM Information (Secondary RAT usage data)). The Cause in step 5 is the same Cause in step 2. If List of PDU Session ID(s) with active N3 user plane is included in step 1b, the step 5 through step 7 are performed before step 2. The Operation Type is set to "UP deactivate" to indicate deactivation of user plane resources for the PDU Session. For PDU Sessions using Control Plane CIoT 5GS Optimization and if the UE has negotiated the use of extended Idle mode DRX, the AMF informs the SMF immediately that the UE is not reachable for downlink data. For PDU Sessions using Control Plane CIoT 5GS Optimization and if the UE has negotiated the use of MICO mode with Active Time, the AMF informs the SMF that the UE is not reachable for downlink data once the Active Time has expired.
6.	The SMF sends N4 Session Modification Request (AN or N3 UPF Tunnel Info to be removed, Buffering on/off) to the UPF. For PDU Sessions not using Control Plane CIoT 5GS Optimization, the SMF initiates an N4 Session Modification procedure indicating the need to remove Tunnel Info of AN or UPF terminating N3. Buffering on/off indicates whether the UPF has to buffer incoming DL PDU or not. If the SMF has received an indication from the AMF that the UE is not reachable for downlink data for PDU Sessions using Control Plane CIoT 5GS Optimization, the SMF initiates an N4 Session Modification procedure to activate buffering in the UPF. If multiple UPFs are used in the PDU Session and the SMF determines to release the UPF terminating N3, step 6a is performed towards the UPF (for example, PSA) terminating N9 towards the current N3 UPF. The SMF then releases the N4 session towards the N3 UPF (the N4 release is not shown in the call flow). If the cause of AN Release is because of User Inactivity, or UE Redirection, the SMF preserves the GBR QoS Flows. Otherwise, the SMF triggers the PDU Session Modification procedure for the GBR QoS Flows of the UE after the AN Release procedure is completed. If the redundant I-UPFs are used for URLLC, the N4 Session Modification Request procedure is done for each I-UPF. In this case, the SMF selects both the redundant I-UPFs to buffer the DL packets for this PDU Session or drop the DL packets for this PDU session or forward the DL packets for this PDU session to the SMF, based on buffering instruction provided by the SMF. If the redundant N3 tunnels are used for URLLC, the N4 Session Modification Request procedure to the UPF of N3 terminating point is to remove the dual AN Tunnel Info for N3 tunnel of the corresponding PDU Session.
6b.	The UPF sends N4 Session Modification Response acknowledging the SMF request to the SMF.

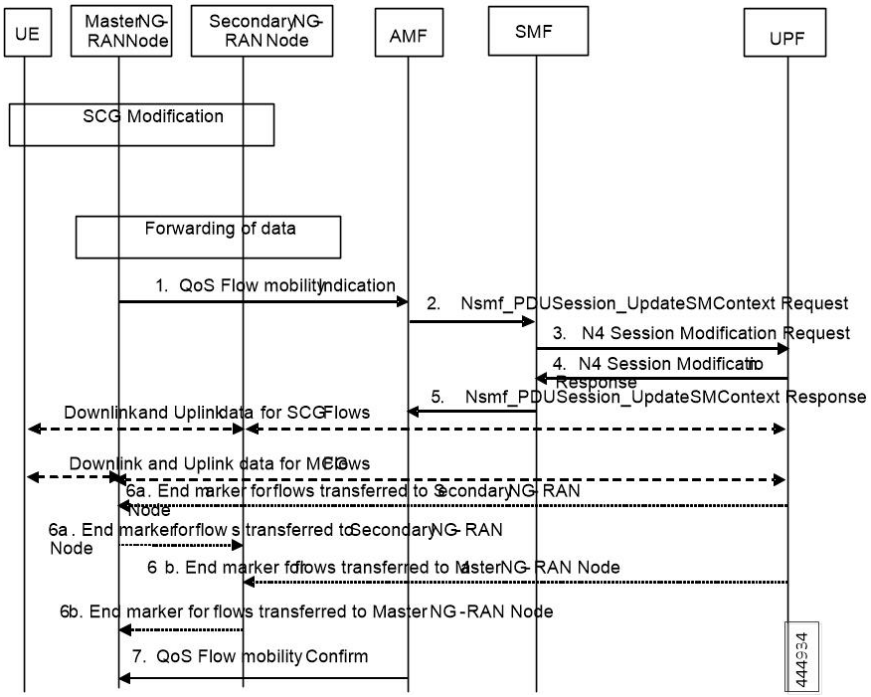
Step	Description
7.	The SMF sends Nsmf_PDUSession_UpdateSMContext Response for step 5 to the AMF. Once the procedure is completed, the AMF considers the N2 and N3 as released and enters CM-IDLE state. After completion of the procedure, the AMF reports towards the NF consumers.

Dual Connectivity Support

This procedure is used to transfer QoS Flows to and from Secondary RAN Node. During this procedure, the SMF, and UPF are never re-allocated. The presence of IP connectivity between the UPF and the Master RAN node, as well as between the UPF and the Secondary RAN node is assumed.

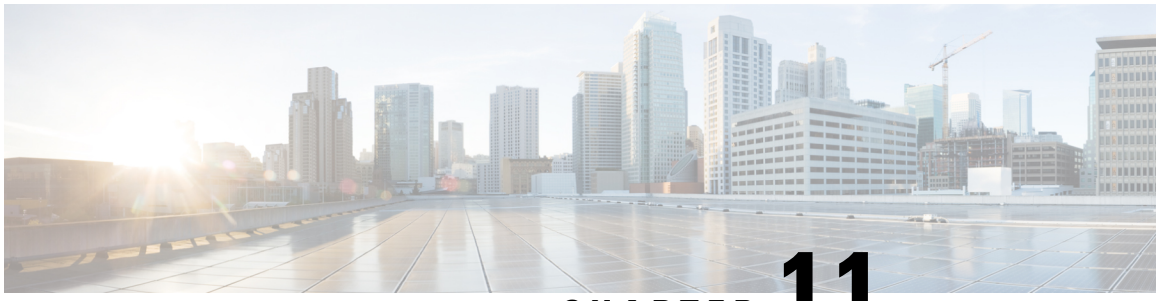
If QoS Flows for multiple PDU Sessions need to be transferred to or from Secondary RAN Node, the procedure shown in the below figure below is repeated for each PDU Session.

Figure 21: NG-RAN initiated QoS Flow mobility procedure



Step	Description
1.	The Master RAN node sends a N2 QoS Flow mobility Indication (PDU Session ID, QFI(s), AN Tunnel Info) message to the AMF. AN Tunnel Info includes the new RAN tunnel endpoint for the QFI(s) for which the AN Tunnel Info shall be modified.
2.	AMF to SMF, Nsmf_PDUSession_UpdateSMContext request (N2 QoS Flow mobility Indication message PDU Session ID).
3.	The SMF sends an N4 Session Modification Request (PDU Session ID(s), QFI(s), AN Tunnel Info for downlink user plane) message to the UPF.

Step	Description
4.	The UPF returns an N4 Session Modification Response (CN Tunnel Info for uplink traffic) message to the SMF after requested QFIs are switched. **Important** Step 7 can occur anytime after receipt of N4 Session Modification Response at the SMF.
5.	SMF to AMF, Nsmf_PDUSession_UpdateSMContext response (N2 SM information (CN Tunnel Info for uplink traffic)) for QFIs of the PDU Session which have been switched successfully. If none of the requested QFIs are switched successfully, the SMF sends an N2 QoS Flow mobility Failure message.
6.	In order to assist the reordering function in the Master RAN node and/or Secondary RAN node, for each affected N3 tunnel the UPF sends one or more "end marker" packets on the old tunnel immediately after switching the tunnel for the QFI. The UPF starts sending downlink packets to the Target NG-RAN.
7.	The AMF relays message 5 to the Master RAN node.



CHAPTER 11

Application-based Alerts

Feature Summary and Revision History

Summary Data

Table 30: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 31: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

When the system detects an anomaly, it generates an alert notification. The system statistics are the cause for these alert notifications. You can set an expression to trigger an alert when the expression becomes true.

How it Works

The Common Execution Environment (CEE) uses the Prometheus Alert Manager for alerting operations. The CEE YANG model - either through CLI or API - allows users to view the active alerts, silenced alerts, and alert history. Also, the applications can call the alert API directly to add or clear alerts. The Prometheus Alert Manager API (v2) is the standard API used.

The Prometheus Alerts Manager includes the following options:

- **Defining Alert Rules**: This option defines the types of alerts that the Alert Manager should trigger. Use the Prometheus Query Language (PromQL) to define the alerts.
- **Defining Alert Routing**: This option defines the action the Alert Manager should take after receiving the alerts. At present, the SNMP Trapper is supported as the outbound alerting. Also, the CEE provides an Alert Logger for storing the generated alerts.

Configuring Alert Rules

To configure the alert rules, use the following configuration:

```
configure
   alerts rules group alert_group_name
   interval-seconds seconds
   rule rule_name
      expression promql_expression
      duration duration
      severity severity_level
      type alert-type
      annotation annotation_name
      value annotation_value
      exit
   exit
```

NOTES:

- **alerts rules**: Specifies the Prometheus alerting rules.
- **group** *alert_group_name*: Specifies the Prometheus alerting rule group. One alert group can have multiple lists of rules. *alert-group-name* is the name of the alert group. The alert-group-name must be a string in the range of 0–64 characters.
- **interval-seconds** *seconds*: Specifies the evaluation interval of the rule group in seconds.
- **rule** *rule_name*: Specifies the alerting rule definition. *rule_name* is the name of the rule.

- **expression** *promql_expression*: Specifies the PromQL alerting rule expression. *promql_expression* is the alert rule query expressed in PromQL syntax.
- **duration** *duration*: Specifies the duration of a true condition before it is considered true. *duration* is the time interval before the alert is triggered.
- **severity** *severity_level*: Specifies the severity of the alert. *severity-level* is the severity level of the alert. The severity levels are critical, major, minor, and warning.
- **type** *alert_type*: Specifies the type of the alert. *alert_type* is the user-defined alert type. For example, Communications Alarm, Environmental Alarm, Equipment Alarm, Indeterminate Integrity Violation Alarm, Operational Violation Alarm, Physical Violation Alarm, Processing Error Alarm, Quality of Service Alarm, Security Service Alarm, Mechanism Violation Alarm, or Time Domain Violation Alarm.
- **annotation** *annotation_name*: Specifies the annotation to attach to the alerts. *annotation_name* is the name of the annotation.
- **value** *annotation_value*: Specifies the annotation value. *annotation_value* is the value of the annotation.

The following example configures an alert, which is triggered when the percentage of Unified Data Management (UDM) responses is less than the specified threshold limit.

Example:

```
 configure terminal
  alerts rules group SMFUDMchk_incr
  interval-seconds 300
  rule SMFUDMchk_incr
  expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[3m]))
 < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UDM responses is less than threshold‟
  exit
 exit
exit
```

You can view the configured alert using the **show running-config alerts** command.

Example:

The following example displays the alerts configured in the running configuration:

```
 show running-config alerts
  interval-seconds 300
  rule SMFUDMchk_incr
  expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[3m]))
 < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UDM responses is less than threshold‟

  exit
 exit
exit
```

Viewing Alert Logger

The Alert Logger stores all the generated alerts by default. You can view the stored alerts using the following **show** command.

show alert history [filtering]

You can narrow down the result using the following filtering options:

- **annotations**: Specifies the annotations of the alert.
- **endsAt**: Specifies the end time of the alert.
- **labels**: Specifies the additional labels of the alert.
- **severity**: Specifies the severity of the alert.
- **source**: Specifies the source of the alert.
- **startsAt**: Specifies the start time of the alert.
- **type**: Specifies the type of the alert.

The following example displays the history of the alerts configured in the system:

Example:

```
show alerts history
alerts active SMFUDMchk_incr ac2a970ab621
state active
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
than threshold.” ]
```

You can view the active and silenced alerts with the **show alerts active** and **show alerts active** commands.

The following example displays the active alerts. The alerts remain active as long as the evaluated expression is true.

Example:

```
show alerts active
alerts active SMFUDMchk_incr ac2a970ab621
state active
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
than threshold.” ]
```

Call Flow Procedure Alerts

This section provides detail of commands that are required to configure alerts related to various call flow procedures.

4G PDN Modify

Use the following commands to configure alerts related to the 4G PDN Modify procedure.

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNModify
   expression
"sum(smf_service_stats{procedure_type=~\"pdn_ho_location_changed|pdn_ho_rat_type_changed|pdn_inter_sgw_handover|pdn_mbr\"
 , status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"pdn_ho_location_changed|pdn_ho_rat_type_changed|pdn_inter_sgw_handover|pdn_mbr\"
 , status=\"attempted\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Modify is below
threshold"
   exit
exit
```

4G PDN Release Success

Use the following commands to configure alerts related to the 4G PDN Release Success procedure.

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNRelease
   expression "sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Release is below
threshold."
   exit
exit
```

4G PDN Setup Success

Use the following commands to configure alerts related to the 4G PDN Setup Success procedure.

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNSetup
   expression "sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Setup is below
threshold."
   exit
exit
```

4G to 5G HO Success

Use the following commands to configure alerts related to the 4G to 5G HO Success procedure.

```
alerts rules group Handover
   interval-seconds 300
   rule 4gTo5gHOSuccess
   expression
"sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\"
, status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\" ,
 status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G to 5G HO is below
threshold."
   exit
exit
```

4G To WiFi HO Success

Use the following commands to configure alerts related to the 4G to WiFi HO Success procedure.

```
alerts rules group Handover
   interval-seconds 300
   rule 4GtoWifiHOSuccess
   expression "sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\"
, status=\"success\"}) /
sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
   exit
exit
```

5G N2 HO Success

Use the following commands to configure alerts related to the 5G N2 HO Success procedure.

```
alerts rules group Handover
   interval-seconds 300
   rule N2HOSuccess
  expression "sum(smf_service_stats{procedure_type=\"n2_handover\" , status=\"success\"})
 / sum(smf_service_stats{procedure_type=\"n2_handover\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage successful 5G N2 HO is below threshold."

   exit
exit
```

5G PDU Idle Success

Use the following commands to configure alerts related to the 5G PDU Idle Success procedure.

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFPDUIdleSuccess
   expression "sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"success\"})
/ sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Idle is below threshold"

   exit
exit
```

5G PDU Modify Success

Use the following commands to configure alerts related to the 5G PDU Modify Success procedure.

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionModifySuccess
   expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Modify is below
threshold"
   exit
exit
```

5G PDU Release Success

Use the following commands to configure alerts related to the 5G PDU Release Success procedure.

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionReleaseFailure
   expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Setup is below
threshold"
   exit
exit
```

5G PDU Setup Success

Use the following commands to configure alerts related to the 5G PDU Setup Success procedure.

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionSetupFailure
   expression "sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when failed to setup sessions is more than 5%"
   exit
exit
```

5G to 4G HO Success

Use the following commands to configure alerts related to the 5G to 4G HO Success procedure.

```
alerts rules group Handover
   interval-seconds 300
   rule 5gTo4gHOSuccess
   expression
"sum(smf_service_stats{procedure_type=\"pdh_5g_4g_handover|pdh_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|eps_fb_5g_4g_handover_idft|pdh_5g_4g_handover_idft\"
 , status=\"success\"}) /
sum(smf_service_stats{procedure_type=\"pdh_5g_4g_handover|pdh_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|eps_fb_5g_4g_handover_idft|pdh_5g_4g_handover_idft\"
 , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G to 4G HO is below
threshold."
   exit
exit
```

5G To WiFi HO Success

Use the following commands to configure alerts related to the 5G to WiFi HO Success procedure.

```
alerts rules group Handover
   interval-seconds 300
   rule 5GtoWifiHOSuccess
   expression "sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\" ,
 status=\"success\"}) / sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\"
 , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
   exit
exit
```

5G Xn HO Success

Use the following commands to configure alerts related to the 5G Xn HO Success procedure.

```
alerts rules group Handover
   interval-seconds 300
   rule XnHOSuccess
  expression "sum(smf_service_stats{procedure_type=\"xn_handover\" , status=\"success\"})
 / sum(smf_service_stats{procedure_type=\"xn_handover\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G Xn HO is below threshold."

   exit
exit
```

PDN Session Create

Use the following commands to configure alerts related to the PDN Session Create procedure.

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDNSessCreate
   expression
"sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=\"pdn_sess_create\",status=\"success\"}[5m]))
  /
sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=\"pdn_sess_create\",status=\"attempted\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of pdn_sess_create procedure is
 lesser threshold."
   exit
exit
```

PDU Session Create

Use the following commands to configure alerts related to the PDU Session Create procedure.

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessCreate
   expression
"sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=\"pdu_sess_create\",status=\"success\"}[5m]))
  /
sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=\"pdu_sess_create\",status=\"attempted\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of pdu_sess_create procedure is
 lesser threshold."
   exit
exit
```

PDU Session Modify

Use the following commands to configure alerts related to the PDU Session Modify procedure.

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessModify
   expression
"sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".*req_pdu_sess_mod\",status=\"success\"}[5m]))
  /
sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".*req_pdu_sess_mod\",status=\"attempted\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of req_pdu_sess_mod procedure
is lesser threshold."
   exit
exit
```

PDU Session Release

Use the following commands to configure alerts related to the PDU Session Release procedure.

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessRelease
   expression
"sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".*req_pdu_sess_rel\",status=\"success\"}[5m]))
  /
sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".*req_pdu_sess_rel\",status=\"attempted\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of req_pdu_sess_rel procedure
is lesser threshold."
   exit
exit
```

Interface Specific Alerts

This section provides detail of commands that are required to configure alerts related to various interfaces.

GTPC Peer Down

Use the following commands to configure alerts related to the GTPC Peer Down procedure.

```
alerts rules group GTPCPeerDown
   interval-seconds 300
   rule GTPCPeerDown
   expression nodemgr_gtpc_peer_status{gtpc_peer_status=\"gtpc_peer_path_down\"})
   severity major
   type "Communications Alarm"
   annotation summary
```

```
   value "This alert is fired when the GTPC Path failure detected for peer crosses
threshold"
   exit
exit
```

N4 Message Success

Use the following commands to configure alerts related to the N4 Message Success procedure.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN4MessageSuccess
   expression "sum(smf_protocol_udp_res_msg_total{message_direction=\"inbound\",
status=\"accepted\"}) /  sum(smf_protocol_udp_res_msg_total{message_direction=\"inbound\",
 status=~\"accepted|denied\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
   exit
exit
```

N4 UPF Association Down

Use the following commands to configure alerts related to the N4 UPF Association Down query by N4 address.

```
alerts rules group N4Association
   interval-seconds 300
   rule SMFAssociationRelease
  expression "smf_proto_udp_res_msg_total{procedure_type=\"n4_association_release_res\",
 message_direction= \"inbound\", status=\"accepted\"}) "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the N4 Association with UPF is released"
   exit
exit
```

N4 UPF Association Up

Use the following commands to configure alerts related to the N4 UPF Association Up query by N4 address.

```
alerts rules group N4Association
   interval-seconds 300
   rule N4AssociationUP
   expression "smf_proto_udp_res_msg_total{procedure_type=\"n4_association_setup_res\",
 message_direction= \"inbound\", status=\"accepted\"}"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the N4 Association with UPF is established"
   exit
exit
```

N7 Interface Outbound

Use the following commands to configure alerts related to an outbound N7 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N7 responses received is lesser
threshold."
   exit
exit
```

N7 Interface Inbound

Use the following commands to configure alerts related to an inbound N7 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\", message_direction=\"inbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of N7 responses sent is lesser threshold."

   exit
exit
```

N7 Message Timed Out

Use the following commands to configure alerts related to the N7 Message Timed Out procedure.

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN7Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the increase in timeout for N7 messages toward PCF
crosses threshold"
   exit
exit
```

N10 Interface

Use the following commands to configure alerts related to the N10 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N10 responses received is lesser
threshold."
   exit
exit
```

N11 Interface Inbound

Use the following commands to configure alerts related to an inbound N11 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"amf\", message_direction=\"inbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N11 responses sent is lesser
threshold."
   exit
exit
```

N11 Interface Outbound

Use the following commands to configure alerts related to an outbound N11 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 60
   rule SMFN11Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"amf\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N11 responses received is lesser
threshold."
   exit
exit
```

N11 Message Timed Out

Use the following commands to configure alerts related to the N11 Message Timed Out procedure.

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN40Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the increase in timeout for N11 messages toward AMF
crosses threshold"
   exit
exit
```

N40 Interface Inbound

Use the following commands to configure alerts related to an inbound N40 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN40Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"chf\", message_direction=\"inbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N40 responses sent is lesser
threshold."
   exit
exit
```

N40 Interface Outbound

Use the following commands to configure alerts related to an outbound N40 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN40Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"chf\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N40 responses received is lesser
threshold."
   exit
exit
```

N40 Message Timed Out

Use the following commands to configure alerts related to the N40 Message Timed Out procedure.

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN11Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired the increase in timeout for N40 messages toward CHF crosses
 threshold"
   exit
exit
```

NRF Discovery

Use the following commands to configure alerts related to the NRF Discovery procedure.

```
alerts rules group NRF
   interval-seconds 300
   rule NRFDiscovery
   expression
"sum(nf_discover_messages_total{result=~\"success|failure\",svc_name=\"nnrf-disc\",
service_name=\"smf-rest-ep\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
   exit
exit
```

SMF Service Start

Use the following commands to configure alerts related to the SMF Service Start procedure.

```
alerts rules group SMFService
   interval-seconds 300
   rule SMFServiceStart
   expression "irate(outgoing_response_msg_total{msg_type=\"NrfNfmRegistration\"}[5m])"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when SMF-Service starts upon registration with NRF"
   exit
exit
```

IP Pool

This section provides detail of commands that are required to configure alerts related to IP Pool.

IP Pool Used

Use the following commands to configure alerts related to the IP Pool used procedure.

```
alerts rules group IPPool
   interval-seconds 300
   rule IPPool
   expression "sum(IPAM_address_allocations_current) > THRESHOLD"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage IP pool addresses used is above the
threshold"
   exit
exit
```

Message Level Alerts

This section provides detail of commands that are required to configure alerts related to various messages.

N11 SM Create

Use the following commands to configure alerts related to N11 SM Create.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Success
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_create_sm_context\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_create_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_create_sm_context responses sent
 is lesser threshold."
   exit
exit
```

N11 SM Update

Use the following commands to configure alerts related to N11 SM Update.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Update
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
 message_direction=\"inbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_update_sm_context responses sent
```

```
 is lesser threshold."
   exit
exit
```

N11 SM Release

Use the following commands to configure alerts related to N11 SM Release.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Release
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
 message_direction=\"inbound\", response_status=\"204\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_release_sm_context responses sent
 is lesser threshold."
   exit
exit
```

N1 N2 Message Transfer

Use the following commands to configure alerts related to N1 N2 Message Transfer.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN1N2Transfer
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_n1_n2_transfer responses received
 is lesser threshold."
   exit
exit
```

N11 EBI Assignment

Use the following commands to configure alerts related to N11 EBI Assignment.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11EBI
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
```

```
  value "This alert is fired when the percentage of amf_assign_ebi responses received is
 lesser threshold."
  exit
exit
```

N11 SM Status Notify

Use the following commands to configure alerts related to N11 SM Status Notify.

```
alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN11StatusNotify
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
message_direction=\"outbound\"}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of amf_status_notify responses received
 is lesser threshold."
  exit
exit
```

N11 SM Context Retrieve

Use the following commands to configure alerts related to N11 SM Context Retrieve.

```
alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN11ContextRetrieve
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of amf_retrieve_sm_context responses
sent is lesser threshold."
  exit
exit
```

N7 SM Policy Create

Use the following commands to configure alerts related to N7 SM Policy Create.

```
alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN7PolicyCreate
  expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\"}[5m])) < 0.95"
  severity major
```

```
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_create responses
 received is lesser threshold."
   exit
exit
```

N7 SM Policy Update

Use the following commands to configure alerts related to N7 SM Policy Update.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyUpdate
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_update responses
 received is lesser threshold."
   exit
exit
```

N7 SM Policy Delete

Use the following commands to configure alerts related to N7 SM Policy Delete.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyDelete
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_delete\",
message_direction=\"outbound\", response_status=\"204\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_delete\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_delete responses
 received is lesser threshold."
   exit
exit
```

N7 SM Policy Notify Update

Use the following commands to configure alerts related to N7 SM Policy Notify Update.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyUpdateNotify
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update_notify\",
```

```
message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update_notify\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of pcf_sm_policy_control_update_notify
 responses sent is lesser threshold."
   exit
exit
```

N7 SM Policy Notify Terminate

Use the following commands to configure alerts related to N7 SM Policy Terminate.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyTerminateNotify
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_terminate_notify\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_terminate_notify\",
 message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_terminate_notify
 responses sent is lesser threshold."
   exit
exit
```

N10 UE Register

Use the following commands to configure alerts related to N10 UE Register.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10UERegister
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of register_ue responses received is
lesser threshold."
   exit
exit
```

N10 UE DeRegister

Use the following commands to configure alerts related to N10 UE DeRegister.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
```

```
   rule SMFN10UEDeRegister
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of deregister_ue responses received is
 lesser threshold."
   exit
exit
```

N10 SM Subscription Fetch

Use the following commands to configure alerts related to N10 Subscription Fetch.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10SubscriptionFetch
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of subscription_req responses received
 is lesser threshold."
   exit
exit
```

N10 SM Subscribe for Notification

Use the following commands to configure alerts related to N10 Subscribe for Notification.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10SubscriptionNotification
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
 message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of sdm_subscription_req responses received
 is lesser threshold."
   exit
exit
```

N10 Charging Data Request

Use the following commands to configure alerts related to N10 Charging Data Request.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10ChargingRequest
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
message_direction=\"outbound\", response_status=\"201\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of chf_charging_data_request responses
 received is lesser threshold.”
   exit
exit
```

N10 Charging Data Notify

Use the following commands to configure alerts related to N10 Charging Data Notify.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10ChargingDataNotify
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
message_direction=\"inbound\", response_status=\"201\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
message_direction=\"inbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of chf_abort_notify responses sent is
lesser threshold.”
   exit
exit
```

Policy Rule Alerts

This section provides detail of commands that are required to configure alerts related to various policy rules.

Addition of Dynamic PCC Rules

Use the following commands to configure alerts related to addition of dynamic PCC rules.

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule AddPCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"install\”}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"install\”}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful addition of dynamic pcc
```

```
rules is lesser threshold."
   exit
exit
```

Modification of Dynamic PCC Rules

Use the following commands to configure alerts related to modification of dynamic PCC rules.

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule ModifyPCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"modify\"}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"modify\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful modification of dynamic
pcc rules is lesser threshold."
   exit
exit
```

Removal of Dynamic PCC Rules

Use the following commands to configure alerts related to removal of dynamic PCC rules.

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule RemovePCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"remove\"}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"remove\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful removal of dynamic pcc
rules is lesser threshold."
   exit
exit
```

SMF Overload/Congestion

This section provides detail of commands that are required to configure alerts related to various SMF Overload/Congestion.

SMF Overload

Use the following commands to configure alerts related to the SMF Overload procedure.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
```

```
   rule SMFOverload
   expression "sum by (component) (system_overload_status) == true"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when increase in events not processed due to system overload"

   exit
exit
```

SMF Sessions

This section provides detail of commands that are required to configure alerts related to various SMF sessions.

Session Release Rate

Use the following commands to configure alerts related to the Session Release Rate procedure.

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionReleaseRate
  expression "sum(rate(smf_service_stats{procedure_type=~\".*pdu_sess_rel|.*pdn_sess_rel\"
 , status=\"attempted\"}[5m])) >  THRESHOLD "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the session release rate exceeds the threshold"
   exit
exit
```

Session Setup Failure

Use the following commands to configure alerts related to the Session Setup Failure procedure.

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionSetupFailure
  expression "sum(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\"
 , status=\"failures\"}) /
sum(smf_service_stats{procedure_type=\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}) >  0.05 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when failed to setup sessions is more than 5%"
   exit
exit
```

Session Setup Rate

Use the following commands to configure alerts related to the Session Setup Rate procedure.

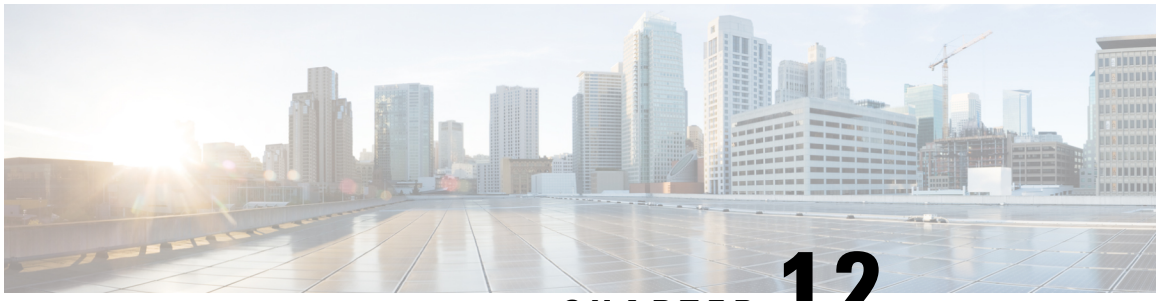
```
alerts rules group SMFSession
   interval-seconds 300
```

```
   rule SMFSessionSetupRate
   expression
"sum(rate(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}[5m]))>  THRESHOLD "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the session setup rate exceeds the threshold"
   exit
exit
```

Subscriber Limit

Use the following commands to configure alerts related to the Subscriber Limit procedure.

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSubscriberLimit
   expression "sum(smf_session_counters{pdu_type=~\"ipv4v6|ipv4|ipv6\"}) > THRESHOLD"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the max number of subscribers is more than the threshold"

   exit
exit
```



CHAPTER 12

Bulk Statistics and Key Performance Indicators

Feature Summary and Revision History

Summary Data

Table 32: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 33: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

This chapter provides details of bulk statistics, and Key Performance Indicators (KPIs) used for performance analysis on SMF.

There are two types of bulk statistics:

- Gauge - A snapshot value that shows the statistic at that reporting moment (for example, the number of current PDP contexts, simultaneous Active EPS Bearers). Gauge statistics can increment or decrement continuously.
- Counter - A historic value that shows the statistic that accumulated over time (for example, the total number of CSR requests received). Counter values can only increment except in two cases: rollover, where a counter exceeds its maximum value and rolls over to zero, and reset, where a counter is manually reset to zero.

How it Works

The following bulk statistics are supported in SMF for Attempted, Success, and Failures:

- 4G and WiFi message-level statistics (CREATE, DELETE, UPDATE)
- PCF and CHF message-level statistics
- Handover:
  - 4G to 5G
  - 5G to 4G
  - Voice over New Radio (VoNR)
  - WiFi to NR
  - NR to WiFi
  - WiFi to eNB
  - eNB to WiFi

Supported KPIs

Common Statistics

The following table provides details of KPIs related to common statistics.

KPI Name	Type	Description/Formula	Label
Total PCF Policy Create Attempted	Counter	Total number of PCF Create attempted (%smPolicyCreate%)	status="attempted",dnn,rat_type
Total PCF Policy Create Success	Counter	(%smPolicyCreate%) Total PCF Policy Create Attempted - Total PCF Policy Create Failure	dnn,rat_type

KPI Name	Type	Description/Formula	Label
Total PCF Policy Create Failure	Counter	(%smPolicyCreate%)	status="failed",dnn,rat_type
Total PCF Policy Update Attempted	Counter	(%smPolicyUpdate%)	status="attempted", dnn, rat_type
Total PCF Policy Update Success	Counter	(%smPolicyUpdate%) Total PCF Policy Update Attempted - Total PCF Policy Update Failure	dnn,rat_type
Total PCF Policy Update Failure	Counter	(%smPolicyUpdate%)	status="failed", dnn, rat_type
Total PCF Update Notify Received	Counter	(%smPolicyUpdateNotify%)	status="accepted",dnn, rat_type
Total PCF Update Notify success	Counter	Total PCF Update Notify Received - Total PCF Update Notify failure	dnn, rat_type
Total PCF Update Notify Failure	Counter	(%smPolicyUpdateNotify%)	status="rejected"/status="failed",dnn, rat_type
Total PCF Terminate Attempted	Counter	(%smPolicyTerminate%)	status="attempted", dnn, rat_type
Total PCF Terminate Success	Counter	(%smPolicyTerminate %)	status="success",dnn, rat_type
Total PCF Terminate Failures	Counter	(%smPolicyTerminate%)	status="failure", dnn, rat_type
Total CHF Update Attempted	Counter	(%charging_update%)	status="attempted", dnn, rat_type
Total CHF Update Success	Counter	(%charging_update%)	status="success", dnn, rat_type
Total CHF Update Failure/Timeout	Counter	(%charging_update%)	status="failure", dnn, rat_typpe
Total CHF terminate Attempted	Counter	(%charging_terminate%)	status="attempted", dnn, rat_type

KPI Name	Type	Description/Formula	Label
Total CHF terminate Success	Counter	(%charging_terminate%)	status="success", dnn, rat_type
Total CHF terminate Failure	Counter	(%charging_terminate%)	status="failure", dnn, rat_type
Total 5gto4g Handover Attempted	Counter	pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="attempted"
Total 5gto4g Handover Success	Counter	pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="success"
Total 5gto4g Handover Failure	Counter	pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="failure", reason="idft_setup_failure" reason="mbr_setup_failure" reason="upf_failure"
Total 4gto5g Handover Attempted	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft n26_4g_to_5g_im_mobility	status="attempted"
Total 4gto5g Handover Success	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft n26_4g_to_5g_im_mobility	status="success"
Total 4gto5g Handover Failure	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft n26_4g_to_5g_im_mobility	status="failure" reason="n26ho_4g_5g_n1n2_transfer_failure" reason="disc_n26_4g_5g_ho_udm_reg_failed" reason="disc_n26_4g_5g_ho_n4_modify_failed"
Total EPSFB Attempted	Counter	eps_fb_5g_4g_handover_dft eps_fb_5g_4g_handover_idft eps_fb_ded_brr	status="attempted",

KPI Name	Type	Description/Formula	Label
Total EPSFB Success	Counter	eps_fb_5g_4g_handover_dft eps_fb_5g_4g_handover_idft eps_fb_ded_brr	status="success",
Total EPSFB Failure	Counter	eps_fb_5g_4g_handover_dft eps_fb_5g_4g_handover_idft eps_fb_ded_brr	status="failure", reason="idft_setup_failure" reason="mbr_setup_failure" reason="upf_failure" reason="sgw_failure"
Total NRtoWifi Attempted	Counter	nr_to_untrusted_wifi_handover pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="attempted"
Total NRtoWifi Success	Counter	nr_to_untrusted_wifi_handover pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="success"
Total NRtoWifi Failure	Counter	nr_to_untrusted_wifi_handover pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="failure", reason="nr_to_untrusted_wifi_invalid_json" reason="nr_to_untrusted_wifi_invalid_paa" reason="nr_to_untrusted_wifi_invalid_msg" reason="nr_to_untrusted_wifi_pcf_failed" reason="nr_to_untrusted_wifi_n40_failed" reason="nr_to_untrusted_wifi_n4_failed" reason="nr_to_untrusted_wifi_pcf_failed_post_cb" reason="nr_to_untrusted_wifi_n40_failed_post_cb" reason="nr_to_untrusted_wifi_n4_failed_post_cb" reason="nr_to_untrusted_wifi_cbr_failed" reason="nr_to_untrusted_wifi_n1n2_release_failed" reason="nr_to_untrusted_wifi_n4_failed_post_ho" reason="nr_to_untrusted_wifi_pcf_update_failed_post_ho" reason="nr_to_untrusted_wifi_chf_update_failed_post_ho"

KPI Name	Type	Description/Formula	Label
Total WifitoNR Attempted	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft	status="attempted"
Total WifitoNR Success	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft	status="success"
Total WifitoNR Failure	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft	status="failure"
Total eNBtoWifi Attempted	Counter	enb_to_untrusted_wifi_handover	status="attempted"
Total eNBtoWifi Success	Counter	enb_to_untrusted_wifi_handover	status="success"

KPI Name	Type	Description/Formula	Label
Total eNBtoWifi Failure	Counter	enb_to_untrusted_wifi_handover	status="failure", reason="enb_to_untrusted_wifi_to_enb_ho_reject" reason="enb_to_untrusted_wifi_to_enb_invalid_sess_state" reason="enb_to_untrusted_wifi_to_enb_invalid_json" reason="enb_to_untrusted_wifi_to_enb_invalid_paa" reason="enb_to_untrusted_wifi_to_enb_invalid_msg" reason="enb_to_untrusted_wifi_to_enb_udm_failed" reason="enb_to_untrusted_wifi_to_enb_n40_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_mbr_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_mbr" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_cbr_failed" reason="enb_to_untrusted_wifi_to_enb_dbr_failed"
Total WifitoeNB Attempted	Counter	untrusted_wifi_to_enb_handover	status="attempted"
Total WifitoeNB Success	Counter	untrusted_wifi_to_enb_handover	status="success",

KPI Name	Type	Description/Formula	Label
Total WifitoeNB Failure	Counter	untrusted_wifi_to_enb_handover	status="failure", reason="enb_to_untrusted_wifi_to_enb_ho_reject" reason="enb_to_untrusted_wifi_to_enb_invalid_sess_state" reason="enb_to_untrusted_wifi_to_enb_invalid_json" reason="enb_to_untrusted_wifi_to_enb_invalid_paa" reason="enb_to_untrusted_wifi_to_enb_invalid_msg" reason="enb_to_untrusted_wifi_to_enb_udm_failed" reason="enb_to_untrusted_wifi_to_enb_n40_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_mbr_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_mbr" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_cbr_failed" reason="enb_to_untrusted_wifi_to_enb_dbr_failed"

4G Subscriber

The following table provides details of KPIs related to 4G subscriber statistics.

Note Labels dnn, qci and rat_type are used to filter the counters. Here, rat_type is eutra.

KPI Name	Type	Description/Formula	Label
Total Active sessions	Gauge	Total number of PDN Contexts (%smf_session_counters%)	dnn,rat_type="eutra"
Total Active Bearers	Gauge	Total number of active Bearers (%total_bearer%)	dnn
Total Active Default Bearers	Gauge	(%total_bearer-dedicated_ bearer%)	dnn
Total Active Dedicated Bearers	Gauge	Total number of active Dedicated Bearers (%dedicated_bearer%)	dnn
Total Bearer Creation Attempted	Counter	(%pdn_sess_create+ pcf_req_ded_brr_create + eps_fb_ded_brr)	status="attempted",dnn
Total Bearers Creation Success	Counter	(%pdn_sess_create+ pcf_req_ded_brr_create + eps_fb_ded_brr)	status="success",dnn
Total Bearers Creation Failure	Counter	(%pdn_sess_create+ pcf_req_ded_brr_create + eps_fb_ded_brr)	status="failure",dnn
Total Dedicated Bearers Attempted	Counter	(%pcf_req_ded_brr_create + eps_fb_ded_brr %)	status="attempted",dnn
Total Dedicated Bearers Failure/Rejected	Counter	(%pcf_req_ded_brr_create + eps_fb_ded_brr %)	status="failure",dnn
Total Dedicated Bearers Success	Counter	(%pcf_req_ded_brr_create + eps_fb_ded_brr %)	status="success", dnn, rat_type="eutra"
Total CSR Attempted	Counter	(%pdn_sess_create%)	status="attempted",dnn
Total CSR Failure/Rejected	Counter	(%pdn_sess_create%)	status="failure",dnn,
Total CSR Success	Counter	(%pdn_sess_create%)	status="success",dnn
Total CBR Attempted	Counter	(%create_bearer_request%)	status="attempted",dnn, fiveqi,rat_type="eutra"
Total CBR failure	Counter	(%create_bearer_request%)	status="failure", fiveqi, dnn, rat_type="eutra"
Total CBR success	Counter	(%create_bearer_request%)	status="success",dnn, fiveqi,rat_type="eutra"
Total CBR retransmission rx	Counter	(%create_bearer_request%)	status="retransmit",dnn, fiveqi,rat_type="eutra"

KPI Name	Type	Description/Formula	Label
Total DBR Attempted	Counter	(%delete_bearer_request %)	status="attempted",dnn, fiveqi,rat_type="eutra"
Total DBR failure/Rejected	Counter	(%delete_bearer_request%)	status="failure", fiveqi, dnn, rat_type="eutra"
Total DBR success	Counter	(%delete_bearer_request %)	status="success", fiveqi, dnn, fiveqi,rat_type="eutra"
Total DBR retransmission tx	Counter	(%delete_bearer_request%)	status="retransmit", dnn, fiveqi, rat_type="eutra"
Total UBR Attempted	Counter	(%update_bearer_ request%)	status="attempted",dnn, fiveqi,rat_type="eutra"
Total UBR failure/Rejected	Counter	(%update_bearer_request %)	status="failure", fiveqi, dnn, rat_type="eutra"
Total UBR Success	Counter	(%update_bearer_ request%)	status="success", fiveqi, dnn, rat_type="eutra"
Total UBR retransmission	Counter	(%update_bearer_request%)	status="retransmit",dnn , rat_type="eutra"
Total EPSFB Dedicated Bearers	Counter	(%eps_fb_ded_brr%)	dnn

5G Subscriber

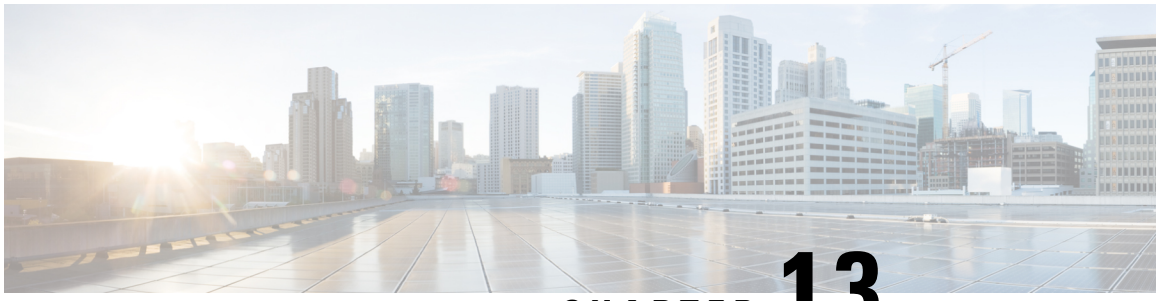
The following table provides details of KPIs related to 5G subscriber statistics.

KPI Name	Type	Description/Formula	Label
Total Active sessions	Gauge	Total number of PDU Contexts (%smf_session_counters%)	dnn,rat_type="nr"
Total Active Flows	Gauge	(%policy_pdu_flows_current%)	dnn,fiveqi,rat_type="nr"
Total Flow Creation Attempted	Counter	(%policy_pdu_flows_total%)	status="attempted",dnn, fiveqi, rat_type="nr"
Total Flow Creation Success	Counter	(%policy_pdu_flows_total%)	status="success",dnn, fiveqi, rat_type="nr"
Total Flow Creation Failure	Counter	(%policy_pdu_flows_total%)	status="failure",dnn, fiveqi, rat_type="nr"

WiFi Subscriber

The following table provides details of KPIs related to WiFi subscriber statistics.

KPI Name	Type	Description/Formula	Label
Total CSR Attempted	Counter	(%untrusted_wifi_to_ enb_handover%)	status="attempted",dnn, rat_type="wlan"
Total CSR failure/Rejected	Counter	(%untrusted_wifi_to_ enb_handover%)	status="failure",dnn, rat_type="wlan"
Total CSR success	Counter	(%untrusted_wifi_to_ enb_handover%)	status="success",dnn , rat_type="wlan"
Total CBR Attempted	Counter	(%create_bearer_request%)	status="attempted", rat_type="wlan"
Total CBR failure	Counter	(%create_bearer_request%)	status="failure", rat_type="wlan"
Total CBR success	Counter	(%create_bearer_request%)	status="success", rat_type="wlan"
Total DBR Attempted	Counter	(%delete_bearer_request%)	status="attempted", rat_type="wlan"
Total DBR failure/Rejected	Counter	(%delete_bearer_request %)	status="failure", rat_type="wlan"
Total DBR success	Counter	(%delete_bearer_request %)	status="success", rat_type="wlan"



CHAPTER 13

Cisco Common Data Layer

Feature Summary and Revision History

Summary Data

Table 34: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 35: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

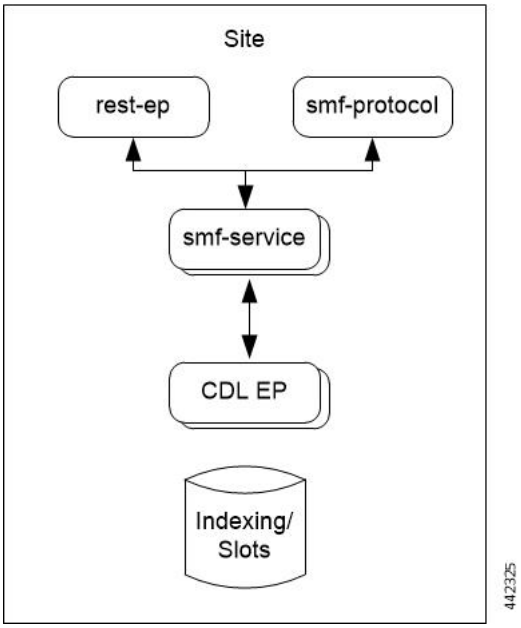
Feature Description

The PCF extends support to the Geo Redundant (GR) version of the Cisco Common Data Layer (CDL). When the primary CDL endpoint fails, PCF attempts the same operation on the next highly rated secondary endpoint thus providing a non-disrupted N7 or Diameter message handling. If the next rated endpoint is unavailable, then PCF reattempts the operation on the subsequent endpoint that has the highest rating and so on.

Architecture

The following figure depicts the failover that happens when the SMF service is unable to access the CDL datastore endpoint.

Figure 22: CDL Datastore Architecture



With relevance to this architecture, you can configure CDL through SMF Ops Center. When the SMF connects to the CDL, it uses the local endpoints.

How it Works

When you configure the CDL in SMF through the SMF Ops Center, SMF gets enabled to support multiple CDL datastore endpoints. You can configure the endpoints by specifying the IP addresses, ports, and assigning ratings to each endpoint. By default, SMF considers the local endpoint as the primary endpoint, which has the highest rating. SMF performs CDL API operations on the primary endpoint. If this endpoint is unavailable, then SMF routes the operations to the next highest rated endpoint. SMF keeps failing over to the accessible secondary endpoint or until all the configured secondaries are exhausted. It does not reattempt a query on the next rated endpoint if the endpoint is reachable but responds with error or timeout.

If SMF is unable to access any of the endpoints in the cluster, then CDL operation fails with the "Datastore Unavailable" error.

Call Flows

This section describes the call flow that is associated with this feature.

• CDL Endpoint Failure Call Flow, on page 163

CDL Endpoint Failure Call Flow

This section describes the SMF local data store endpoint failure call flow.

Figure 23: CDL Endpoint Failure Call Flow

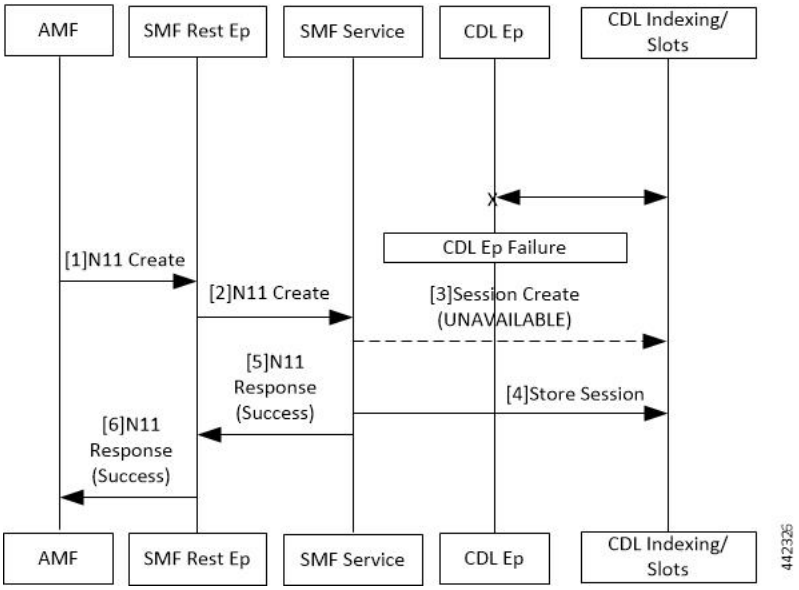


Table 36: CDL Endpoint Failure Call Flow Description

Step	Description
1	The AMF sends a Create Request to SMF REST endpoint over the N11 interface.
2	After receiving the request, the SMF REST endpoint forwards the Create Request to the SMF service.
3	The SMF service attempts to reach the CDL endpoint to send the session creation request. However, the CDL endpoint is unreachable.
4	The Create Request is evaluated in the stored session and the SMF service forwards the request to the CDL endpoint.
5	After the call request is successful, the SMF service notifies the Success Message to the SMF REST endpoint.
6	The SMF REST endpoint forwards the Success Message to the AMF.

Limitations

The CDL configuration in SMF has the following limitations:

- The SMF service attempts to reroute the calls only when it encounters gRPC errors such as UNAVAILABLE. It does not acknowledge errors that the datastore endpoint returns and actual gRPC timeouts such as DEADLINE_EXCEEDED gRPC status code.
- The SMF service does not resolve failures occurring with the datastore such as indexing and slot failures. The CDL layer must resolve these failures and if necessary, send an API call on the remote.

Configuring the CDL Through SMF Ops Center

The configuration of the CDL using SMF Ops Center involves the following steps:

1. Configuring the CDL Session Database and Defining the Base Configuration, on page 164
2. Configuring the Zookeeper in CDL, on page 165

Configuring the CDL Session Database and Defining the Base Configuration

This section describes how to configure the CDL session database and define the base configuration in SMF.

1. From the SMF Ops Center, run the following command to configure the CDL session database and base configuration.

```
configure
   cdl system-id system_id
   cdl node-type node_type
   cdl zookeeper replica zookeeper_replica_id
   exit
   cdl logging default-log-level debug_level
      cdl datastore session
      cluster-id cluster_id
      endpoint replica 1
      endpoint replica num_replica
         index map map_value
         slot replica num_replica
         slot map num_map/shards
         slot write-factor write_factor
         slot notification host host
         slot notification port port
         slot notification limit tps
         index replica num_replica
         index map num_map/shards
         index write-factor write_factor
         end
```

NOTES:

- **cdl system-id** *system_id*: This is an optional command. Specifies the system or Kubernetes cluster identity. The default value is 1.
- **cdl node-type** *node_type*: This is an optional command. Specifies the Kubernetes node label to configure the node affinity. The default value is "session." Accepted length of the value is 0–64 alphabets.
- **cdl zookeeper replica** *zookeeper_replica_id*: Specifies the zookeeper replica server's ID.
- **endpoint replica** *num_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 1. Must be an integer in the range of 1–16.
- **slot replica** *num_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 1. num_replica must be an integer in the range of 1–16.
- **slot map** *num_map/shards*: This is an optional command. Specifies the number of partitions in a slot. The default value is 1. num_map/shards must be an integer in the range of 1–1024.
- **slot write-factor** *write_factor*: This is an optional command. Specifies the number of copies to be written before successful response. The default value is 1. write_factor must be an integer in the range of 0–16. Make sure that the value is lower than or equal to the number of replicas.
- **slot notification host** *host*: This is an optional command. Specifies the notification server hostname or IP address. The default value is datastore-notification-ep.
- **slot notification port** *port*: This is an optional command. Specifies the notification server Port number. The default value is 8890.
- **slot notification limit** *tps*: This is an optional command. Specifies the notification limit per second. The default value is 2000.
- **index replica** *num_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 2. num_replica must be an integer in the range of 1–16.
- **index map** *num_map/shards*: This is an optional command. Specifies the number of partitions in a slot. The default value is 1. num_map/shards must be an integer in the range of 1–1024. Avoid modifying this value after deploying the CDL.
- **index write-factor** *write_factor*: This is an optional command. Specifies the number of copies to be written before successful response. The default value is 1. write_factor must be an integer in the range of 0–16.

Configuring the Zookeeper in CDL

This section describes how to configure the Zookeeper in CDL.

1. Open the Policy Ops Center console and navigate to the datastore CLI.
2. Run the following command to define the parameters.

```
configure
   cdl zookeeper data-storage-size data_storage_size_in_gb
      log-storage-size log_storage_size_in_gb
      replica number_of_replicas
      enable-JMX-metrics boolean_value
```

```
enable-persistence boolean_value
 end
```

NOTES:

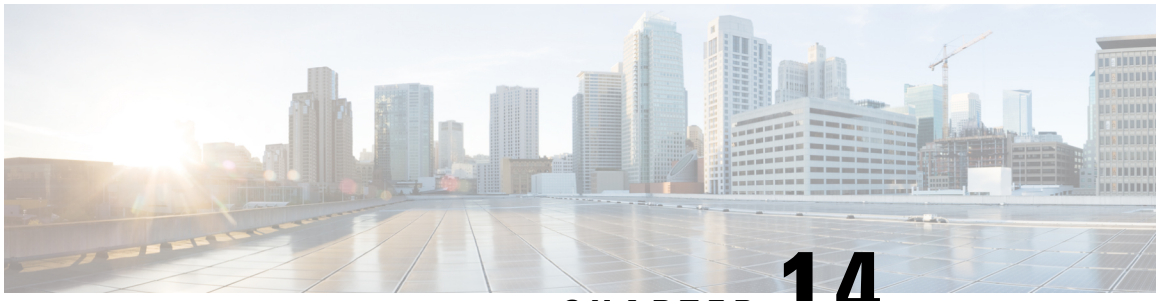
All the following parameters are optional.

- **cdl zookeeper data-storage-size** *data_storage_size_in_gb*: Specifies the size of the Zookeeper data storage in gigabyte. The default value is 20 GB. Accepted value is an integer in the range of 1-64.
- **log-storage-size** *log_storage_size_in_gb*: Specifies the size of the Zookeeper data log's storage in gigabyte. The default value is 20 GB. Accepted value is an integer in the range of 1-64.
- **replica** *num_replicas*: Specifies the number of replicas that must be created. The default value is 3. Accepted value is an integer in the range of one to 16.
- **enable-JMX-metrics** *boolean_value*: Specifies the status of the JMX metrics. The default value is true.
- **enable-persistence** *boolean_value*: Specifies the status of the persistent storage for Zookeeper data. The default value is *false*.

Sample Configuration

This section shows a sample configuration of CDL in a HA environment.

```
cdl system-id system_id
cdl zookeeper replica num_zk_replica
cdl datastore session
 endpoint replica ep_replica
index map index_shard_count
 slot replica slot_replica
 slot map slot_shard_count
exit
```



CHAPTER 14

CHF and PCF Integration for Access and Mobility Procedures

Feature Summary and Revision History

Summary Data

Table 37: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 38: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF leverages the 3GPP provision for the access and mobility procedures. With this provision, the SMF integrates the Charging Function (CHF) and Policy Control Function (PCF). SMF supports the following integration functions:

- CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers—SMF supports this function when a UE moves from one NG-RAN to another NG-RAN for Data Forwarding Tunnel (DFT) and Indirect Data Forwarding Tunnel (IDFT) cases.
- CHF and PCF Integration for N26 4G to 5G Handover—SMF supports the EPS to 5GS procedures with the N26 interface. SMF establishes Uplink (UL) Packet Detection Rule (PDR) or Downlink (DL) PDR toward with the qualified EPS Bearer Identity (EBI) list in 5GS and replicate EBIs to the respective flows. SMF also creates IDFT to support the Downlink forwarding traffic between SGW-U to NR over UPF.
- CHF and PCF Integration for N26 5G to 4G Handover—SMF supports 5GS to EPS procedures with the N26 interface. PGW-C establishes UL PDRs or DL PDRs toward SGW-U with qualified flows in 5GS and replicate EBIs to respective flows. PGW-C also creates an IDFT tunnel to support Downlink forwarding traffic between NR to SGW-U over UPF. Session-Level or Rating-Group level Charging Triggers are received during PDU Session establishment or in response to SMF-initiated Charging Update Request or CHF-initiated Charging Update Notify response in EPS procedures.
- CHF and PCF Integration for Xn Handover—SMF supports the Xn-based inter NG-RAN handover with and without UPF reallocation. The SMF supports Xn handovers for intra-AMF mobility only. SMF processes the received SM context update request that includes the path switch request N2-based message and the access-ide parameters. These parameters identify the CHF and PCF triggers that are received during PDU session establishment.
- CHF and PCF Integration for Service Request Procedures—SMF supports the service requests from both the UE and network-initiated procedures. Either a UE in CM-Idle state or the 5GC uses the Service Request procedure to request the establishment of a secure connection to an AMF. The UE in both the CM-Idle and in CM-Connected state use the Service Request procedure to activate a User Plane connection for an established PDU Session. The UE does not initiate a Service Request procedure if an ongoing Service Request procedure exists.

SMF saves the CHF and PCF triggers that SMF receives from CHF and PCF as part of session creation or PCF or UE-initiated modifications. When a UE triggers access and mobility procedures for the preceding functions, SMF identifies the triggers from CHF and PCF against the received access parameters. Then, SMF sends an update toward CHF and PCF.

How it Works

The SMF integrates the CHF and PCF functions based on the following information:

- Policy control request triggers that are received in the SM policy decision while PDU session is established or PCF or UE initial modification.
- Session-level or rating-group-level charging triggers that are received while PDU session is established or in response to SMF-initiated Charging Update Request or CHF-initiated Charging Update Notify Request.

The SMF supports the following access-side information to detect the PCF and CHF triggers. The SMF sends the trigger information to the CHF and PCF during the N2-based handover.

Table 39: Access-Side Information for PCF and CHF Triggers

Access-Side	CHF-Triggers	PCF-Triggers
UserLocation	USER_LOCATION_CHANGE	SAREA_CH
UeTimeZone	UE_TIMEZONE_CHANGE	SAREA_CH
ServingNetwork	PLMN_CHANGE	PLMN_CH
TargetServingNfId	SERVING_NODE_CHANGE	

Call Flows

This section describes the following call flows:

- CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow
- CHF and PCF Integration for N26 4G to 5G Handover Call Flow
- CHF and PCF Integration for N26 5G to 4G Handover Call Flow
- CHF and PCF Integration for Xn Handover Call Flow
- CHF and PCF Integration for Service Request Procedures

CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow

This section describes the call flow for the CHF and PCF Integration for Intra-AMF and Inter-AMF N2-based handovers.

Figure 24: CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow

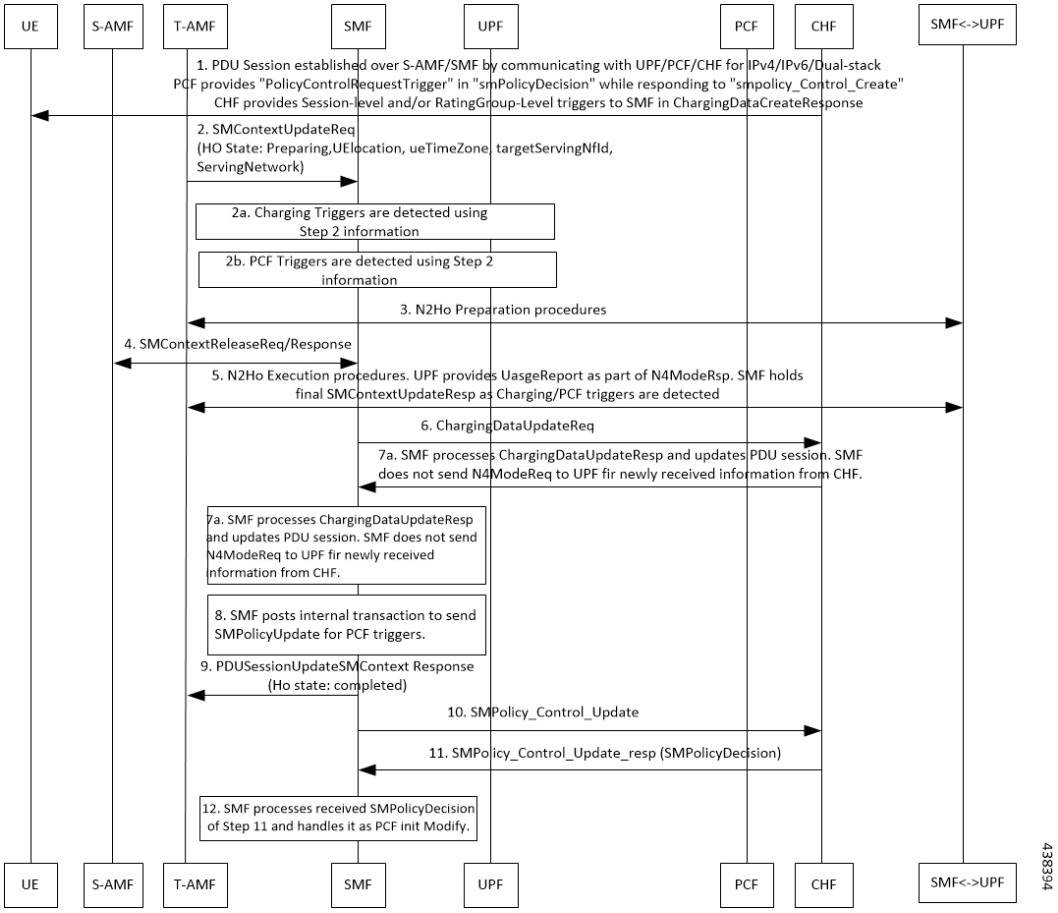


Table 40: CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow Description

Step	Description
1	The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The T-AMF sends SM Context Update Request by including handover state to the SMF. The handover state includes the information on preparation, UE location, UE time zone, target serving NFID, and serving network. The AMF includes target serving NFID information for inter-AMF handoff.
2a	The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.

Step	Description
3	The N2-based Handover Preparation procedure starts from T-AMF towards the SMF and CHF and vice-versa.
4	In the N2-based Handover Execution procedure, in case of inter-AMF handoff, the SMF receives SM Context Release Request from S-AMF and responds with the SM Context Release Response to the S-AMF.
5	In N2-based Handover Execution procedure, the UPF provides the usage report as part of N4 modification response. The SMF holds the final SM Context Release Response when the SMF detects the CHF or PCF triggers.
6	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers with usage report), customer identification, and PDU session charging information.
7	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
7a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
8	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
9	The SMF sends the SM Context Update Response, for which the handover state is complete, to the T-AMF.
10	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update information includes details, such as the user location information, UE time zone, and serving network.
11	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
12	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure.

CHF and PCF Integration for N26 4G to 5G Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for N26 4G to 5G handovers.

Figure 25: CHF and PCF Integration for N26 4G to 5G Handover Call Flow

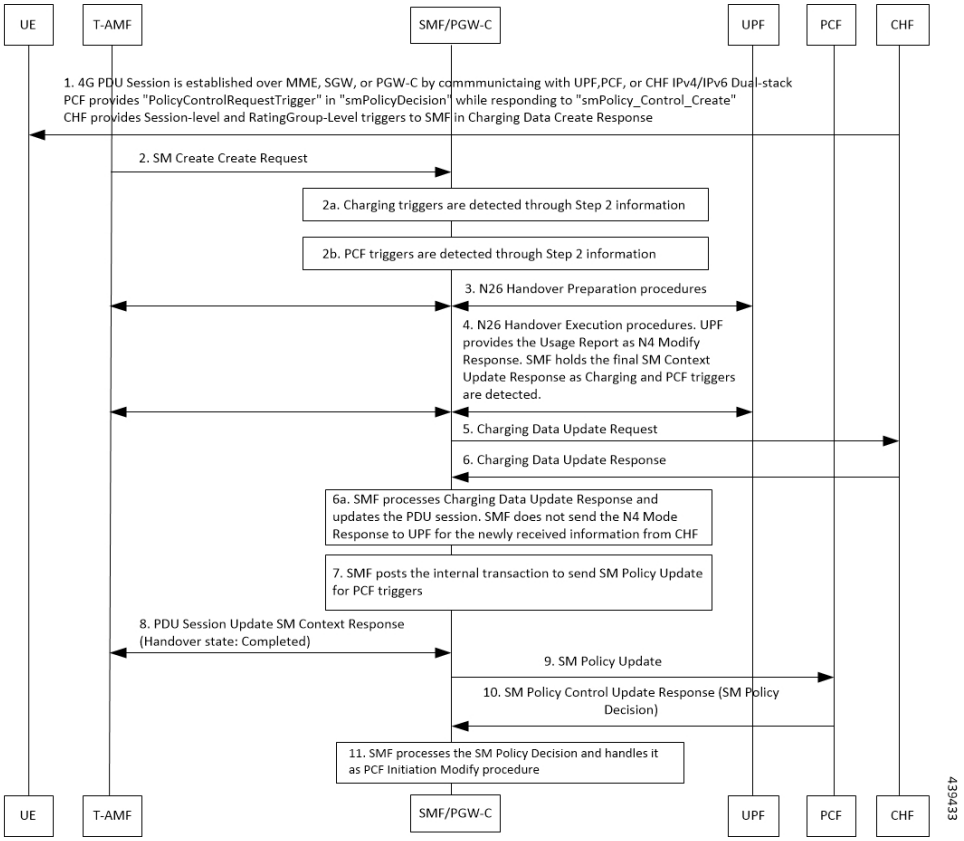


Table 41: CHF and PCF Integration for N26 4G to 5G Handover Call Flow Description

Step	Description
1	The PDU session is established over MME, SGW, and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The T-AMF sends SM Context Update Request by including handover state to the SMF. The SM Context Update Request includes the information on handover state as preparing, UE location, UE time zone, serving NFID, serving network, and RAT type.
2a	The SMF detects access-side changes that are received in the SM Context Create Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.
3	The N26-based Handover Preparation procedure starts from T-AMF toward the SMF or PGW-C and UHF and vice versa, as defined in 3GPP TS 23.502, section 4.1.9.3.

Step	Description
4	In the N26 Handover Execution procedure, the UPF sends the usage report as part of N4 modification response to SMF. The SMF holds the final SM Context Update Response when the SMF detects the CHF or PCF triggers.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
6	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
7	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
8	The SMF sends the SM Context Update Response, for which the handover state is complete, to the AMF.
9	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information, UE time zone, and serving network.
10	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
11	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in 3GPP TS 23.502, section 4.3.3.2.

CHF and PCF Integration for N26 5G to 4G Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for N26 5G to 4G handovers.

Figure 26: CHF and PCF Integration for N26 5G to 4G Handover Call Flow

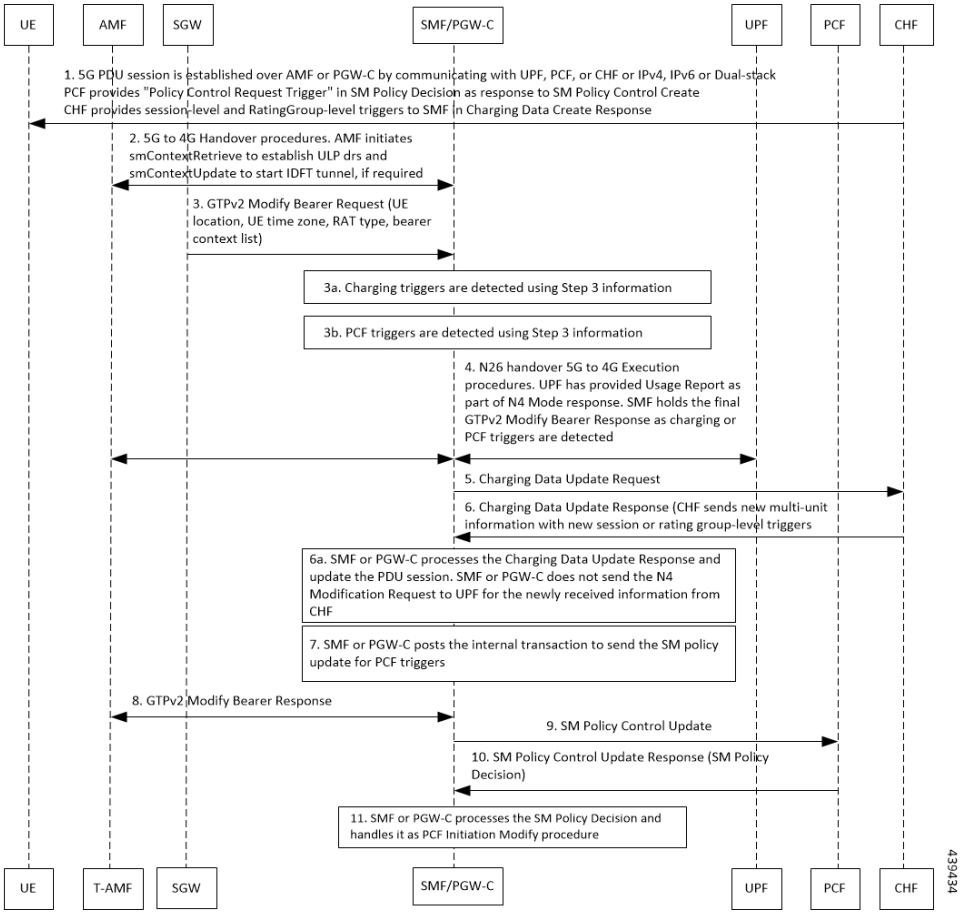


Table 42: CHF and PCF Integration for N26 5G to 4G Handover Call Flow Description

Step	Description
1	The PDU session is established over S-AMF or SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The 5G to 4G Handover procedure starts from AMF toward the SMF or PGW-C and vice versa. AMF initiates the SM Context Retrieve Request to establish the UL PDRs and send SM Context Update Response to start the IDFT tunnel, if necessary.
3	In the N26 5G to 4G Handover Execution procedure, the SGW sends the GTPv2 Modify Bearer Request to PGW-C. This request includes the information on UE location, UE time zone, RAT type, and Bearer Context List.
3a	The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 3.

Step	Description
3b	The SMF detects the PCF triggers with the information that is available in Step 3.
4	In the N26 Handover 5G to 4G Execution procedure, the PGW-C requests UPF to create a GTP-U tunnel for each flow. This tunnel is for the EBIs received in the Bearer Context List of GTPv2 Modify Bearer Request. After the DL PDRs are established, UPF sends the usage report as part of N4 modification response to SMF. The SMF holds the final GTPv2 Modify Bearer Response when the SMF detects the CHF or PCF triggers.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
6	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
6a	The SMF or PGW-C processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
7	The SMF or PGW-C posts the internal transaction to send the SM policy update information for PCF triggers.
8	The SMF or PGW-C sends the SM Context Update Response, for which the handover state is complete, to the AMF.
9	The SMF or PGW-C sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information, UE time zone, and serving network.
10	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
11	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in 3GPP TS 23.502, section 4.3.3.2.

CHF and PCF Integration for Xn Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for the Xn handover.

Figure 27: CHF and PCF Integration for Xn Handover Call Flow

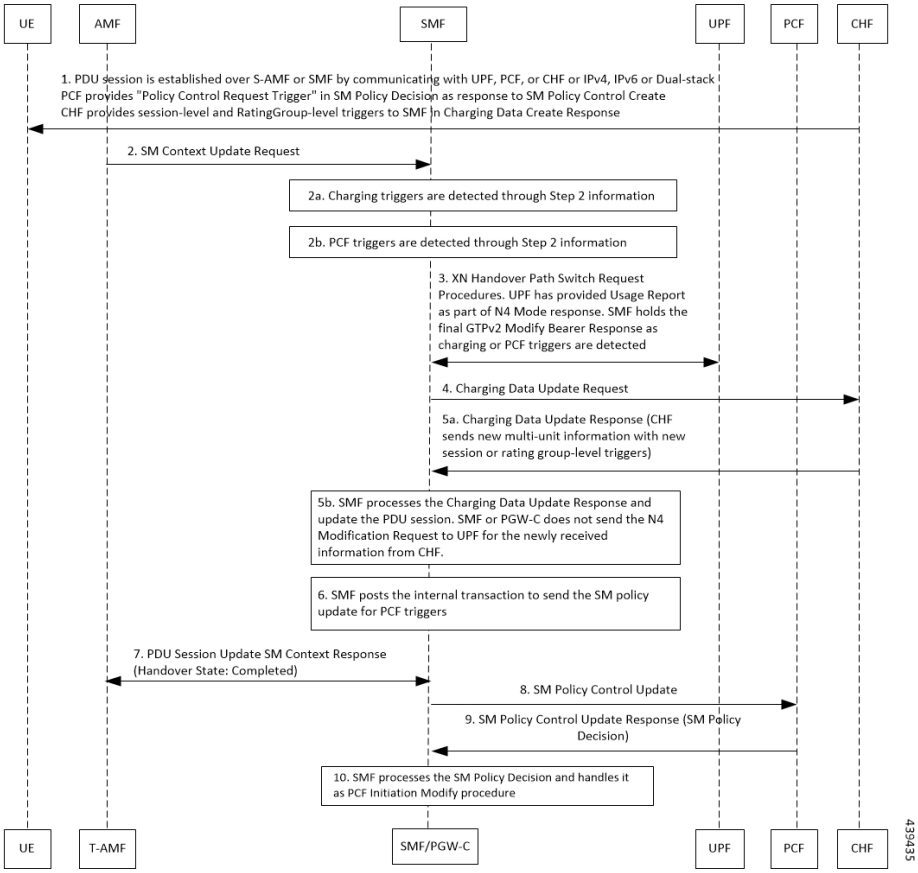


Table 43: CHF and PCF Integration for Xn Handover Call Flow Description

Step	Description
1	The PDU session is established over MME, SGW, and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The AMF sends SM Context Update Request to the SMF. The SM Context Update Request includes the information on UE location, UE time zone, and path switch request N2 message.
2a	The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.

Step	Description
3	The Xn Handover Preparation procedure starts from SMF toward UPF and vice versa, as defined in 3GPP TS 23.502 section 4.9.1.2. SMF sends the N4 Modification Request to UPF and updates the received DL tunnel information of T-gNB. After the tunnel information is updated, UPF provides the usage report as part of N4 modification response. The SMF holds the final SM Context Update Response when the SMF detects the CHF or PCF triggers.
4	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
5	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
5a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
6	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
7	The SMF sends the SM Context Update Response to the AMF. This response includes the path switch request acknowledgment N2 message.
8	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information and UE time zone.
9	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
10	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in 3GPP TS 23.502, section 4.3.3.2.

CHF and PCF Integration for Service Request Procedures

This section describes the CHF and PCF integration for service request procedures.

SMF processes the received SM Context Update Request to update N3 tunnel path state from Idle to Active or Active to Idle. SMF performs the following steps:

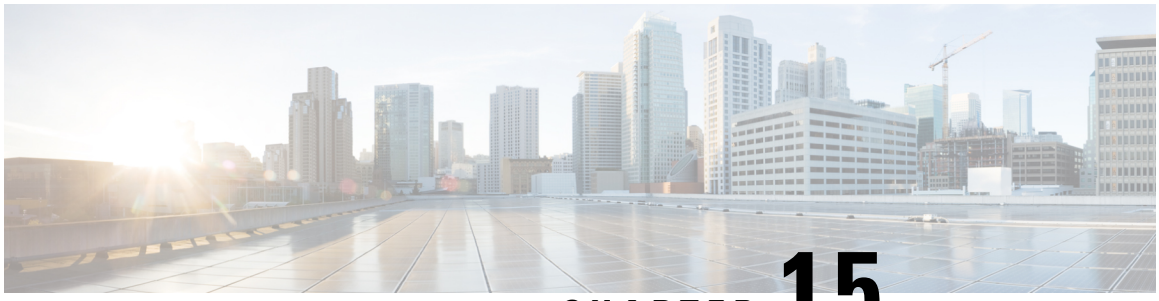
1. When UE is in CM-Idle state at AMF, which is Active to Idle mode—Based on the configuration, SMF updates UPF for N3 tunnel state to drop or buffer by sending the N4 session mode request. Based on charging configuration, SMF receives a usage report. Based on the Charging Triggers that qualify during session creation, SMF sends the N40 Charging Update request.
2. When UE is in CM-Connected state at AMF, which implies SMF receives UE-requested Procedures to change the subscriber N3 Tunnel Path from Idle to Active State—SMF receives the updated user location and UE time zone in the SM Context Update Request. SMF sends the N4 Session Modification Request to UPF to update the DL tunnel details of gNB. Based on charging configuration, SMF receives a usage report. Based on the Charging Triggers that qualify during session creation, SMF sends the N40 Charging Update request.

3. When the N3 Tunnel is unavailable for the Network Service Request Triggers, which implies that UE is in CM-Idle state at AMF—SMF initiates the Network Service Request Procedures for AMF to initiate Paging toward the end user. Then, AMF begins the UE Service Request Procedures to configure the N3 Tunnel as specified in Step 2.

Standards Compliance

The CHF and PCF integration for Intra-AMF and Inter-AMF N2-based handovers feature complies with the following standards:

- 3GPP TS 23.502 V15.2.0 (2018-09)



CHAPTER 15

Content Filtering, Event Detail Records, and X-Header Enrichment Support

Feature Summary and Revision History

Summary Data

Table 44: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 45: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the following functionality:

- Content Filtering
- Event Detail Record (EDR)
- X-header Enrichment

Content Filtering Support

The Content Filtering (CF) service prevents subscribers from inadvertently getting exposed to universally unacceptable content, or content that is inappropriate as per subscriber preferences. Based on the URLs in the subscriber requests, the CF service filters HTTP and WAP requests from mobile subscribers. Operators can filter and control the content for an individual subscriber to access.

The CF service provides the following solutions:

- URL Blacklisting—In this solution, all HTTP or WAP URLs in subscriber requests must match against a database of "blacklisted" URLs. If there is a match, it discards the flow, redirects, or terminates as per the configuration. In case of no match, subscribers view the content as usual.

  URL Blacklisting may not be a subscriber opt-in service. Operators can enable URL Blacklisting either for all subscribers or for a subset of subscribers. Typical cases include applying a blacklisted database of child porn URLs to all subscribers so that they are inadvertently not exposed to the universally unacceptable content.

- Category-based Static Content Filtering—In this solution, all HTTP or WAP URLs in subscriber requests must match against a static URL categorization database. Action initiates based on the URL's category and as per the configuration in the subscriber CF policy. Possible actions include:
  - Permitting
  - Blocking
  - Redirecting
  - Inserting content

EDR Support

EDRs are usage records with support to configure content information, format, and generation of triggers by the system administrative user. The EDRs are generated according to explicit action statements in rule commands. Several EDR schema types, where each schema type includes a series of analyzer parameter names, exist in the EDR. The EDRs are generated in CSV format at the time of each event.

The EDRs are stored in timestamped files that you can download through SFTP from the configured context. The EDRs are generated on per flow basis, and they catch whatever bytes get transmitted over that flow including those retransmitted.

Metadata Provided by SMF for EDR

The SMF provides the following metadata to the User Plane Function (UPF), which includes the data in the generated EDRs:

- Called-Station-ID: Specifies the DNN for the session
- Calling-Station-ID: Specifies the MSISDN of the UE
- RAT Type: RAT type for the current session (NR or EUTRAN)
- ULI: User location for the current session

The UPF receives the above data in the "Subscriber Parameters" IE in the PFCP Session Establishment Request message. The RAT type and ULI can change during the lifetime of session (for events, such as 5G to 4G handover). The UPF receives the changed values of these parameters in the PFCP Session Modification Request message.

NOTES:

- All the parameters are always sent from the SMF to the UPF irrespective of EDR configuration being available. These parameters ensure that any change in configuration after the session creation is immediately applied on the UPF.
- The SMF supports EDR-related configurations. However, the SMF does not require these configurations for its functionality. These configurations are sent to the UPF through RCM.

X-Header Insertion Support

With the X-Header Insertion and X-Header Encryption features, collectively known as Header Enrichment, you can append headers to HTTP or WSP GET and POST request packets, and HTTP response packets for use by end applications. For example, mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on.

Supported X-Header Information

Out of all the configurable X-header information, some information requires control plane (SMF) to send the corresponding values to the user plane (UPF). The following table lists the information that is sent from the SMF to the UPF for X-header Insertion support.

Xheader Field	Description	Present in Session Establishment	Modified in Session Modification
String Constant	Inserts the configured string in xheader	N/A	N/A
Charging ID	Per Flow/Bearer Charging Id	Yes	N/A
IMEI	IMEI for the call	Yes	N/A
IMSI	IMSI for the call	Yes	N/A
Rat-Type	RAT type for the UE session	Yes	Yes
s-mcc-mnc	MCC/MNC of the SGW/AMF	Yes	N/A
Sgsn-address	AMF/SGW address	Yes	Yes
ULI	User Location Info	Yes	Yes
GGSN-Address	N4/S5 endpoint of SMF	Yes	Yes
Radius-station-ID	MSISDN of the UE	N/A	N/A
Sn-rulebase	Rulebase for a call	Yes	Yes
Subscriber-ip-address	IP address allocated to UE	N/A	N/A
Msisdn-no-cc	Obtained from MSISDN	Yes	No

The subscriber-specific fields—IMSI, MSIDN, and IMEI—are encoded in the "User ID" standard IE. See, 3GPP 29.244, Section 8.2.101 for more information.

Rest of the fields are sent in the "Subscriber Parameters" proprietary AVP. Some fields, such as the "Rulebase" and "UE IP address", are sent as a part of the created PDRs.

NOTES:

- All the parameters are always sent from the SMF to the UPF irrespective of whether X-header configuration is available. These parameters ensure that any change in configuration after session creation is immediately applied on the UPF.
- The SMF supports X-header Insertion-related configurations. The SMF does not require these configurations for its functionality. These configurations are sent to the UPF through the RCM.

Configuring Content Filtering, EDR, and X-Header Insertion Support

This section describes how to configure the following:

- Content Filtering
- Event Detail Records (EDRs)
- X-Header Enrichment

Configuring Content Filtering Support

This section describes how to configure CF support.

NOTE: Apart from the following configurations, all other configurations are used only in the UPF, and are only sent from the SMF to the UPF via RCM. The SMF does not use these configurations.

Configuring Content Filtering under Active Charging Service

To configure CF support under the active charging service, use the following configuration:

```
configure
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
         analyze priority priority { all | category category | x-category
xcategory } action { allow | content-insert content_string | discard |
redirect-url url | terminate-flow | www-reply-code-and-terminate-flow
reply_code } [ edr edr_format ] failure-action { allow | content-insert
content_string | discard | redirect-url url | terminate-flow |
www-reply-code-and-terminate-flow reply_code } [ edr edr_format ]
         end
```

Configuring Content Filtering under Rulebase

To configure CF under the rulebase, use the following configuration:

```
configure
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
      content-filtering mode category static-only
      end
```

Configuring Content Filtering under APN

To configure CF under the APN, use the following configuration:

```
configure
   context context_name
      apn apn_name
         content-filtering category policy-id cf_policy_id
         end
```

Content Filtering Policy ID on N7 Interface

The CF categories are configured under the active charging service under specific policy IDs. The rulebase and APN also have an associated policy ID. For any session, one policy ID can be associated with the session at anytime. The categories configured under that CF policy ID are applicable for the session on the UPF.

The PCF can override the CF policy ID by sending this value on the N7 interface. For this purpose, a proprietary IE is available in the YAML definition for the N7 interface. The hierarchy for the CF policy ID is as follows:

```
smPolicyDecision
   ciscoAvpSet:
      cfPolicyId: uint32 value
```

When the PCF does not send a CF policy ID, the existing CF policy ID in the rulebase configuration or the policy ID configured in the APN configuration is selected, in the order of precedence. This CF policy ID value is sent to the UPF in PFCP Session Establishment Request message in the "Subscriber Parameters" attribute. During PDU Session Modification, if the PCF changes the CF policy ID, the ID is sent to the UPF in PFCP Session Modification Request message.

Configuring EDR Support

The SMF supports EDR-related configurations. The SMF does not require configurations for EDR functionality. The required configurations are sent to the UPF through RCM.

To configure the EDR formats, use the following configuration:

```
configure
   active-charging service acs_service_name
      edr-format edr_format_name
         attribute attribute_name { [ format { MM/DD/YY-HH:MM: SS |
MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } ]
 [ localtime ] | [ { ip | tcp } { bytes | pkts } { downlink | uplink } ]
 priority priority_value }
         rule-variable protocol rule priority priority
         event-label event_label priority  priority
         delimiter { comma | tab }
         end
```

Configuring X-Header Insertion Support

The SMF supports X-Header Insertion-related configurations. The SMF does not require configurations for X-Header Insertion functionality. The required configurations are sent to the UPF through RCM.

Configuring an X-Header Format

To create and/or configure an x-header format, use the following configuration:

```
configure
   active-charging service acs_service_name
      xheader-format xheader_format_name
        insert xheader_field_name { string-constant xheader_field_value | variable
 { bearer { 3gpp { apn | charging-characteristics | charging-id | imei |
```

```
 imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id
| ggsn-address | mdn | msisdn-no-cc | radius-string |
radius-calling-station-id | session-id | sn-rulebase |
subscriber-ip-address | username } [ encrypt ] | http { host | url } }
         end
```

Configuring Charging Action for Insertion of X-Header Fields

To configure a charging action for insertion of x-header fields, use the following configuration:

```
configure
   active-charging service acs_service_name
      charging-action charging_action_name
         xheader-insert xheader-format xheader_format_name [ encryption {
rc4md5 | aes-256-gcm-sha384 [ salt ] } [ encrypted ] key key ] [
first-request-only ] [ msg-type { response-only | request-and-response }
 ] [ -noconfirm ]
         end
```

Bearer QCI Support

Feature Description

The User Plane function (UPF) requires the Bearer level information (BLI) for each QoS flow like QFI for 5G and Bearer Id for 4G, 5G QoS Identifier (5QI) allocation and retention priority (ARP), and Charging ID, to support inline services. The Bearer QCI Support feature facilitates this requirement with the SMF.

Note The Bearer QCI Support feature also includes support for Bli_ID and QFI values in the “Create PDR” message.

The SMF sends the Bearer QoS Class Identifier (QCI) Information Element (IE), which is cisco proprietary IE, in the PFCP session establishment request and PFCP session modification request. The UPF implicitly derives the deletion indication. If a BLI ID is no longer associated with any PDR, the UPF removes it from the PFCP session context. The UPF adds the 5QI or QCI value in the EDR. Currently, the Bearer QCI field is used for 5G to add the 5QI.

The BLI is reported to the UPF as shown in the following table. The formats and encoding and decoding of these IEs are the same as other 3GPP IEs as described in TS 29.244.

Information Elements	Mandatory /Optional	Data Type	Description
valid		guint8	Validity of the Bearer level information IE
bli_id	Mandatory	PfcpBliId	QoS flow identifier (QFI) of 5G or Bearer ID (4G)

qci	Optional	PfcpQci	Used by PGW-C, not relevant for SMF
_5qi	Optional	Pfcp5qi	5QI associated with the QoS flow
arp	Mandatory	PfcpArp	ARP comprises of pre-emption capability, Pre-emption vulnerability, and priority level.
charging_id	Optional	PfcpChargingId	Charging ID associated with the QoS flow or Bearer (or both).

Bearer Level Information ID

The unique ID for each Bearer level information sent from SMF. The recommended value of this IE is QFI (in 5G) or Bearer-id (in 4G). The format of IE is as below:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 232 (decimal)							
3 to 4	Length = 1							
5	BLI_ID value							
6 to n+4	These octets are present only if explicitly specified							

QCI : This is not applicable for 5G. It is used in CUPS, if required.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 233 (decimal)							
3 to 4	Length = 1							
5	QCI value							
6 to n+4	These octets are present only if explicitly specified							

5QI: The SMF uses this this IE to send the 5QI value.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 234 (decimal)							
3 to 4	Length = 1							

5	5QI value
6 to n+4	These octets are present only if explicitly specified

ARP: The ARP value is sent with this IE.

Note From SMF, the ARP value is encoded as arp->pci)<<4) | arp->pl)<<2)| arp->pvi)

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 235 (decimal)							
3 to 4	Length = 1							
5	ARP value							
6 to n+4	These octets are present only if explicitly specified							

Charging ID: The Charging IE is sent with this IE.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 236 (decimal)							
3 to 4	Length = 1							
5	Charging Id value							
6 to n+4	These octets are present only if explicitly specified							

Triggers for Bearer Level Information IE

The following are the triggers for sending the BLI IE in PFCP messages:

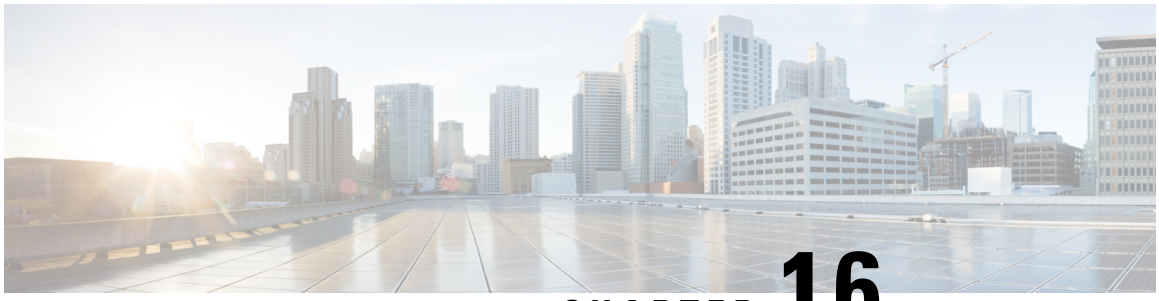
PFCP Session Establishment Message

The Bearer level information IE is sent for each new QoS flow with the unique QFI ID. This IE is added in the policy decision in the N7 Policy Control Create Response message from the PCF. Therefore, SMF sends multiple instances of this IE, in a single PFCP message.

PFCP Session Modification Message:

Any new QoS flow addition or new PCC rule referring to an existing QoS flow that results in a new QER or PDR IE that has a new Bearer level information IE for each unique QFI ID.

The BLI IE is not included in the PFCP Session Modification Message if the modification is for IDFT tunnels.



CHAPTER 16

Customization of StarOS-based UPF on N4 Interface

Feature Summary and Revision History

Summary Data

Table 46: Feature Summary

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 47: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The initial trials for SMF are planned using the StarOS-based UPF node that is already available. The SMF must meet some non-standard requirements on the UPF node to interwork with this UPF.

Important Currently, the SMF does not support the Node Level Report Messages from the UPF.

Support for Prime PFD Message

The StarOS-based UPF node needs basic ECS rules configuration pushed from SMF. These default rules need to be provisioned in UPF dynamically even for dynamic PCC policy.

- The StarOS UPF expects SMF to send the configuration in a new custom message. This message is called SX_PRIME_PFD_MANAGEMENT_REQUEST. The custom message ID of this message is 0x2F.
- The response sent by UPF for this message is SX_PRIME_PFD_MANAGEMENT_RESPONSE with message ID 0x30.

The following snapshot shows the contents of this message:

```
[U-PLANE]PFCP Rx PDU, from 192.60.181.6:40259 to 192.60.181.2:8805 (81)
SEID: NA, Message type: SX_MSG_PRIME_PFD_MANAGEMENT_REQUEST (0x2F)
Sequence Number: 0x000001 (1)
PFCP HEADER
        Version number: 1
        SEID flag: Not present
        Message Length: 0x004D (77)
INFORMATION ELEMENTS
        CONFIG ACTION:
            Type: 202  Length: 1
            Value: ADD
            Hex: 00CA 0001 01
        CORRELATION ID:
            Type: 203  Length: 2
            Value: 4
            Hex: 00CB 0002 0004
        SUB PART NUMBER:
            Type: 204  Length: 1
            Value: 245
            Hex: 00CC 0001 F5
        CONTENT TLV:
            Type: 206  Length: 53
            Value:
                Content Type: ACS_LEVEL_INFO
                Content Length: 50
            Hex: 00CE 0035 0B00 325C 00F1 015F 5F64 657F
                 6661 756C 745F 5F10 0113 2C01 0111 C801
                 132C 0101 132C 0101 532C 0101 0155 01FF
                 01FF 0101 1001 032C 01
Tuesday August 21 2018
<<<<OUTBOUND  09:43:39:380 Eventid:221302(3)
[U-PLANE]PFCP Tx PDU, from 192.60.181.2:8805 to 192.60.181.6:40259 (19)
SEID: NA, Message type: SX_MSG_PRIME_PFD_MANAGEMENT_RESPONSE (0x30)
Sequence Number: 0x000001 (1)
```

```
PFCP HEADER
        Version number: 1
        SEID flag: Not present
        Message Length: 0x000F (15)
INFORMATION ELEMENTS
        CAUSE:
            Type: 19  Length: 1
            Value:
                Cause: PFCP_CAUSE_REQUEST_ACCEPTED (0x01)
            Hex: 0013 0001 01
        CORRELATION ID:
            Type: 203  Length: 2
            Value: 4
            Hex: 00CB 0002 0004
```

Dynamic IP Pool Provisioning on UPF

The StarOS UPF expects SMF to send the configured IP pool range for assigning the IP address to UE during PDU Session Creation. The UPF uses this information to install static routes for the entire range of IP addresses and advertises the same. The IP pool range information consists of:

- Start and End IP address of the pool range.
- VPN context ID in which the pool will be dynamically configured in UPF.
- SMF does not have any VPN ID supported in this release. It sends a configured value that also needs to be configured on UPF.
- IP pool chunk ID.

  SMF currently does not break the pool into smaller chunks and hence, it always sends 1 as the chunk ID.
- The IP pool information is sent to UPF in an N4 Association Update Request message after the N4 Association Setup Request/Response has been successfully exchanged with UPF and also after the SX Prime PFD Management Request/Response has been exchanged. The Content TLV IE (IE type 206) is used to send this pool information in the N4 Association Update Request.

Absence of NodeID Attribute from N4 Messages

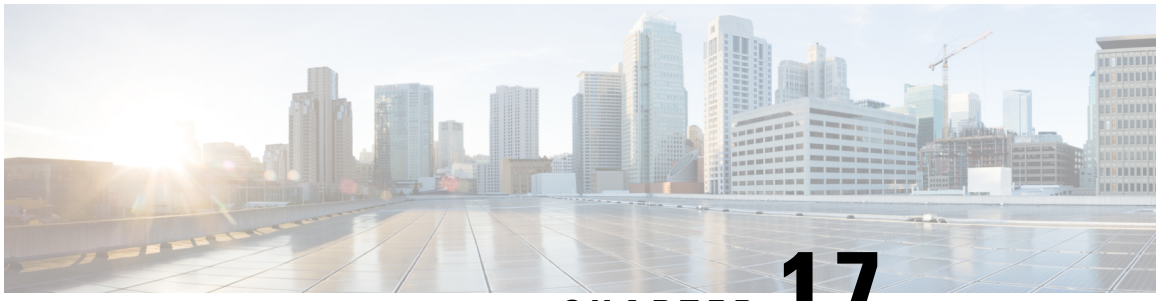
As per 3GPP specifications, the NodeID attribute uniquely identifies an SMF to a UPF. This IE is a mandatory attribute in the N4 Session Establishment Request/Response message. The StarOS UPF currently does not support this IE in any of the Session Management related messages. As a customization, the SMF does not send this IE and does not expect this IE in the response messages.

Non Standard Attribute Type

As per 3GPP specifications, the FAR ID attribute has an ID type 108. The StarOS UPF assumes this IE type as 200. As a customization, the SMF sets 200 as the FAR ID IE type.

Single QFI Support

As per 3GPP specifications, the PDR sent to UPF may have a list of QFIs associated to all the QERs. The StarOS UPF currently supports only one QFI. As a customization, the SMF includes only one QFI.



CHAPTER 17

DNS Proxy Integration

Feature Summary and Revision History

Summary Data

Table 48: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 49: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The Domain Name System (DNS) is a network of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice-versa. The DNS Proxy allows you to configure the proxy servers

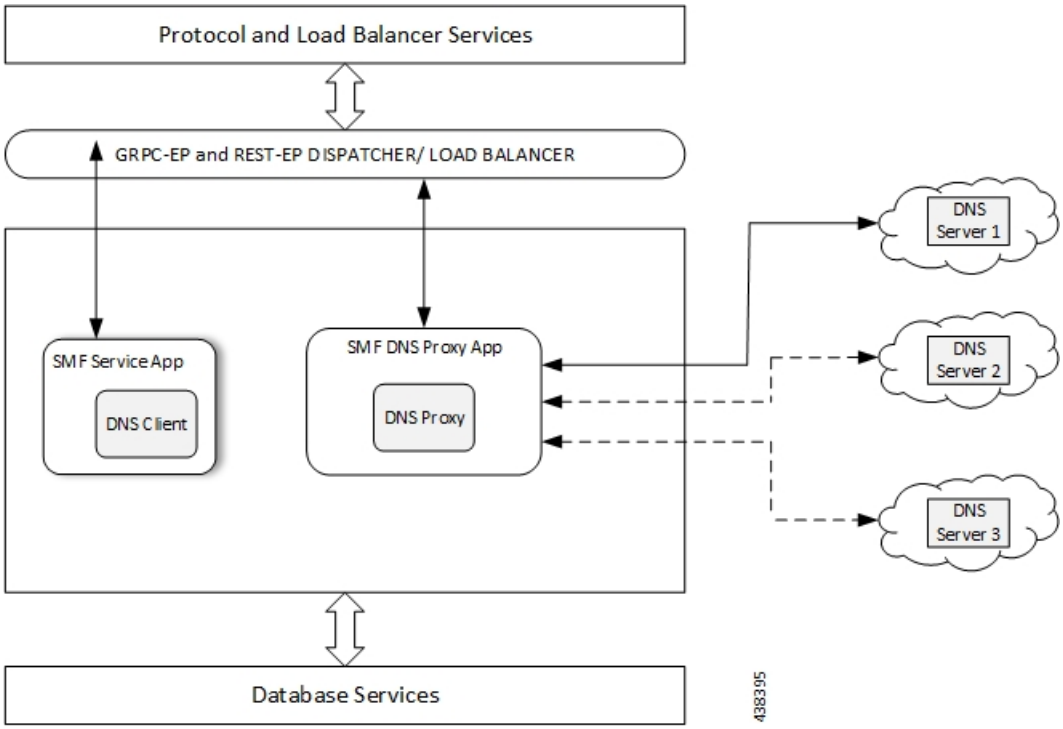
(one or more) for resolving the host names. The DNS queries – for resolving host names to their IP addresses – are sent to the configured DNS servers through the DNS proxy servers.

The DNS proxy feature is integrated in the SMF network function.

How it Works

The DNS proxy feature is integrated in the SMF cluster. For sending the list of host names to resolve the DNS Proxy server, the SMF Client Library calls the smfdnsclnt.DNSLookupRequest() Request. The DNS Proxy server forwards the request to the Open source DNS package for host name to IP address resolution.

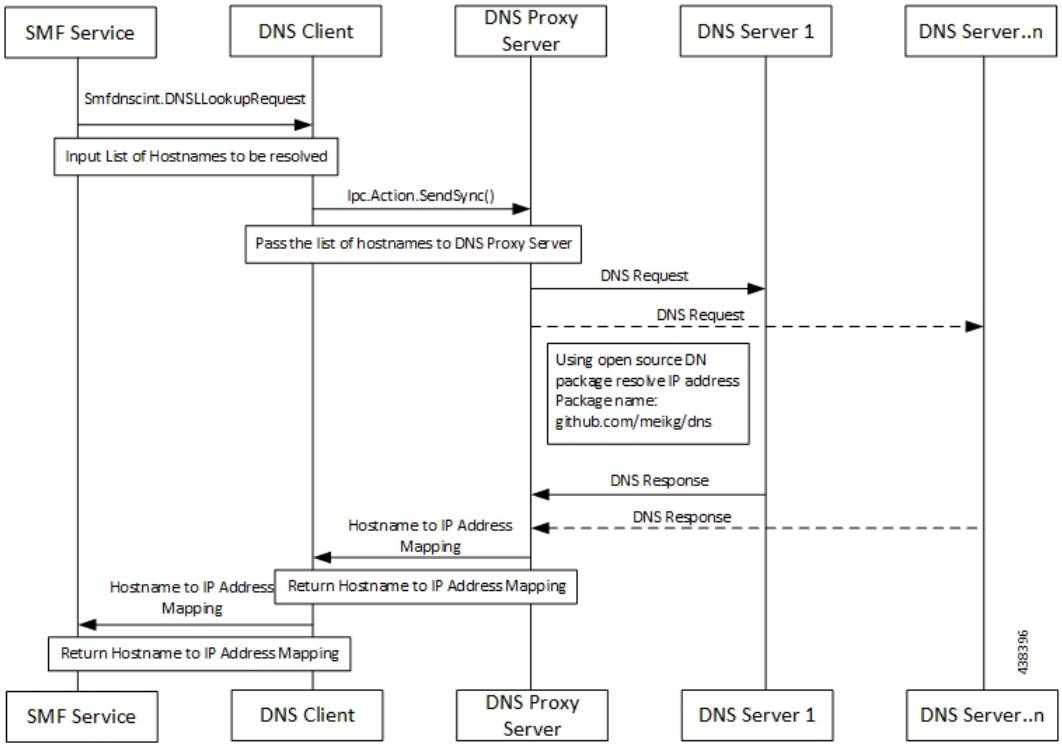
Figure 28: DNS Proxy Feature Integration



Call Flows

The following call flow illustrates the communication between the DNS client and the Proxy server.

Figure 29: DNS Client and Proxy Server Communication Call Flow



Configuring the DNS Proxy Feature

This section describes how to configure the DNS proxy feature.

Configuring the DNS proxy feature involves the following steps:

1. Configuring SMF DNS proxy replica
2. Configuring SMF DNS proxy

Configuring SMF DNS Proxy Replica

Use the following configuration to configure the SMF DNS proxy replica.

```
configure
  k8 smf profile dns-proxy no-of-replicas integer
  commit
  end
```

NOTES:

- **k8 smf profile dns-proxy no-of-replicas** *integer* : Specifies the number of replicas of the DNS proxy pod.

- **commit**: Commits the configuration.

Configuring SMF DNS Proxy

Use the following configuration to configure the SMF DNS proxy feature.

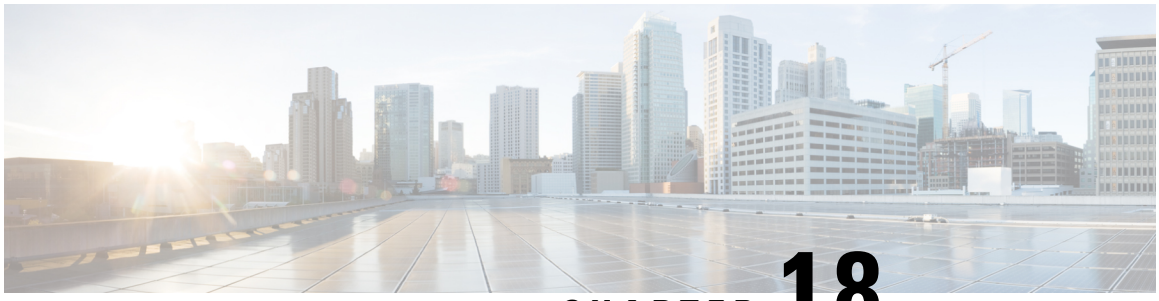
```
configure
   profile dns-proxy
      timeout integer
      query-type { ipv4v6 | ipv4 | ipv6 }
      servers string
      ip string
      port integer
      priority integer
      protocol { tcp | udp }
      commit
```

NOTES:

- **profile dns-proxy** – Enters the DNS Proxy Configuration mode.
- **timeout***integer* – Specifies the client timeout value.
- **query-type** – Specifies the DNS query type.
- **servers** *string* – Specifies the name of the DNS server. For example, serv1.
- **ip** *string* – Specifies the IP address of the DNS server.
- **port** *integer* – Specifies the priority of the DNS server.
- **protocol** – Specifies the protocol of the DNS server.
- **commit** – Commits the configuration.

The following is an example configuration where two DNS servers – serv1 and serv2 – are configured:

```
show running-config profile dns-proxy profile1
   query-type ipv4
   timeout 5
   servers serv1
   ip 10.105.227.227
   port 53
   protocol tcp
   priority 1
   exit
      servers serv2
      ip 10.105.227.228
      port 20
      protocol udp
      priority 2
      exit
exit
```



CHAPTER 18

DSCP Marking

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

DSCP Marking supports granular configuration of DSCP. For Interactive Traffic Class (ITC), the SMF supports per-APN configurable DSCP marking for Uplink and Downlink direction that is based on 5QI and ARP-Priority level. This allows users to assign different DSCP values for flows with the same 5QI but different ARP priority values. For example, the ability to assign DSCP values that are based on 5QI+ARP can be used to meet compliance on priority and emergency calling via VoLTE.

DSCP Marking is a CLI-controlled feature, which enables to create and map 5QI and ARP values to enforceable QoS parameters.

How it Works

Allocation of different DSCP values for flows with the same 5QI, but different ARP values, works as follows:

- Allows DSCP marking of packets that is based on 5QI+ARP combination.
- 5QI+ARP configuration overrides any pre-entry of DSCP marking of packets that was based on 5QI+ARP combination.
- 5QI-only DSCP entry overrides all existing 5QI+ARP configuration.
- Allows implementation of associated DSCP marking for 5QI+ARP for Uplink and Downlink functionality.

Configuring 5QI-QoS Mapping

Use the following CLI commands to create and map 5QI values to enforceable QoS parameters.

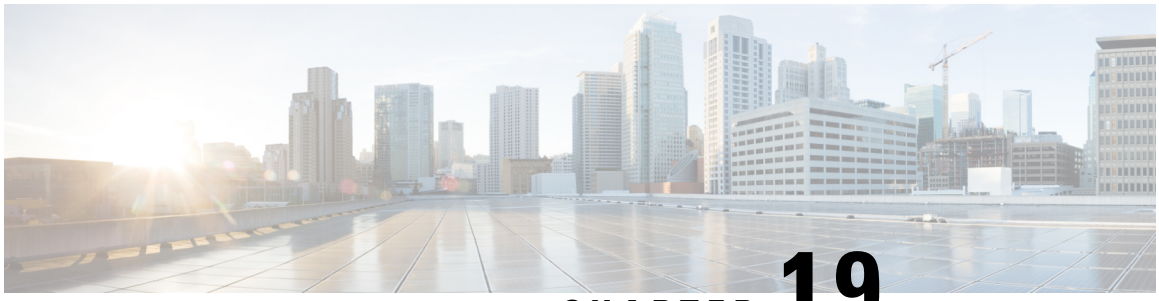
```
configure
   profile qos qos_name
      dscp-map qi5 qi5_value [ arp-priority-level arp_value ] uplink
user-datagram dscp-marking dscp_marking_value
      dscp-map qi5 5qi_value [ arp-priority-level arp_value ] downlink {
encaps-header { copy-inner | dscp-marking dscp_marking_value } | user-datagram
 dscp-marking dscp_marking_value encaps-header { copy-inner | dscp-marking
dscp_marking_value } }
      commit
```

NOTES:

- **dscp-map**: Configures 5QI (referred as qi5 in the code) to DSCP-Marking mapping.
- **qi5** *5qi_value*: Identifier for the authorized QoS parameters. The *5qi_value* must be within the range of 0 through 255.
- **arp-priority-level** *arp_value*: Configures the ARP Priority Level. The *arp_value* must be an integer from 1 through 15.
- **downlink**: Configures the downlink traffic.
- **uplink**: Configures the uplink traffic.
- **user-datagram**: Specifies the DSCP value to be applied to user datagram. Use this keyword to set the DSCP in the inner IP header in uplink/downlink direction.
- **dscp-marking**: Specifies the DSCP value to be applied to packets with this 5QI. The dscp_marking_value must be a hexadecimal number from 0x00 through 0x3F.
- **encaps-header**: Configures the DSCP value to be applied to encaps header. Use this keyword to set the DSCP in the outer-ip header in downlink direction.
- **copy-inner**: Copies the DSCP value from inner IP header to the outer IP header.

- The following is a sample configuration.

```
profile qos test
 dscp-map qi5 1 downlink encaps-header copy-inner
 dscp-map qi5 1 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 2 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 3 downlink user-datagram dscp-marking 0x3b encaps-header copy-inner
 dscp-map qi5 4 downlink user-datagram dscp-marking 0x3b encaps-header dscp-marking
0x3f
 dscp-map qi5 2 uplink user-datagram dscp-marking 0x3b

 dscp-map qi5 1 arp-priority-level 1 downlink encaps-header copy-inner
 dscp-map qi5 2 arp-priority-level 2 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 4 arp-priority-level 3 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 2 arp-priority-level 4 downlink user-datagram dscp-marking 0x3b
encaps-header copy-inner
 dscp-map qi5 4 arp-priority-level 5 downlink user-datagram dscp-marking 0x3b
encaps-header dscp-marking 0x3f
 dscp-map qi5 4 arp-priority-level 5 uplink user-datagram dscp-marking 0x3b
```



CHAPTER 19

EPS Interworking

Feature Summary and Revision History

Summary Data

Table 50: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 51: Revision History

Revision Details	Release
New CLI command is added in DNN profile configuration to reject calls from 4G-only UE devices.	2020.02.1
First introduced.	Pre-2020.02.0

Feature Description

The SMF implements the 3GPP recommendations for interworking of Evolved Packet System (EPS) and 5G Core Network (5GC).

The UEs capable of supporting both 4G and 5G NAS connect to the Evolved Terrestrial Radio Access Network (E-UTRAN) and the 5GC network. The SMF with the EPS interworking capability acts as a PGW-C+SMF and uses the S5/S8 interface with S-GW to receive the 4G Session Creation Request. All the other interfaces involved in the 4G Session Creation (for example, Gx, Gy, Gz, and so on) are replaced by the corresponding 5GC Service Based Interfaces (Npcf and Nchf).

After a PDU session is created on the PGW-C+SMF with E-UTRAN, Mobility Management Entity (MME) and Serving Gateway (S-GW), the UE can hand over E-UTRAN to 5G New Radio (NR) and vice-versa.

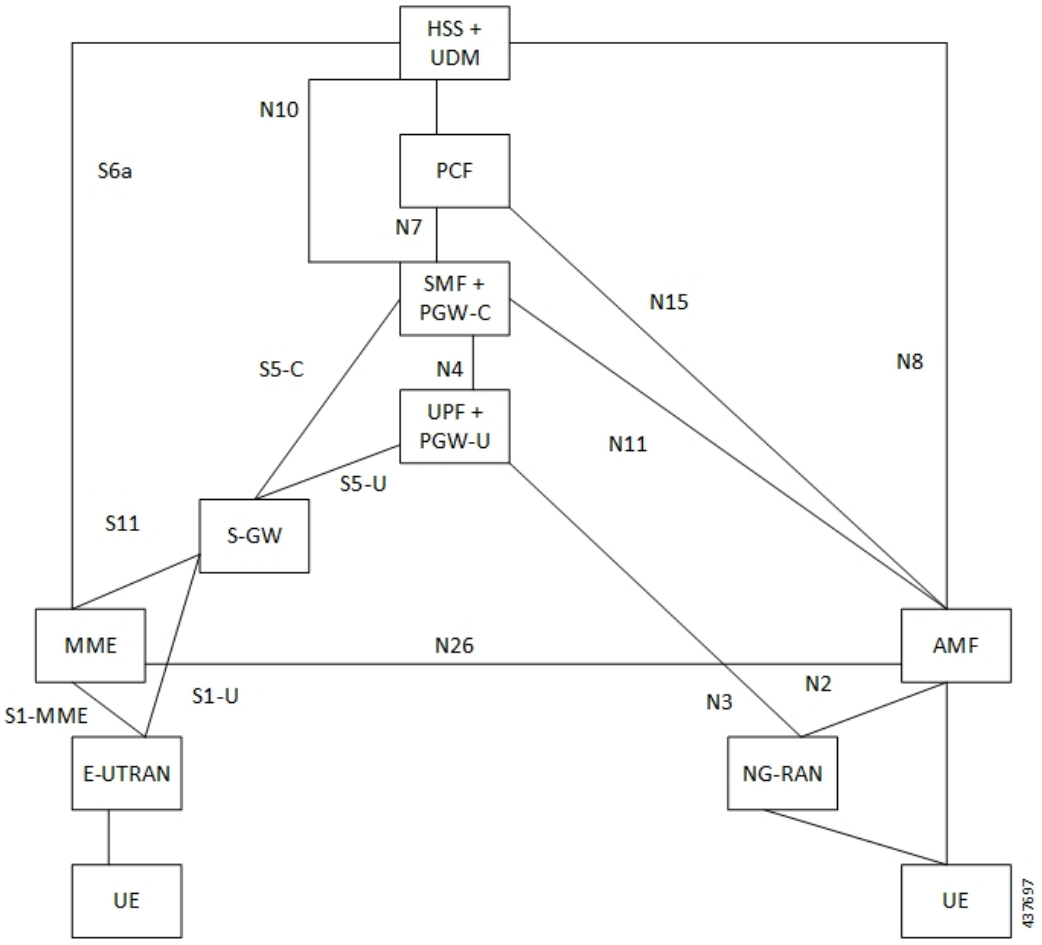
The SMF currently supports interworking with EPS using N26 interface. N26 interface is an inter-CN interface between the MME and 5GS AMF to enable interworking between Evolved Packet Core (EPC) and the NG core networks. Support of N26 interface in the network is optional for interworking. N26 supports a subset of the functionalities over S10 interface to enable interworking.

The UE uses EPC NAS or 5GC NAS procedures depending on the core network by which it is served.

Architecture

The following figure shows the network architecture for the EPS-5G Core interworking.

Figure 30: 3GPP Non-Roaming Architecture for EPS-5GC Interworking



How it Works

A UE that supports only EPS based Dual Connectivity with secondary RAT NR:

- always performs initial access through E-UTRA (LTE-Uu) but never through NR
- performs EPS NAS procedures over E-UTRA (i.e. Mobility Management, Session Management etc.) as defined in 3GPP specification 24.301

A UE that supports camping on 5G Systems with 5GC NAS:

- Performs initial access either through E-UTRAN that connects to 5GC or NR towards 5GC
- Performs initial access through E-UTRAN towards EPS, if supported and needed
- Performs EPS NAS or 5GC NAS procedures over E-UTRAN or NR respectively (that is, Mobility Management, Session Management, and so on) depending on whether the UE requests 5GC access or EPS access, if the UE also supports EPS NAS

For interworking with EPS, the UE that supports both 5GC and EPS NAS can operate in one of the following modes:

- Single-registration mode: UE has only one active MM state (either RM state in 5GC or EMM state in EPS) and it is either in 5GC NAS mode or in EPS NAS mode (when connected to 5GC or EPS, respectively).
- Dual-registration mode: UE handles independent registrations for 5GC and EPS using separate RRC connections. In this mode, the UE may be registered to 5GC only, EPS only, or to both 5GC and EPS.

Networks that support interworking with EPS, may support interworking procedures that use the N26 interface or interworking procedures that do not use the N26 interface.

- Interworking procedures with N26 support provide IP address continuity on inter-system mobility to UEs that support 5GC NAS and EPS NAS and that operate in single registration mode. Interworking procedures using the N26 interface, enables the exchange of MM and SM states between the source and target network.
- Networks that support interworking procedures without N26 support procedures to provide IP address continuity on inter-system mobility to UEs operating in both single-registration mode and dual-registration mode. For interworking without the N26 interface, IP address preservation is provided to the UEs on inter-system mobility by storing and fetching PGW-C+SMF and corresponding APN/DNN information via the HSS+UDM.

NOTE: Interworking of SMF and EPS currently works only with N26 interface.

Standards Compliance

The 5GC and EPS Interworking feature complies with the following standards:

- 3GPP TS 23.401, Version 15.6.0
- 3GPP TS 23.501, Version 15.4.0
- 3GPP TS 23.502, Version 15.4.0
- 3GPP TS 29.502, Version 15.2.1
- 3GPP TS 29.512, Version 15.2.0

Support for UE Initial Attach on E-UTRAN

Feature Description

The SMF supports the UE performing initial attach on E-UTRAN via MME and S-GW to create the default bearer.

Initial attach on E-UTRAN or EPS follows the procedure defined in 3GPP specification 23.401, Section 5.3.2.1. There are few deviations from the defined procedure to enable connectivity through the 5G core. The deviations are as follows:

- The Packet Data Network Gateway (P-GW) in the procedure is replaced by SMF+PGW.
- The IP-CAN Session establishment and modification is replaced by SM Policy Association Establishment procedure.

- The online and offline charging functionality using Gy and Gz interfaces is replaced by integrated charging over Nchf interface with Charging Function (CHF).
- The interface with the user-plane node is through N4 interface instead of Sxb interface.

How it Works

Call Flows

Initial Attach on E-UTRAN/EPS Procedure

The following figure shows the call flow derived from 3GPP reference for initial attach on E-UTRAN/EPS.

Figure 31: Initial Attach on E-UTRAN via 5G Core Call Flow

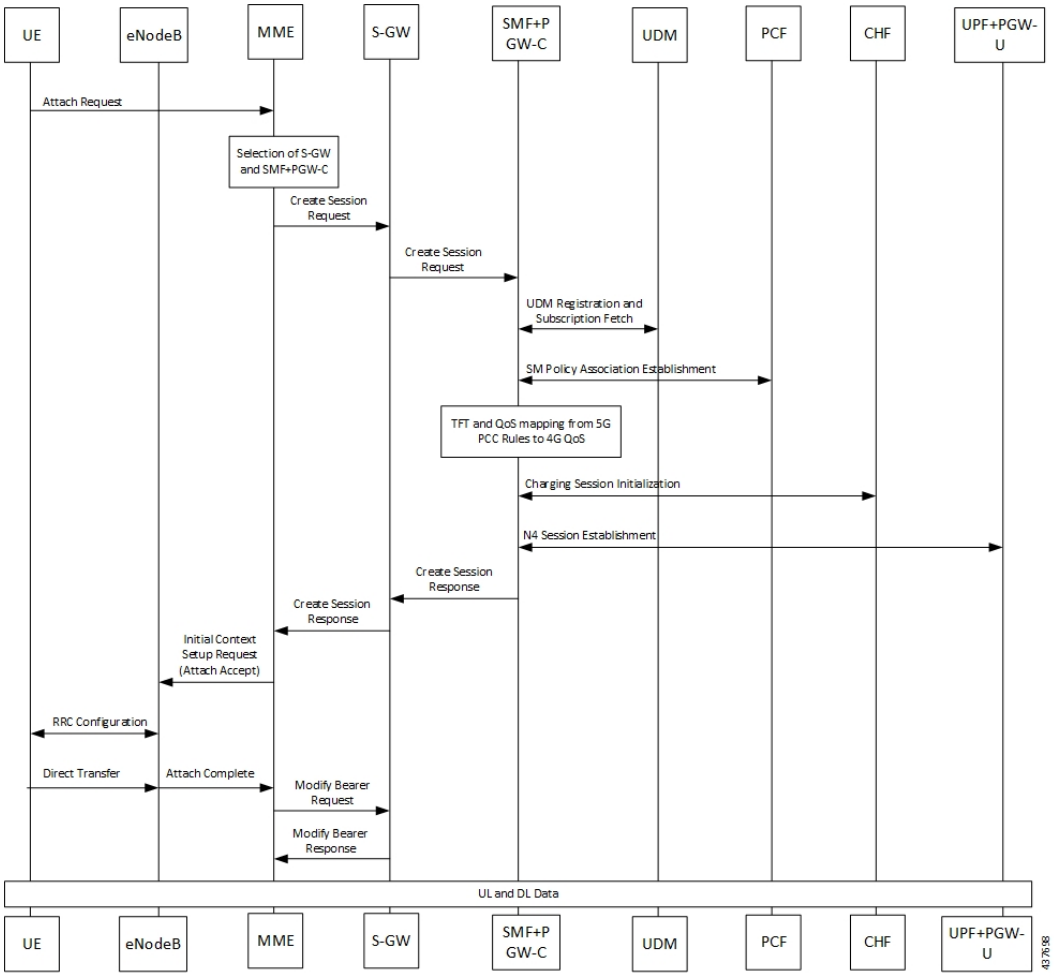


Table 52: Initial Attach on E-UTRAN via 5G Core Call Flow Description

Step	Description
1	UE sends Attach Request to MME through eNodeB.

Step	Description
2	MME determines that the UE is capable and subscribed for handoff to NR. It selects a SMF+PGW-C node as the P-GW for this PDU session.
3	MME sends Create Session Request to the selected S-GW and includes the selected SMF+PGW-C address in it.
4	S-GW initiates Create Session Request towards SMF+PGW-C.
5	SMF+PGW-C extracts the PDU Session Id sent by UE in the Protocol Configuration Option (PCO) 001AH (PDU session ID) and saves it. It then performs a Unified Data Management (UDM) registration and sends PGW Fully Qualified Domain Name (FQDN) to the UDM. After registration, SMF+PGW-C initiates subscription fetch from UDM.
6	SMF+PGW-C sends Npcf_SMPolicyControl_Create to PCF to initiate SM policy Association Establishment. In this procedure, the PGW-C+SMF includes the information elements received in Create Session Request message into the Npcf_SMPolicyControl_Create Service as follows: • The SUPI contains the IMSI. • The DNN contains the APN. • The PEI contains the IMEI-SV. • The Session AMBR contains the APN-AMBR. • The default QoS information that contains the default EPS bearer QoS. Note that QCI values are mapped into 5QI values.
7	The PGW-C+SMF receives Policy Charging and Control (PCC) Rules and PDU Session Policy Information, 5G QoS information in the PCC Rule and in PDU Session Policy Information which are mapped into EPS QoS information. The SMF+PGW-C creates Traffic Flow Template (TFT) from the Service Data Filters (SDFs) received in PCC rules and associates them with the corresponding default and dedicated bearers.
8	Based on the charging policies received from PCF, SMF+PGW-C initiates Nchf_ConvergedCharging_Create operation towards CHF. This procedure is similar to a 5G session and is based on the charging rules received from PCF.
9	SMF+PGW-C performs a UPF+PGW-U selection and N4 Session Establishment procedure. Since this session is a 4G session connecting to SMF+PGW-C, a separate CN tunnel is created for each bearer and QoS Flow ID (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
10	SMF+PGW-C sends Create Session Response to SGW and includes the bearer information and Tunnel Endpoint Identifier (TEID) for the default bearer. SMF+PGW-C also includes the 5G QoS parameters in PCO options 001CH (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime) and 001FH (QoS flow descriptions) to the UE.
11	S-GW sends Create Session Response to MME.
12	MME sends Initial Context Setup Request to eNodeB with N1 Attach Accept message.
13	eNodeB and UE perform Radio Resource Control (RRC) configuration.
14	UE sends Direct transfer message to eNodeB.

Step	Description
15	eNodeB sends Attach Complete message in Initial Context Setup Response to MME along with the TEID of eNodeB.
16	MME sends a Modify Bearer Request to S-GW with eNodeB TEID.
17	SMF+PGW-C sends the Modify Bearer Response to S-GW.
18	S-GW sends Modify Bearer Response to MME.

Configuring the UE Initial Attach Feature

This section describes how to configure the UE Initial Attach feature.

Configuring the UE Initial Attach feature involves the following steps:

1. Define FQDN in SMF Profile Configuration
2. Configure S5 Binding Address in SMF Service Configuration
3. Enable Kubernetes Configuration for SMF GTP Endpoint PODs

Define FQDN in SMF Profile Configuration

Use the following configuration to specify the FQDN of SMF+PGW-C. The configured FQDN is sent to the UDM during registration.

```
configure
   profile smf smf_profile_name
      fqdn fqdn_name
      end
```

NOTES:

- **fqdn** *fqdn_name*: Configures the FQDN of SMF+PGW-C. *fqdn_name* must be an alphanumeric string.

Configure S5 Binding Address in SMF Service Configuration

Use the following configuration to configure the S5 binding address, that is, the address at which the SMF listens for GTP messages from S-GW (S5 interface).

```
configure
   profile smf smf_profile_name
   service name smf_service_name
      s5 bind-address { ipv4 ipv4_address | ipv6 ipv6_address }
      end
```

NOTES:

- **s5 bind-address { ipv4** *ipv4_address* | **ipv6** *ipv6_address* **}**: Enter the IP address at which SMF listens for GTP messages from S-GW via S5 interface. Enter the address in either standard IPv4 dotted decimal format or in standard IPv6 colon notation format.

Enable Kubernetes Configuration for SMF GTP Endpoint PODs

Use the following configuration to define the SMF GTP Endpoint (gtp-ep) PODs.

```
configure
   k8 smf profile gtp-ep { external-ip | grpc-port | no-of-replicas }
   end
```

NOTES:

- **k8 smf profile gtp-ep**: Specifies Kubernetes configuration for SMF gtp-ep PODs.
- **no-of-replicas**: Enter the number of replicas for gtp-ep POD to be created. Default is 1.
- **external-ip**: Specifies the IP address on which gtp-ep kubernetes service listens.
- **grpc-port:** Enter the grpc port at which gtp-ep POD listens on for internal grpc messages, Default is 9003.

Verifying the UE Initial Attach Feature Configuration

This section describes how to verify the UE Initial Attach feature configuration.

The following configuration is a sample output of the show running-config command:

```
show running-config
.
.
.
profile smf smf1
 node-id          ABC123
 bind-address ipv4 127.0.0.1
 bind-port        8008
 allowed-nssai    [ slice1 ]
 plmn-id mcc 123
 plmn-id mnc 456
 fqdn ciscosmf1
 service name nsmf-pdu
  type               pdu-session
  .
  .
  .
  n4 bind-address ipv4 10.81.70.229
  s5 bind-address ipv4 10.81.70.229
  http-endpoint base-url http://smf-service
.
.
.
k8 smf local redis-endpoint redis-primary:6379
k8 smf local service no-of-replicas 1
k8 smf local nodemgr no-of-replicas 1
k8 smf local tracing enable true
.
.
.
```

Detach Procedure for EPS on SMF and P-GW

Feature Description

The SMF supports the default bearer deletion procedures for a UE attached through E-UTRAN, MME, and S-GW.

How it Works

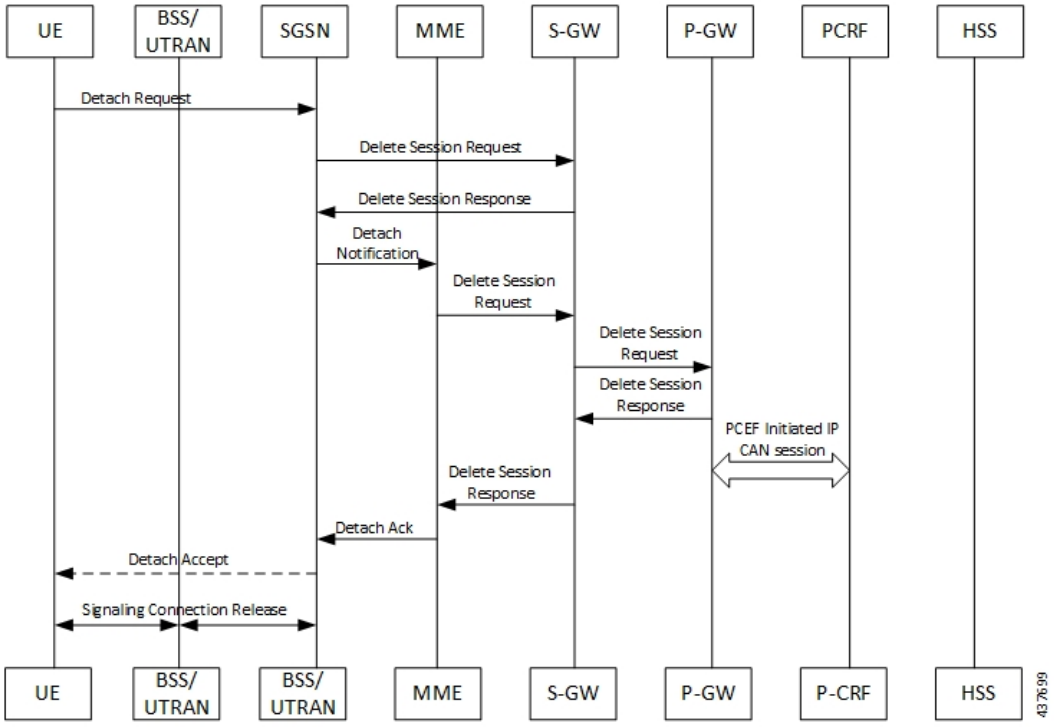
Call Flows

This section describes the call flows associated with this feature.

UE-initiated EPS Call Release Procedure

The following figure shows the call flow for UE-initiated release of EPS call.

Figure 32: UE-initiated Release of EPS Call Flow



The detach procedures for the EPS are defined in 3GPP 23.401, Section 5.3.8. When the UE is attached to E-UTRAN, the detach procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

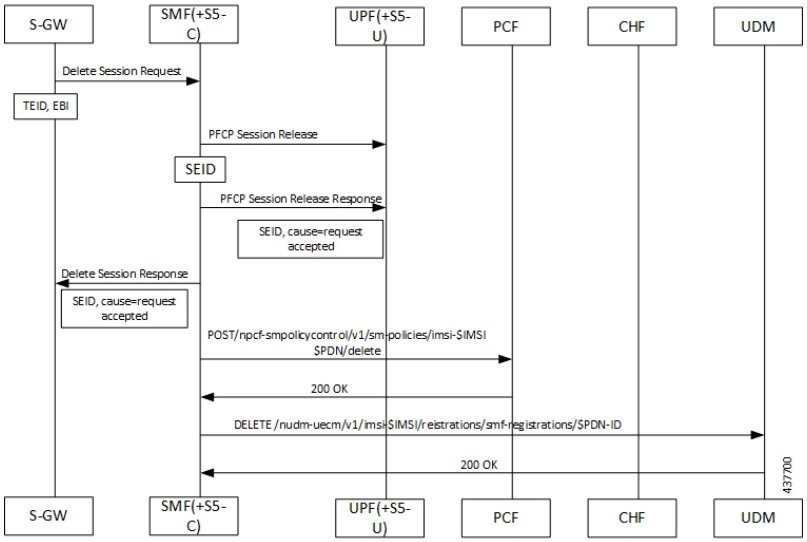
- Any interaction towards PCRF (CCR-T), that is PCEF initiated IP-CAN session between P-GW and PCRF, is replaced by Npcf_SMPolicyControl_Update Request from the SMF to the PCF. The parameters sent in this message follow a mapping from Delete Session Request contents in a way similar to the Create Session Request message for initial attach.

- All Gy and Gz interface messages are replaced by Nchf_ConvergedCharging_Release service operations.
- The user plane resources are removed using the N4 Session Release procedure towards UPF.

UE-initiated Call Release Detail Procedure

The following figure shows the detailed procedure of UE-initiated release of EPS call.

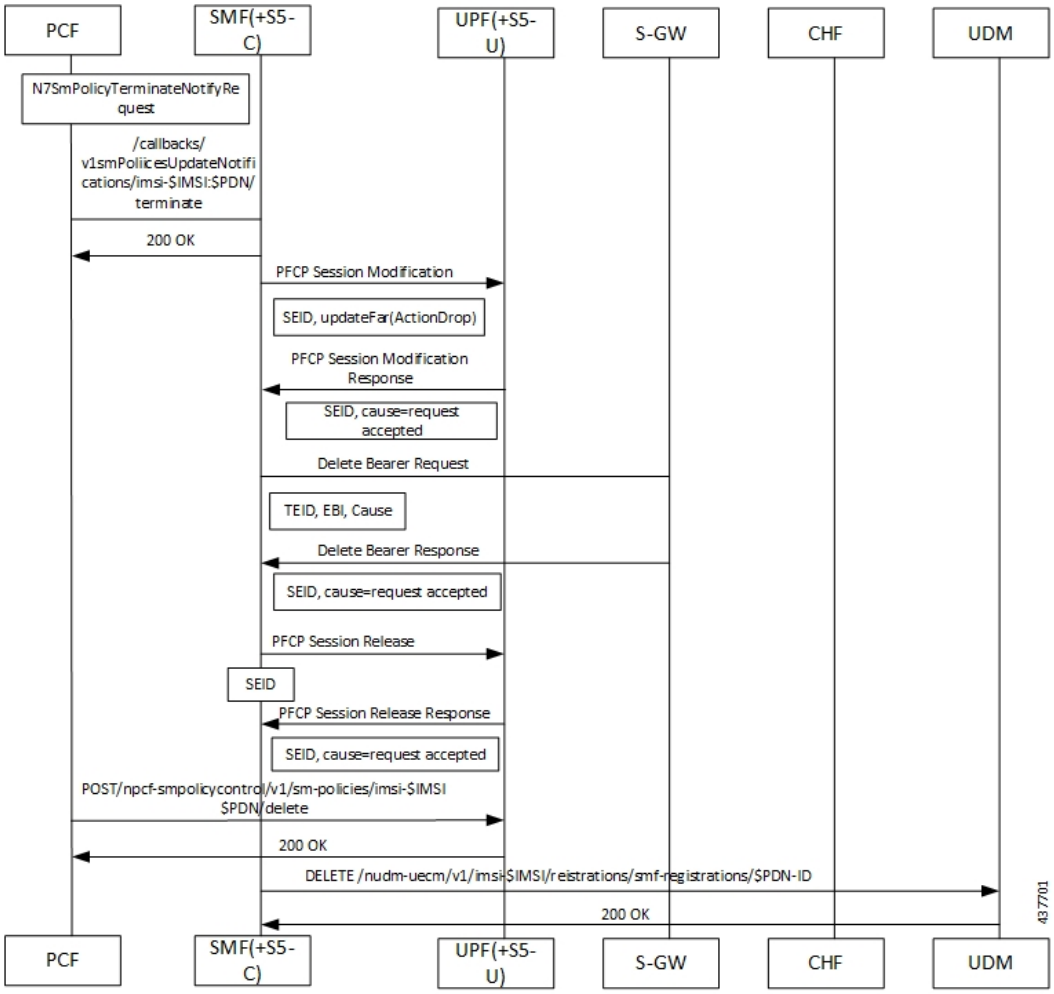
Figure 33: Detailed Call Flow of UE-initiated EPS Call Release



PCF-initiated Call Release Detail Procedure

The following figure shows the detailed procedure of PCF-initiated release of EPS call.

Figure 34: Detailed Call Flow of PCF-initiated EPS Call Release



Dedicated Bearer Activation and Deactivation

Feature Description

SMF supports the PCF-initiated dedicated bearer creation and dedicated bearer deletion procedures for a UE attached via E-UTRAN, MME, and S-GW.

How it Works

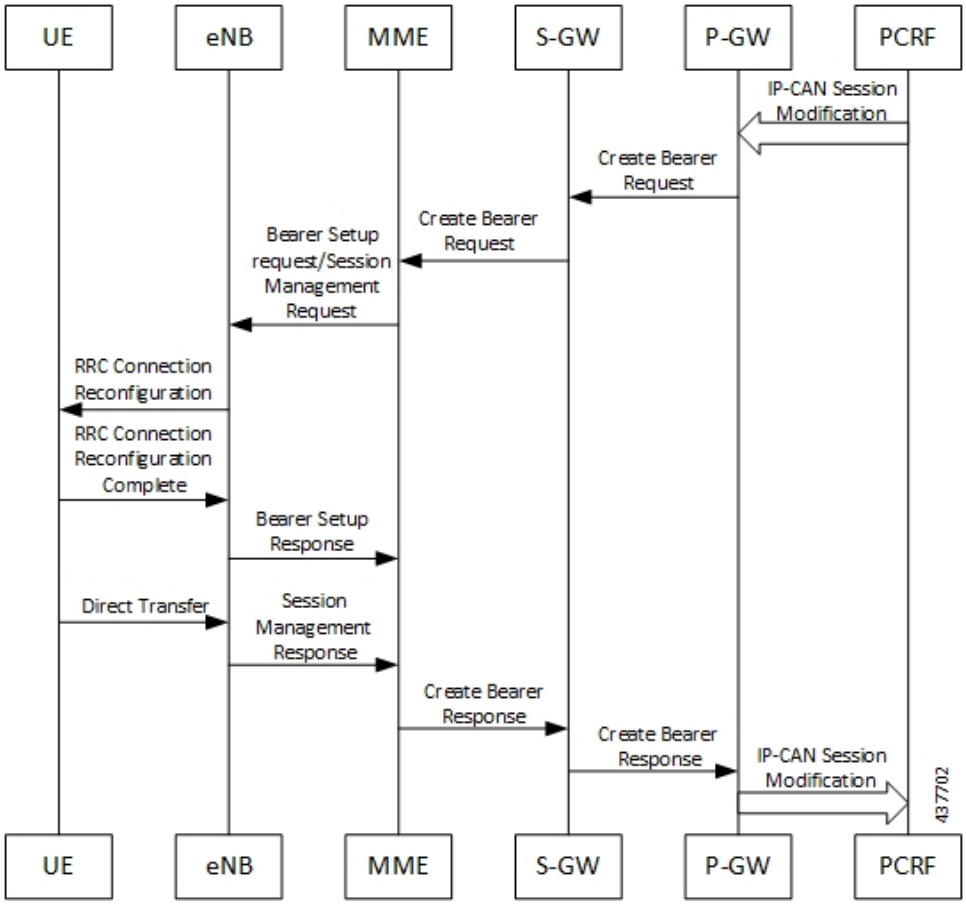
Call Flows

This section describes the call flows associated with this feature.

Dedicated Bearer Creation Call Flow

The following figure describes the Dedicated Bearer Creation procedure.

Figure 35: Dedicated Bearer Creation Call Flow

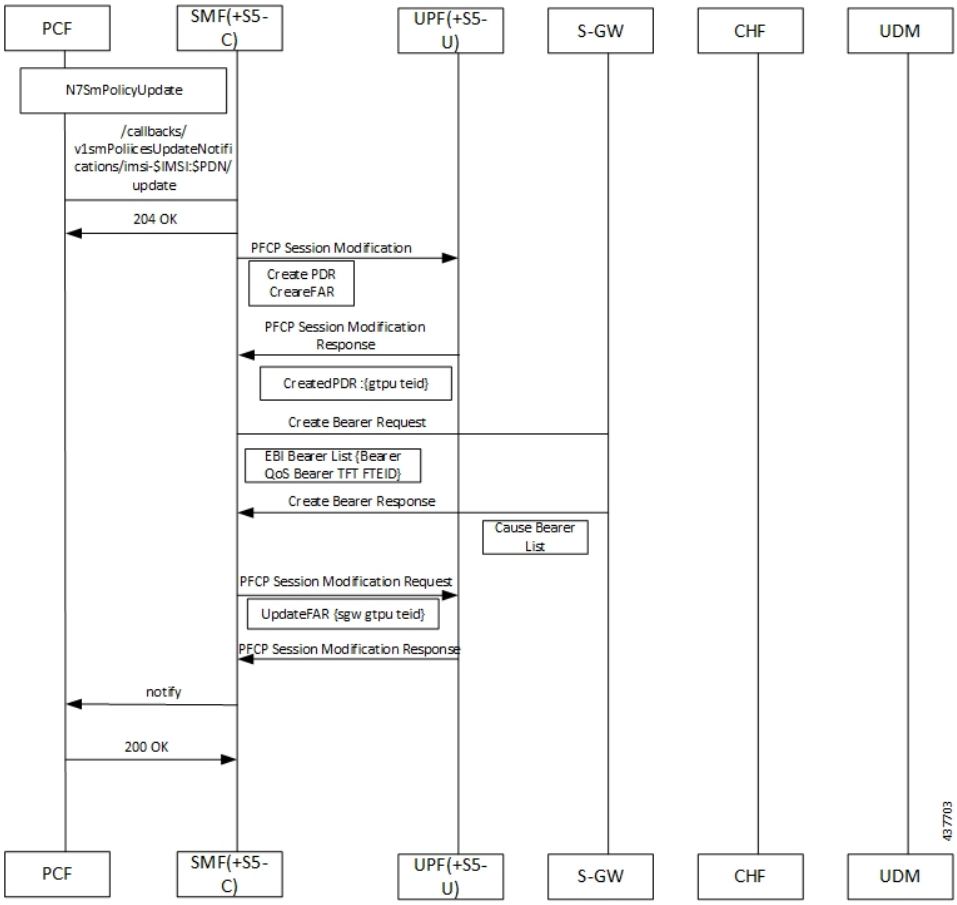


The dedicated bearer creation or activation procedure for the EPS session is defined in 3GPP 23.401, Section 5.4.1. When the UE is attached to E-UTRAN, the dedicated bearer procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

- Any interaction towards PCRF (RAR from PCRF/CCR-U to PCRF) are replaced by Npcf_SMPolicyControl_UpdateNotify request from PCF to SMF and Npcf_SMPolicyControl_Update Request from the SMF to the PCF respectively.
- The PCC rules provided by PCF are mapped to TFTs for the new dedicated bearer and the associated QoS is mapped to 4G QoS as defined in the Generating EPS PDN Connection Parameters from 5G PDU Session Parameters, on page 256.
- All Gy and Gz interface messages are replaced by Nchf_ConvergedCharging_Update service operations.
- The user plane resources for dedicated bearers are added using the N4 Session Modification procedure towards UPF where PDRs, QERs and FARs are added for the SDF filters for the new dedicated bearer.
- SMF+PGW-C saves the EBI for the dedicated bearer as received in Create Bearer response.

The following figure describes the PCF-initiated Dedicated Bearer Activation procedure.

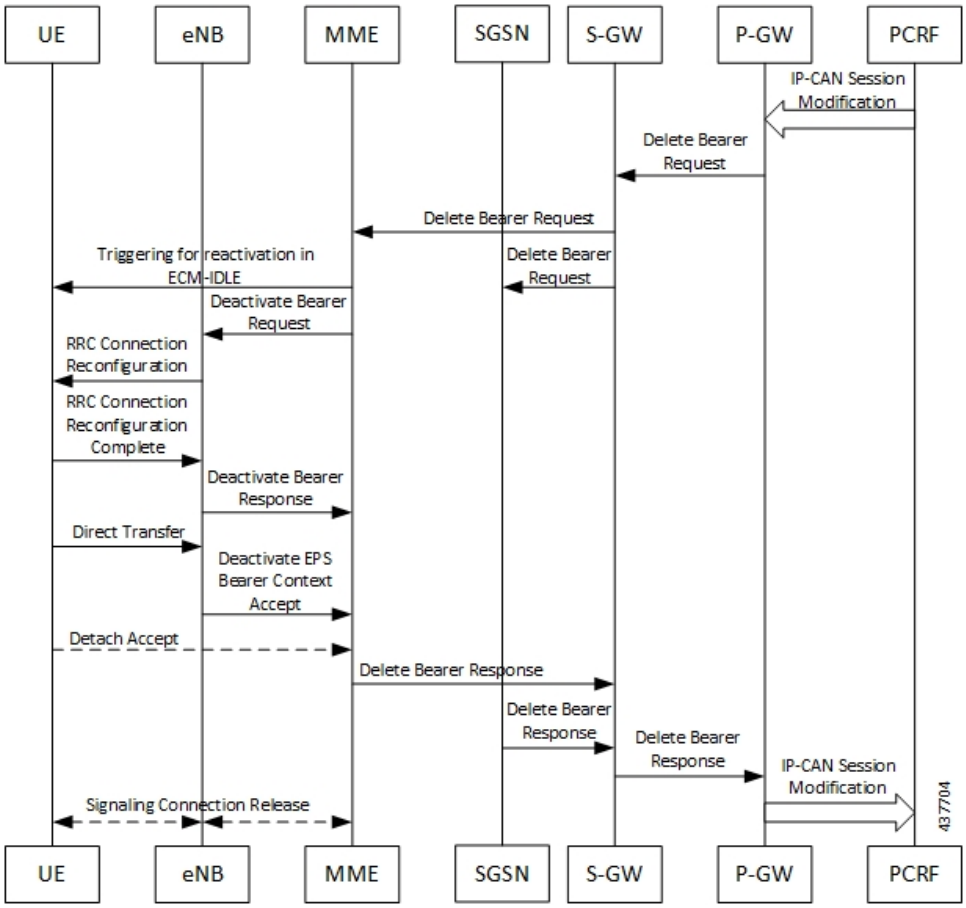
Figure 36: PCF-initiated Dedicated Bearer Activation



Dedicated Bearer Deactivation Call Flow

The following figure describes the Dedicated Bearer Deactivation procedure.

Figure 37: Dedicated Bearer Deactivation Call Flow



The dedicated bearer deactivation procedure for the EPS session is defined in 3GPP 23.401, Section 5.4.4. When the UE is attached to E-UTRAN, the dedicated bearer procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

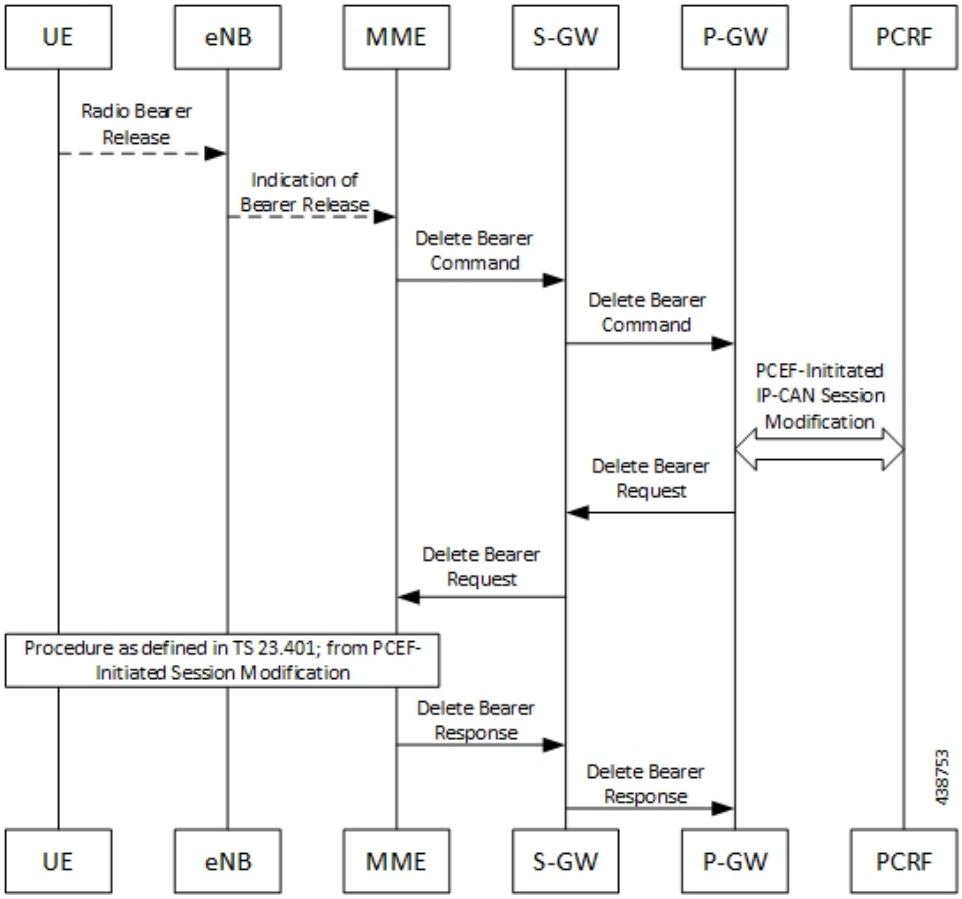
- Any interaction towards PCRF (RAR from PCRF/CCR-U to PCRF) are replaced by Npcf_SMPolicyControl_UpdateNotify request from PCF to SMF and Npcf_SMPolicyControl_Update Request from the SMF to the PCF respectively.
- The PCC rules removed by PCF are mapped to corresponding dedicated bearers and the bearer deactivation is triggered for these bearers.
- All Gy and Gz interface messages are replaced by Nchf_ConvergedCharging_Update service operations.
- The user plane resources for dedicated bearers are removed using the N4 Session Modification procedure towards UPF where PDRs, QERs and Forward Action Rule (FARs) are removed for the SDF filters for the deleted dedicated bearer.

MME-initiated Dedicated Bearer Deactivation

The MME uses the UE or MME requested PDN Disconnection procedure to initiate the release of PDN connections. The following call flow illustrates the procedure in which the dedicated bearers are deactivated.

Note The default bearers are not affected during the disconnection process.

Figure 38: MME-initiated Dedicated Bearer Deactivation



Step	Description
1	Radio bearers for the UE in the ECM-CONNECTED state are released due to local reasons, for example, abnormal resource limitation. The UE deletes the bearer contexts related to the released radio bearers.
2	When eNodeB releases radio bearers, it sends an indication of bearer release to the MME. This indication could either be the Bearer Release Request (EPS Bearer Identity) message to the MME, or Initial Context Setup Complete, Handover Request Ack and UE Context Response. Path Switch Request can also indicate the release of a bearer. The eNodeB includes the ECGI and TAI in the indication sent to the MME.

Step	Description
3	The MME sends the Delete Bearer Command (EPS Bearer Identity, User Location Information, UE Time Zone, RAN/NAS Release Cause if available) message per PDN connection to the S-GW to deactivate the selected dedicated bearer. RAN/NAS Release Cause indicates the RAN release cause and/or the NAS release cause. RAN/NAS Release Cause is only sent by the MME to the P-GW if this is permitted according to the MME operator's policy.
4	The S-GW sends the Delete Bearer Command (EPS Bearer Identity, User Location Information, UE Time Zone, RAN/NAS Release Cause) message per PDN connection to the P-GW.
5	If PCC infrastructure is deployed, the P-GW informs the PCRF about the loss of resources by means of a PCEF-initiated IP-CAN Session Modification procedure as defined in TS 23.203 and provides the User Location Information, UE Time Zone and RAN/NAS Release cause (if available) received in the Delete Bearer Command from the S-GW if requested by the PCRF as defined in TS 23.203. The PCRF sends an updated PCC decision to the P-GW. **Note** User Location Information and UE Time Zone might not be available if the MME or the S-GW are of a previous release and did not provide this information.
6	The P-GW sends a Delete Bearer Request (EPS Bearer Identity) message to the S-GW.
7	The S-GW sends the Delete Bearer Request (EPS Bearer Identity) message to the MME.
8	Steps between steps 5 and 8 are invoked. They are omitted if the bearer deactivation was triggered by the eNodeB in step 1 and step 2. Also, these steps are omitted if the MME initiated bearer release due to failed bearer set up during handover, the UE and the MME deactivate the failed contexts locally without peer-to peer ESM signaling.
9	The MME deletes the bearer contexts related to the deactivated EPS bearer and acknowledges the bearer deactivation to the S-GW by sending a Delete Bearer Response (EPS Bearer Identity, User Location Information (ECGI)) message.
10	The S-GW deletes the bearer context related to the deactivated EPS bearer and acknowledges the bearer deactivation to the P-GW by sending a Delete Bearer Response (EPS Bearer Identity) message.

SMF-initiated Dedicated Bearer Deactivation

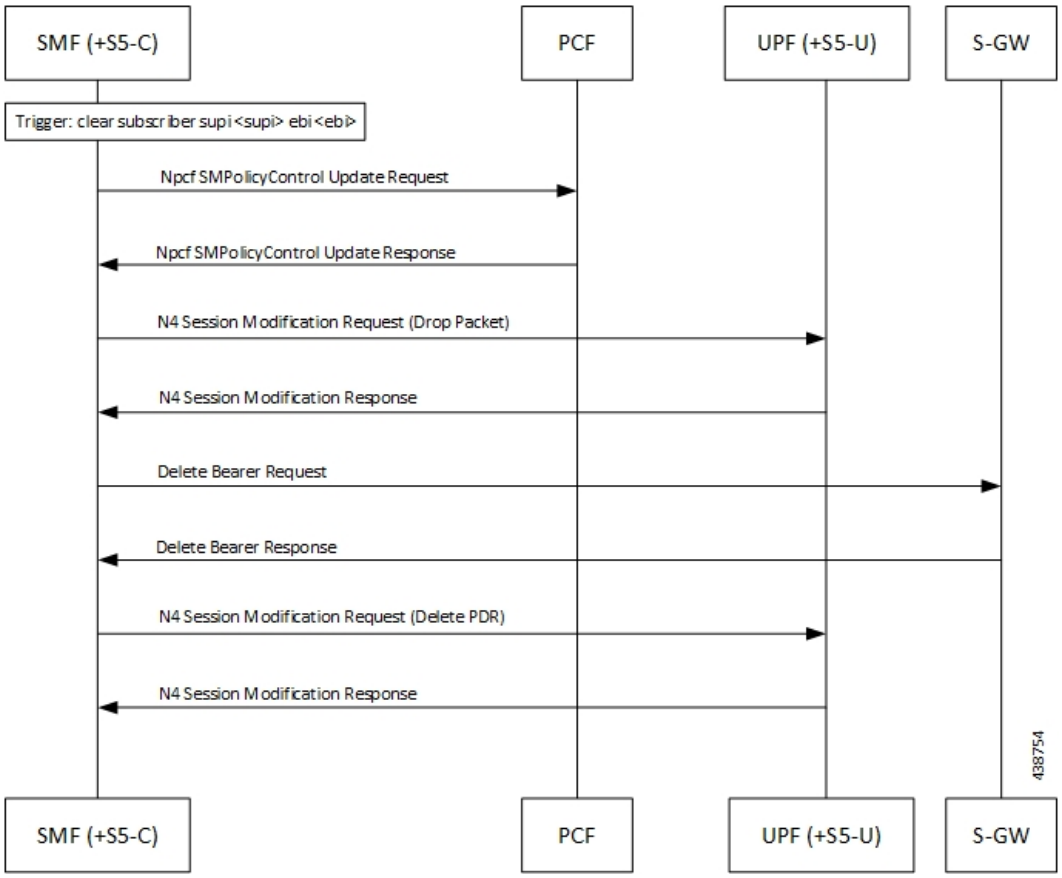
The following procedure describes the SMF-initiated dedicated bearer deactivation process as defined in 3GPP TS 23.203.

Note Default bearers are not affected during the dedicated bearer deactivation process.

- The SMF-initiated delete bearer is triggered using the **clear subscriber** command.
- If the PCC infrastructure is deployed, the P-GW informs the PCRF about the loss of resources by means of a PCEF-initiated IP-CAN Session Modification procedure and provides the User Location Information, UE Time Zone and RAN/NAS Release cause (if available) received in the **clear subscriber** command if requested by the PCRF. The PCRF sends an updated PCC decision to the P-GW.
- The P-GW sends a Delete Bearer Request (EPS Bearer Identity) message to the S-GW.
- The S-GW deletes the bearer context related to the deactivated EPS bearer and acknowledges the bearer deactivation to the P-GW by sending a Delete Bearer Response (EPS Bearer Identity) message.

The following call flow illustrates the SMF-initiated dedicated bearer deactivation.

Figure 39: SMF-initiated Dedicated Bearer Deactivation



EPS Fallback

Feature Description

SMF supports fallback to EPS from 5GC for IMS sessions if gNB rejects the dedicated bearer creation with ims-voice-eps-fallback or rat-fallback triggered.

For the UE devices not supporting VoNR, the SMF performs a fallback to EPS for voice calls. This includes 5G to EPS handover and dedicated bearer creation in 4G for voice call.

How it Works

Call Flows

The following call flow depicts the EPS Fallback procedure.

Figure 40: EPS Fallback Call Flow

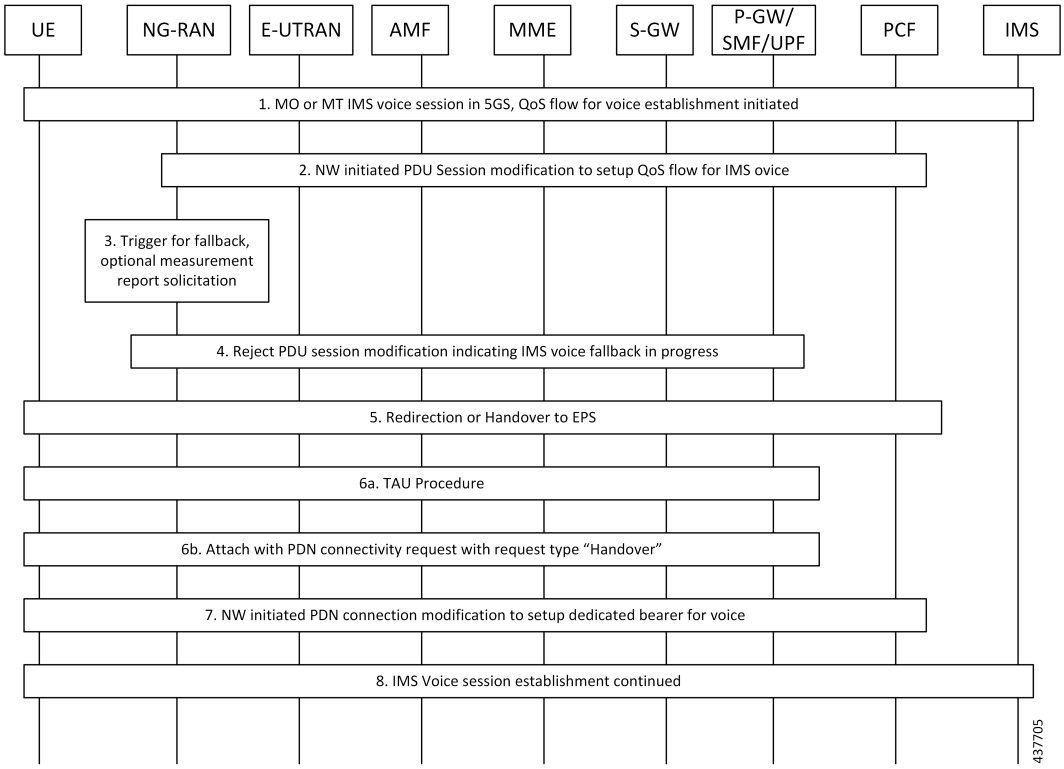


Table 53: EPS Fallback Call Flow Description

Step	Description
1	In the 5GS, UE is with NG-RAN and a Mobile-Originated (MO) or a Mobile-Terminated (MT) IMS voice session establishment is initiated.
2	The Network-initiated PDU Session modification request to setup QoS flow for voice reaches the NG-RAN.
3	The NG-RAN is configured to support the EPS fallback for IMS voice. Based on the UE functionalities, indication from the AMF to redirect EPS fallback for voice, network configuration, and radio conditions, the NG-RAN triggers fallback to EPS. If the NG-RAN determines to not trigger the fallback to EPS, then the procedure stops, and the following steps are not performed. The NG-RAN may initiate measurement report solicitation from the UE including E-UTRAN as target.

Step	Description
4	The NG-RAN rejects the PDU Session modification request received in Step 2 with an indication that mobility due to fallback for IMS voice is ongoing. The NG-RAN indicates the rejection of the PDU session modification to configure QoS flow for IMS voice that is received in Step 2 as PDU Session Response message toward the SMF through the AMF. This message includes the details on the ongoing mobility due to fallback for IMS voice. The SMF maintains the PCC rules that are associated with the QoS flows. For a roaming scenario, the PDU Session Response message is sent toward H-SMF through V-SMF.
5	Based on the UE functionalities, the NG-RAN initiates handover to EPS. The SMF reports change of the RAT type, if the PCF is subscribed for it. A timer starts to track failure in the EPS fallback. After the timer expires, the SMF notifies the PCF about the dedicated bearer creation failure and new statistics, with the "smf_eps_fb" and "timeout" labels, is incremented.
6a	For 5GS to EPS handover, the UE initiates TAU procedure.
6b	The UE attaches the PDN connectivity request with the "handover" request type.
7	After the completion of the 5GS to EPS handover procedure, the SMF or P-GW re-initiates the configuration of the dedicated bearer for IMS voice and mapping the 5G QoS to EPC QoS parameters. The SMF notifies about the Successful Resource Allocation and Access Network Information, if the PCF is subscribed for it.
8	The IMS voice session establishment continues.

EPS Fallback Guard Timer Support

Feature Description

SMF supports the guard timer to track failure in the EPS fallback. After the timer starts, it waits for the EPS fallback to happen before the bearer creation failure information is communicated to PCF.

How It Works

The EPS fallback timer starts after receiving the notification for dedicated bearer creation failure with the EPS fallback cause from gNB through AMF. In this case, SMF does not send the failure notification to PCF and waits for 5G to 4G handover to complete. Then, SMF triggers the bearer creation in 4G. The EPS fallback timer stops on the completion of the 5G to 4G handover.

In case the timer expires before the completion of the 5G to 4G handover, SMF sends a notification for dedicated bearer creation failure to PCF. Then, the new statistics counter, with the "smf_eps_fb" and "timeout" labels, is incremented. However, the 5G to 4G handover procedure continues.

Call Flows

This section includes the following call flow.

EPS Fallback Guard Timer Call Flow

This section describes the 5G to EPS fallback guard timer call flow.

Figure 41: EPS Fallback Guard Timer Call Flow

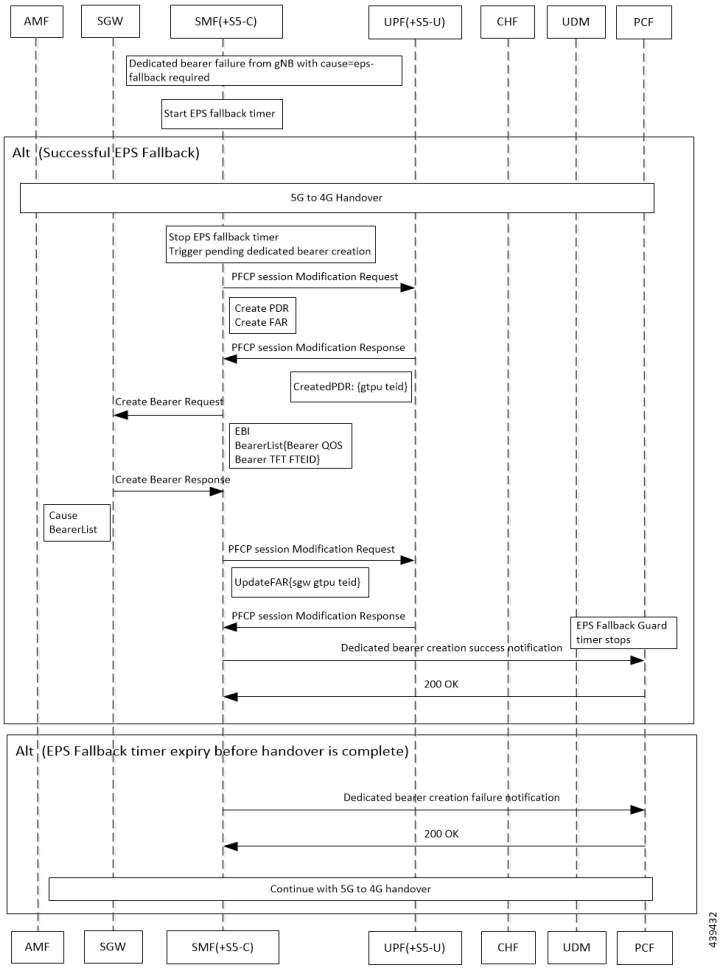


Table 54: EPS Fallback Guard Timer Call Flow Description

Step	Description
1	gNB sends the dedicated bearer creation failure information with the fallback cause through AMF.
2	EPS fallback timer starts.
In the successful EPS fallback with 5G to 4G handover scenario, Steps 3 –12 happen.	
3	EPS fallback timer stops and triggers pending dedicated bearer creation.
4	SMF(+S5-C) sends the PFCP session modification request to UPF(+S5-U).
5	PDR and FAR are created.
6	UPF(+S5-U) sends the PFCP session modification response to SMF(+S5-C).

Step	Description
7	The information on the created PDR with the GTP-U TEID is available.
8	SMF(+S5-C) sends the Create Bearer Request to SGW.
9	SGW sends the Create Bearer Response to SMF(+S5-C).
10	SMF(+S5-C) sends the PFCP Session Modification Request to UPF(+S5-U).
11	UPF(+S5-U) sends the notification of the successful dedicated bearer creation to PCF.
12	EPS fallback guard timer stops.
13	PCF sends the “200 OK” acknowledgment to SMF(+S5-C)
In the EPS fallback timer expiry before handover completion scenario, Steps 13–15 happen.	
14	SMF(+S5-C) sends the failure notification of the dedicated bearer creation to PCF.
15	PCF sends the “200 OK” acknowledgment to SMF(+S5-C).
16	The 5G to 4G handover procedure continues.

Standards Compliance

The EPS fallback guard timer support feature complies with the following standards:

- 3GPP TS 23.502 V16.1.1 (2019-06).

Configuring the EPS Fallback Guard Timer

This section describes how to configure the EPS Fallback Guard Timer feature.

```
configure
  profile access test [ eps-fallback | n2 | n26 ]
  eps-fallback guard timeout timeout_value
  n26 idft enable timeout n26_timeout_value
  n2 idft enable timeout n2_timeout_value
  end
```

NOTES:

- **profile access**: Accesses the profile configuration.
- **test**: Accesses the profile instance.
- **eps-fallback**: Enters the EPS fallback configuration.
- **eps-fallback guard timeout**: Enters the value for the EPS fallback timer from the range of 500 to 15000 milliseconds
- **n26**: Enters the N26 interface, which is the E-UTRAN and NG-RAN configuration
- **n2**: Enters the N2 interface, which is the NG-RAN configuration.
- **idft enable timeout**: Enters the value from 15 to 60 for the IDFT timer to expire.

Indirect Data Forwarding Tunnel (IDFT) Timer Support

Feature Description

SMF supports the Indirect Data Forwarding Tunnel (IDFT) timer during the IDFT procedures for 5G to a 4G handover. During the handover, the IDFT tunnels of 5G are released. SMF receives the NSMF PDU Session Update SM Context Request to release the forwarding tunnels from AMF. When SMF does not receive this request, the IDFT timer ensures the release of unused tunnels.

Call Flows

This section includes the following call flow.

5G to EPS Handover with IDFT Timer Call Flow

This section describes the 5G to EPS handover with IDFT timer call flow.

Figure 42: 5G to EPS Handover with IDFT Timer Call Flow

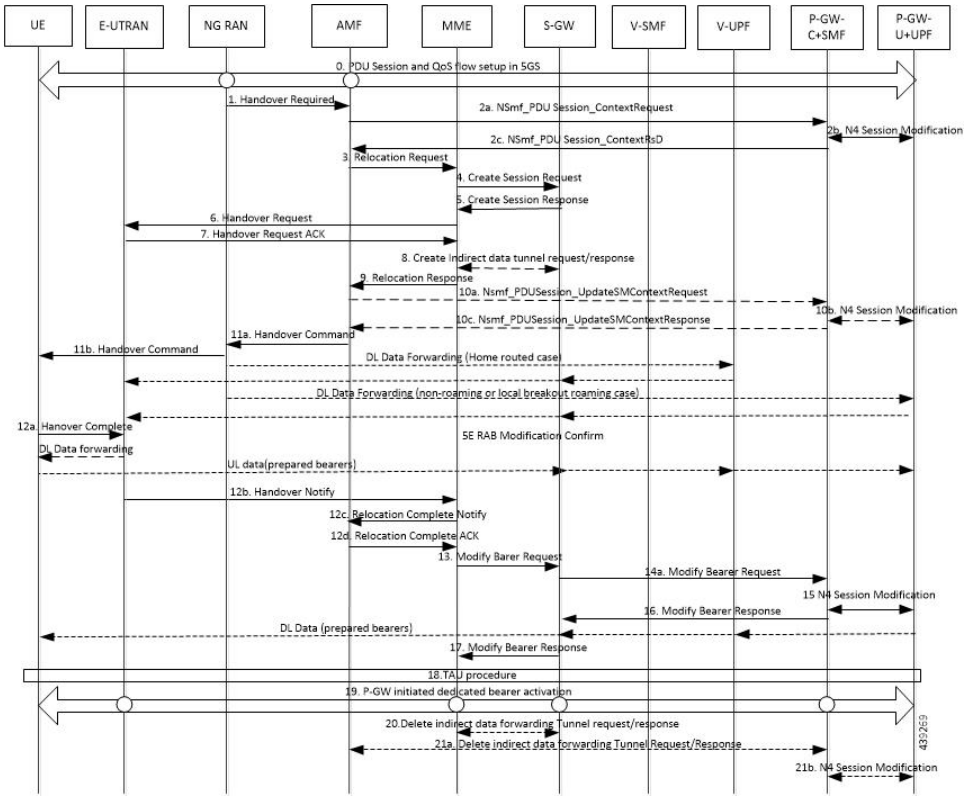


Table 55: 5G to EPS Handover with IDFT Timer Call Flow Description

Step	Description
1	NG-RAN determines to handover UE to E-UTRAN. If NG-RAN is configured to perform inter-RAT mobility due to the IMS voice fallback that is triggered by QoS flow setup and request to set up QoS flow for IMS voice is received, then NG-RAN indicates the rejection of the QoS flow establishment. This indication is because of mobility due to fallback for the IMS voice through N2 SM information and triggers the handover to E-UTRAN. The NG-RAN sends a Handover Required message to the AMF. This message includes the details on target eNB ID, direct forwarding path availability, source to target transparent container, and inter-system handover indication. NG-RAN uses the source to target transparent container to indicate bearers for the corresponding 5G QoS flows for data forwarding.
2a	AMF sends the NSMF PDU Session Context Request to the SMF+PGW-C to provide SM Context.
2b	SMF+PGW-C sends the N4 session modification to PGW-U+UPF to establish the CN tunnel for each EPS bearer. The bearer mapping to the 5G QoS and PCC rules, which PCC sends, are available in the SMF. The SMF also has the bearer IDs that are received from the bearer ID allocation procedure. The SMF+PGW-C creates new PDRs for the N4 session and gets the TEID allocated for each bearer as required by the 4G system. The timer in SMF+PGW-C starts in this step. This timer monitors the resources for indirect data forwarding in UPF that are to be released. Following are the cases for the IDFT timer expiry: • Step 21a does not happen and the timer expires—The PDRs and FARs that are not required for the indirect tunnels, are removed before Step 21a. • The timer expires before or during the Steps 14a and 16—The PDRs and FARs that are not required for the indirect tunnels, are removed and the call flow continues independently. • Step 21a happens after the timer expiry—The SMF does not send the N4 Modification Request to UPF+PGW-U as the resources are released on the timer expiry.
2c	SMF+PGW-C sends the EPS bearer contexts to AMF. The bearer context is a string with the byte format, which is the base64-encoded characters, encoding the UE EPS PDN Connection IE. The SMF+PGW-C also provides the CN tunnel information to AMF for all the bearers for the uplink traffic from E-UTRAN.
3	AMF sends a Forward Relocation Request to MME. The AMF includes the mapped SM EPS UE Contexts for the PDU Sessions with and without active UP connections.
4	MME sends the Create Session Request to SGW. See S1-based handover in the normal case section in 3GPP TS 23.401 clause 5.5.1.2.2 for details.
5	SGW sends the Create Session Response to MME. See S1-based handover in the normal case section in 3GPP TS 23.401 clause 5.5.1.2.2 for details.

Step	Description
6	MME sends the handover request to E-UTRAN.
7	E-UTRAN sends the handover request acknowledgment to MME.
8	MME and SGW send and receive the indirect data forwarding request and response to each other.
9	MME sends the Relocation Response to AMF.
10a	In case of indirect data forwarding, AMF sends the NSMF PDU Session Update SM Context Request to PGW-C+SMF. This request is for SGW addresses and SGW DL TEIDs for data forwarding and for creating the indirect data forwarding tunnel.
10b	PGW-C+SMF sends the N4 Modification Request to UPF+PGW-U to create more PDRs and FARs. The PDRs and FARS are created to receive the redirected DL data over the indirect tunnel from NG RAN and to forward them to eNodeB. The UL PDRs have the QFI to match the forwarded DL data from NG RAN. The associated QER has the QFI to forward the data to eNodeB. Also, the FAR redirects the received data to eNodeB over the appropriate tunnel based on the QFI.
10c	PGW-C+SMF sends the NSMF PDU Session Update SM Context Response to AMF. This response includes details on cause, CN tunnel information for data forwarding, and QoS flows for data forwarding. PGW-C+SMF sends this response to create indirect data forwarding. Based on the correlation between QFIs and SGW addresses and TEIDs for data forwarding, the PGW-U+UPF maps the QoS flows into the data forwarding tunnels in EPC.
11a	AMF sends the Handover Command to the source NG-RAN.
11b	The source NG-RAN sends the Handover Command to UE to handover to the target access network. The UE correlates the ongoing QoS Flows with the indicated EPS Bearer IDs (EBI) that are to be set up in the handover command. If the QoS Flow associated with the default QoS rule in the PDU Session has an unassigned EBI, the UE deletes the PDU Session locally. If the QoS Flow that is associatedthat is with the default QoS rule has an assigned EBI, the UE retains the PDU session. For the QoS Flow with unassigned EBIs, the UE deletes the QoS rules and the QoS Flow level QoS parameters locally if any associated with those QoS Flows. Then, the UE notifies the impacted applications that the dedicated QoS resource has been released. The UE deletes any UE-derived QoS rules. The EBI that was assigned for the QoS Flow of the default QoS rule in the PDU Session becomes the EBI of the default bearer in the corresponding PDN connection.
12a	UE sends the notification of handover completion to E-UTRAN.
12b	E-UTRAN sends the Handover Notify request to MME.
12c	MME sends the Relocation Complete Notification to AMF.
12d	AMF sends the Relocation Complete Notification acknowledgment to MME.
13	MME sends the Modify Bearer Request to SGW.

Step	Description
14a	SGW sends the Modify Bearer Request to SMF+PGW-C. This request includes the information on DL TEIDs on SMF for the bearers.
15	PGW-C+SMF initiates a N4 Session Modification procedure toward the UPF+PGW-U to update the User Plane path, which implies that DL User Plane for the indicated PDU Session is switched to E-UTRAN. The PGW-C+SMF releases the resource of the CN tunnel for PDU Session in UPF+PGW-U.
16	PGW-C+SMF sends Modify Bearer Response to SGW. At this stage, the User Plane path is established for the default bearer and the dedicated EPS bearers between the UE, target eNodeB, SGW, and the PGW-U+UPF. The PGW-C+SMF uses the EPS QoS parameters as assigned for the dedicated EPS bearers during the QoS Flow establishment. PGW-C+SMF maps all the other IP flows to the default EPS bearer. If indirect forwarding tunnels are established, the PGW-C+SMF starts a timer to release the resources that are used for indirect data forwarding.
17	SGW sends Modify Bearer Response to MME.
18	UE initiates a Tracking Area Update procedure. See the S1-based handover in the normal case section in 3GPP TS 23.401 clause 5.5.1.2.2 for details. This procedure deregisters the old AMF for 3GPP access from HSS+UDM. Any registration that is associated with the non-3GPP access in the old AMF is not removed. It implies that an AMF that is serving the UE over both the 3GPP and non-3GPP accesses does not consider the UE as deregistered over non-3GPP access and remains registered and subscribed to subscription data updates in UDM.
19	If PCC is deployed, then PCF determines to provide the earlier removed PCC rules to the PGW-C+SMF again. With these PCC rules, the PGW-C+SMF initiates the dedicated bearer activation procedure.
20	SGW sends the Delete Indirect Data Forwarding Tunnel Request to MME. The MME sends the Delete Indirect Data Forwarding Tunnel Response to SGW.
21a	AMF initiates NSMF PDU Session Update SM Context Request service operation with an indication to release the forwarding tunnels.
21b	SMF sends the N4 Modification Request to UPF+PGW-U to delete the PDRs and FARs for the indirect tunnels. The PDRs and FARs for the 5G session which are not required are also removed. The IDFT timer that started in Step 2b stops.

Standards Compliance

The IDFT timer support feature complies with the following standards:

- 3GPP TS 23.502 V16.1.1 (2019-06)
- 3GPP TS 23.401 version 12.6.0 Release 12

Configuring the IDFT Timer

This section describes how to configure the IDFT timer.

```
configure
  profile access test [ eps-fallback | n2 | n26 ]
  eps-fallback guard enable timeout timeout_value
  n26 idft enable timeout n26_timeout_value
  n2 idft enable timeout n2_timeout_value
    end
exit
```

NOTES:

- **profile access**: Accesses the profile configuration.
- **test**: Accesses the profile instance.
- **eps-fallback**: Enters the EPS fallback configuration.
- **n26**: Enters the N26 interface, which is the E-UTRAN and NG-RAN configuration
- **n2**: Enters the N2 interface, which is the NG-RAN configuration.
- **idft enable timeout**: Enters the value from 15 to 60 for the IDFT timer to expire.

Bearer Modification for EPS Session on SMF

Feature Description

SMF supports modification of EPS bearer that a PCF or an MME initiates. The SMF+PGW handles the following triggers for this feature:

- QoS modifications.
- RAT, ULI, and SGW modifications.
- UE time zone modifications.

How it Works

The bearer modification for an EPS session on SMF works with the following modifications:

- PCF and MME-Initiated Bearer Modifications for EPS session on SMF—These procedures are used either when one or multiple EPS Bearer QoS parameters QCI, GBR, MBR, or ARP are modified or to modify the APN-AMBR. The PCF-initiated or the MME-initiated bearer modification procedures do not support the modification from a QCI of non-GBR resource type to a GBR resource type QCI and vice versa.
- X2 and S1 Based Handover for EPS Session Connected to SMF—The X2-based handover procedure is used to hand over a UE from a source eNodeB to a target eNodeB using X2. In this procedure, the MME is unchanged and the MME determines to relocate the SGW.

The S1-based handover procedure is used when the X2-based handover cannot be used. The source eNodeB initiates a handover by sending the Handover Required message over the S1-MME reference point. This procedure may relocate the MME or the SGW.

Call Flows

This section includes the following call flows:

- PCF-Initiated Bearer Modification for EPS session on SMF call flow
- MME-Initiated Bearer Modification for EPS session on SMF call flow
- X2 and S1 Based Handover for EPS Session Connected to SMF call flow

PCF-initiated Bearer Modification for EPS session on SMF Call Flow

This section describes the PCF-Initiated Bearer Modification for EPS session on SMF call flow.

Figure 43: PCF-Initiated Bearer Modification for EPS session on SMF Call Flow

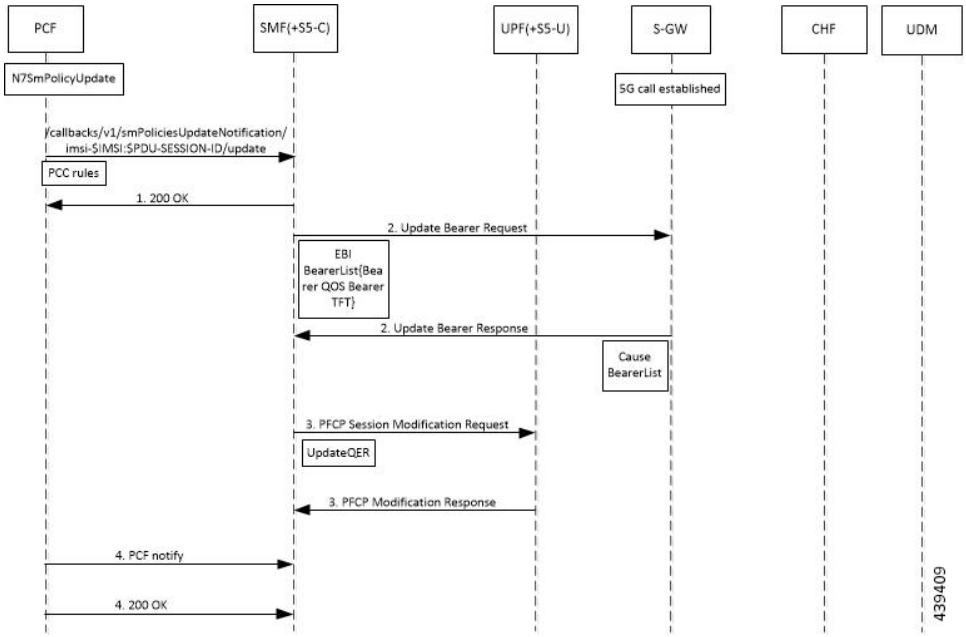


Table 56: PCF-Initiated Bearer Modification for EPS session on SMF Call Flow Description

Step	Description
1	PCF initiates the N7 Policy Update Notify with the updated parameters of QoS or TFT toward SMF.
2	SMF sends the “200 OK” acknowledgment to PCF. The PCC rules that the PCF provides are mapped to TFTs for the modified dedicated bearer. The associated QoS is mapped to 4G QoS.
3	SMF sends the Update Bearer Request to SGW.

Step	Description
4	SGW sends the Update Bearer Response to SMF with EPS Bearer ID and the modified QoS or TFT for the associated bearer.
5	SMF initiates the PFCP Modification request toward UPF.
6	UPF sends the PFCP Modification Response to SMF with updated QER.
7	SMF sends the PCF Notify message to PCF.
8	PCF sends the “200 OK” acknowledgment to SMF.

MME-initiated Bearer Modification for EPS session on SMF Call Flow

This section describes the MME-Initiated Dedicated Bearer Modification for EPS session on SMF call flow.

Figure 44: MME-Initiated Bearer Modification for EPS session on SMF Call Flow

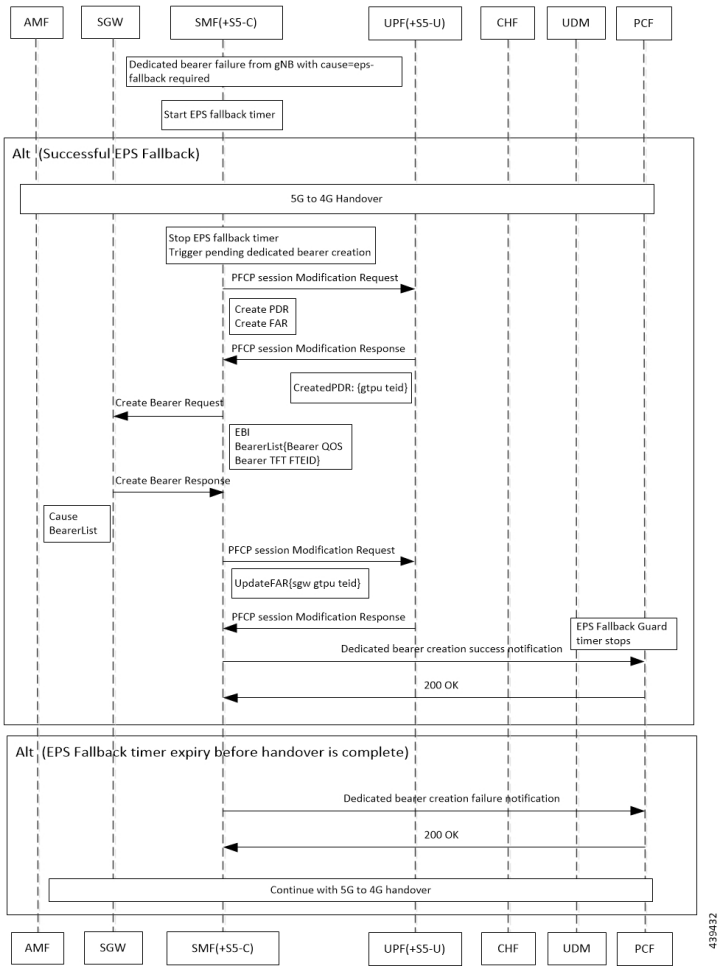


Table 57: MME-Initiated Bearer Modification for EPS session on SMF Call Flow Description

Step	Description
1	HSS sends an Insert Subscriber Data message to the MME. The subscription data includes the details on IMSI, EPS subscribed QoS (QCI and ARP), and the subscribed UE-AMBR and APN-AMBR.
2	If the subscribed UE-AMBR is modified, the MME calculates a new UE-AMBR value and sends the Modify Bearer Command to SGW.
3	SGW sends the Modify Bearer Command message to the SMF or PDN GW. This message includes the details on EPS Bearer Identity, EPS Bearer QoS, and APN-AMBR.
4	SMF or PDN GW sends the updated APN-AMBR to PCF.
5	PCF sends the updated PCC decision to the SMF or PDN GW. The PCF modifies the APN-AMBR that is associated with the default bearer in response to the SMF or PDN GW.
6	SMF sends the Update Bearer Request to SGW.
7	SGW sends the Update Bearer Request to MME. This request message includes the details on EBI, EPS Bearer QoS, TFT, and APN-AMBR.
8	MME sends the Update Bearer Response to SGW.
9	SGW sends the Update Bearer Response as acknowledgment for the bearer modification to the SMF or PDN GW. The response message includes the details on EBI and user location information.
10	UPF sends the PFCP Session Modification Response to SMF. Based on the PCC decision provision message (QoS policy) that is received from the PCF, the SMF or PDN GW initiates the dedicated bearer modification procedure. SMF or PDN GW uses the QoS policy to determine if a service data flow is to be added or removed from an active bearer or if the authorized QoS of a service data flow is changed.
11	UPF updates the PFCP parameters and sends a PFCP Session Modification Response to the SMF or PDN GW. UPF confirms the successful modification of the PFCP session.
12	SMF or PDN GW notifies PCF on the requested PCC decision whether it was enforced or not.
13	PCF sends the “200 OK” acknowledgment to SMF or PDN GW.

X2 and S1 based Handover for EPS Session Connected to SMF

This section describes the X2 and S1-Based Handover for EPS Session Connected to SMF.

Figure 45: X2 and S1 based Handover for EPS Session Connected to SMF

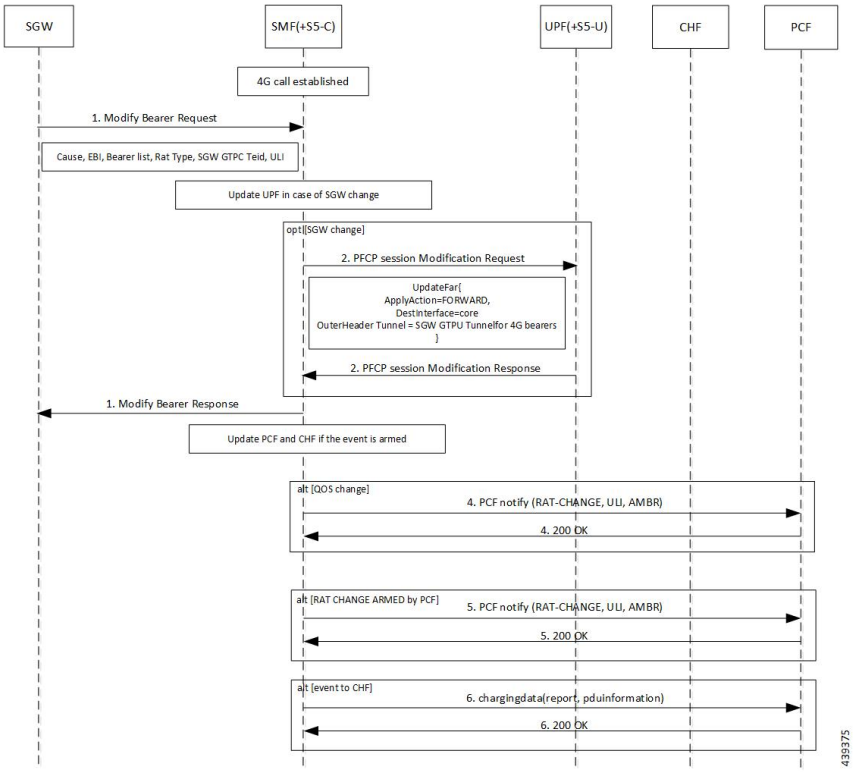


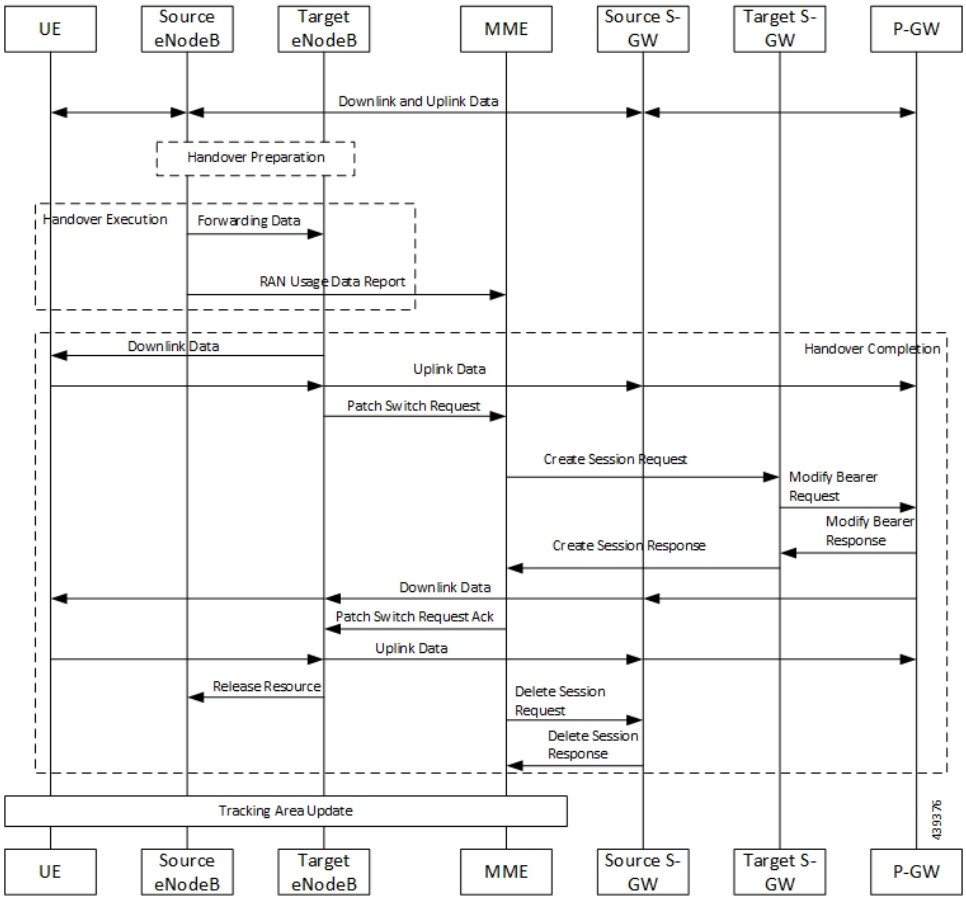
Table 58: X2 and S1 based Handover Call Flow Description

Step	Description
1	The SGW sends the Modify Bearer Request to the SMF. This request includes the user location information IE, UE time zone IE, and the serving network IE per PDN connection to the associated PDN GWs information that is received from the MME.
2	In case of change in S-GW, SMF or P-GW sends the PFCP Session Modification Request to the UPF.
3	If Step 2 occurs, the UPF sends the PFCP Session Modification Response to SMF or PDN GW.
4	After receiving the response from the UPF, the SMF or P-GW sends the Modify Bearer Response to S-GW.
5	If PCF has armed notification for QoS modification, the SMF or P-GW sends a notification to the PCF.
6	If Step 5 occurs, the PCF sends the “200 OK” acknowledgment to the SMF or P-GW.
7	If PCF has armed notification for ULI or RAT modifications, SMF or PDN GW sends a notification to PCF.
8	If Step 7 occurs, PCF sends the “200 OK” acknowledgment to SMF or PDN GW.
9	If CHF has armed notification for QoS, ULI, or RAT modifications, SMF or PDN GW sends a notification to PCF.

Step	Description
10	If Step 9 occurs, PCF sends the “200 OK” acknowledgment to SMF or PDN GW.

The following call flow shows the X2-based handover with S-GW relocation:

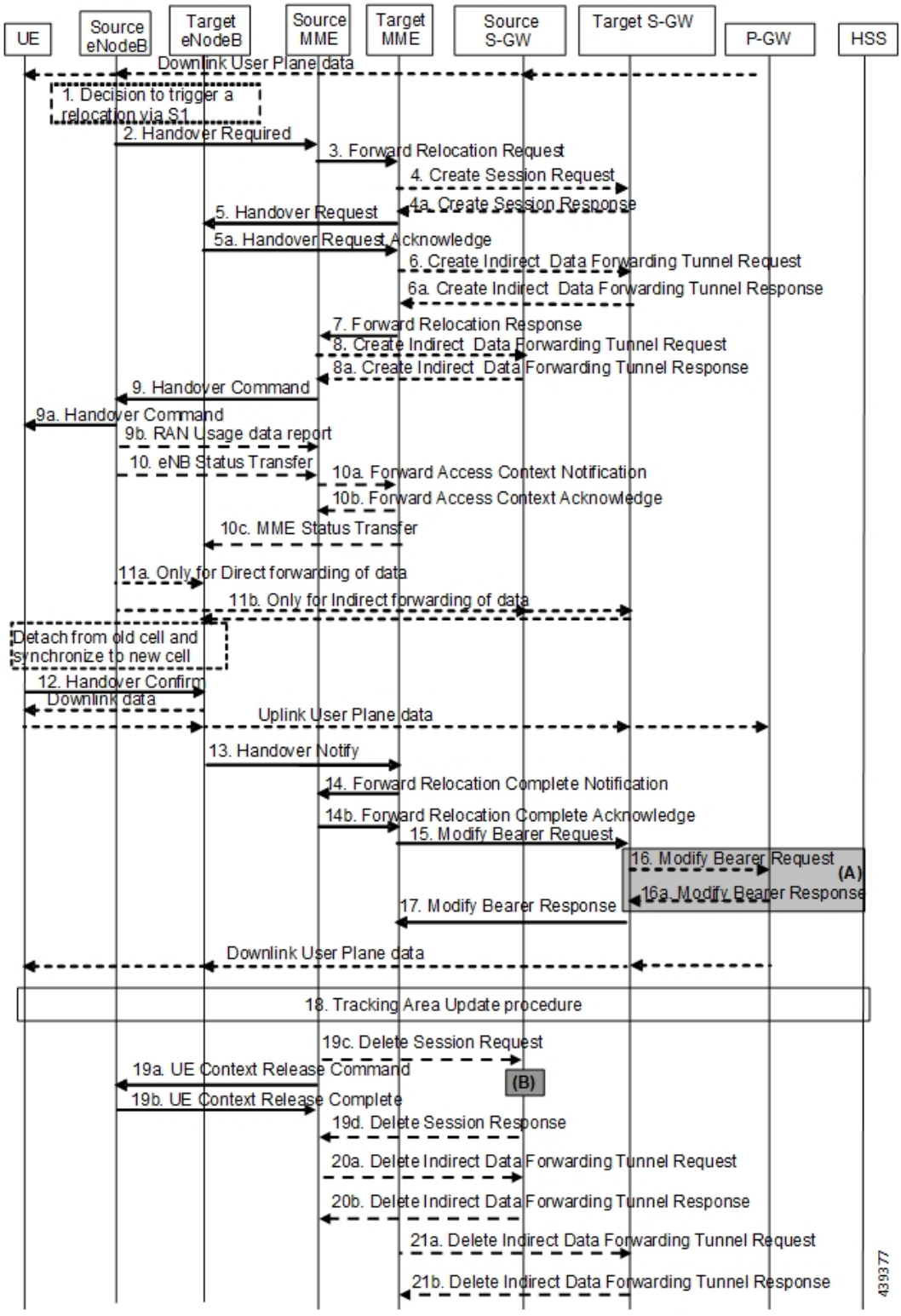
Figure 46: X2-Based Handover with SGW Relocation Call Flow



For call flow description, see the section 5.5.1.1.3 "X2-based handover with Serving GW relocation" from 3GPP TS 23.401.

The following call flow shows the S1-based handover:

Figure 47: S1-based Handover Call Flow



For call flow description, see section 5.5.1.2.2 "S1-based handover, normal" from 3GPP TS 23.401.

Standards Compliance

The Bearer Modification for EPS Session on SMF feature complies with the following standards:

- 3GPP TS 23.401
- 3GPP TS 23.502 V16.1.1 (2019-06)

Session Management Procedures for EPS and 5GC Interworking

Feature Description

The 5G Session Management procedures defined in 3GPP TS 23.502 ensure that the EPS interworking is successful when the UE moves to an LTE 4G radio after performing the initial attach to a 5G NR radio.

Support for Number of Packet Filters in NAS Message

The UE sends the Number of packet filter IE to the SMF in PDU Establishment and Modification request messages. By default, the UE sends a maximum of 16 packet filters.

The UE supports more than 16 packet filters in the following scenarios:

- When the UE is attaching to the SMF in N1 mode.
- When the initial attach to the SMF in S1 mode is complete and the 4G to 5G handover is ongoing.

The SMF sends the maximum filters to the PCF in PolicyCreateControl in "NumOfPackFilter" field. If the Number of packet filter IE is received from the UE in N1 mode, then the SMF uses the “Maximum number of supported filters” field in PDU establishment request. If this IE is not received from the UE in N1 mode or if the received value is lesser than 16, the SMF sends the max filters as 16. If the UE attaches to the SMF in S1 mode and the 4G to 5G or 5G to 4G handover is ongoing, the SMF sends the default value, that is, 16 packet filters.

If there is any change in the packet filter value, then the SMF sends the new value to the PCF through PolicyUpdate message along with NUM_OF_PACKET_FILTER trigger.

The SMF controls the maximum filters allowed per PDU session based on the numOfPackFilter IE. If the number of packet filters crosses the maximum allowed by the UE, the SMF caps the packet filters. This means that the SMF drops the PCC rules when the limit crosses and sends the rule report with INCOR_FLOW_INFO failure code.

Note INCOR_FLOW_INFO is not the correct failure code for this kind of deletion. Use the appropriate failure code when available in the 3GPP specification.

Maximum supported filters are only valid for dynamic rules and not for static and predefined rules.

The "pcc_rule_report_max_supported_filter" statistics is introduced under the policy_pcc_rule_report category. This statistics is incremented if the PCC rule report is generated upon reaching the maximum supported filters.

Support for PCF ID in SmContextCreate

The AMF includes the PCF ID in the Nsmf_PDUSession_CreateSMContext Request. The PCF ID identifies the Home Policy Control Function (H-PCF) in the non-roaming case and the Visited Policy Control Function (V-PCF) in the local breakout roaming case. See the 3GPP specification 23.501, section 6.3.7.1 for more details on when the AMF forwards the PCF ID to the SMF.

When the SMF receives the PCF ID, use the following CLI configuration in the PCF network profile to control the SMF behaviour in using the PCF ID.

UseAmfProvidedPCF [True/False]

The default behaviour is to use the PCF ID provided by AMF in SmContextCreate.

If the PCF ID provided by AMF is not reachable, the SMF behaves as per the configured failure handling template. In this case, it uses the static configuration.

Support for DNN Selection Mode in SmContextCreate

The SMF uses the DNN Selection Mode for deciding whether to accept or reject the UE request.

The SMF uses the DNN Selection Mode for deciding whether to retrieve the Session Management Subscription data. In case the DNN, S-NSSAI of the HPLMN is not explicitly subscribed, the SMF uses the local configuration instead of the Session Management Subscription data.

Note The preceding use case is not supported.

The SMF validates the IE present in SmContextCreate data. If there is a DnnSelectionMode failure due to the mismatch between DnnSelectionMode and the configured CLI, the SMF does not proceed with the registration. When the DnnSelectionMode failure is observed, the “disc_pdusetup_sm_cxt_unsupported_ie" is incremented as part of the disconnect reasons.

DnnSelectionMode Type	Description
Not Present	The SMF sends the subscription request to fetch the subscription data.
Verified	The SMF sends the subscription request to fetch the subscription data.
UE_DNN_NOT_VERIFIED	If the **dnn-selection-mode verified ue-provided** CLI command is configured as shown in the following configuration, the SMF sends the subscription request to fetch the subscription data. Otherwise, the SMF rejects the Context Request with "Invalid DNN selection Mode" cause.
NW_DNN_NOT_VERIFIED	If the **dnn-selection-mode verified network-provided**CLI is configured, the SMF sends the subscription request to fetch the subscription data. Otherwise, the SMF rejects the Context Request with "Invalid DNN selection Mode" cause.

The SMF uses the following configuration to configure the DnnSelectionMode.

```
configure
  profile smf profile_name
    dnn-selection-mode [ verified ue-provided | network-provided ]
    end
```

One or more DnnSelectionMode types can be configured. By default, the DnnSelectionMode is verified.

Post the subscription request, if no subscription data is fetched from UDM, the SMF falls back to the local DNN profile for subscription data. Neither the subscription data is fetched from the UDM nor the local configuration is present, the SMF sends the SmContextCreateError with subscription failure.

How it Works

Call Flows

This section describes the 5G Session Management procedures to support EPS and 5GC interworking.

PDU Session Creation Call Flow

This section describes the PDU Session Creation procedure as specified in 3GPP TS 23.502, Section 4.3.2.2.1.

Figure 48: PDU Session Creation Call Flow

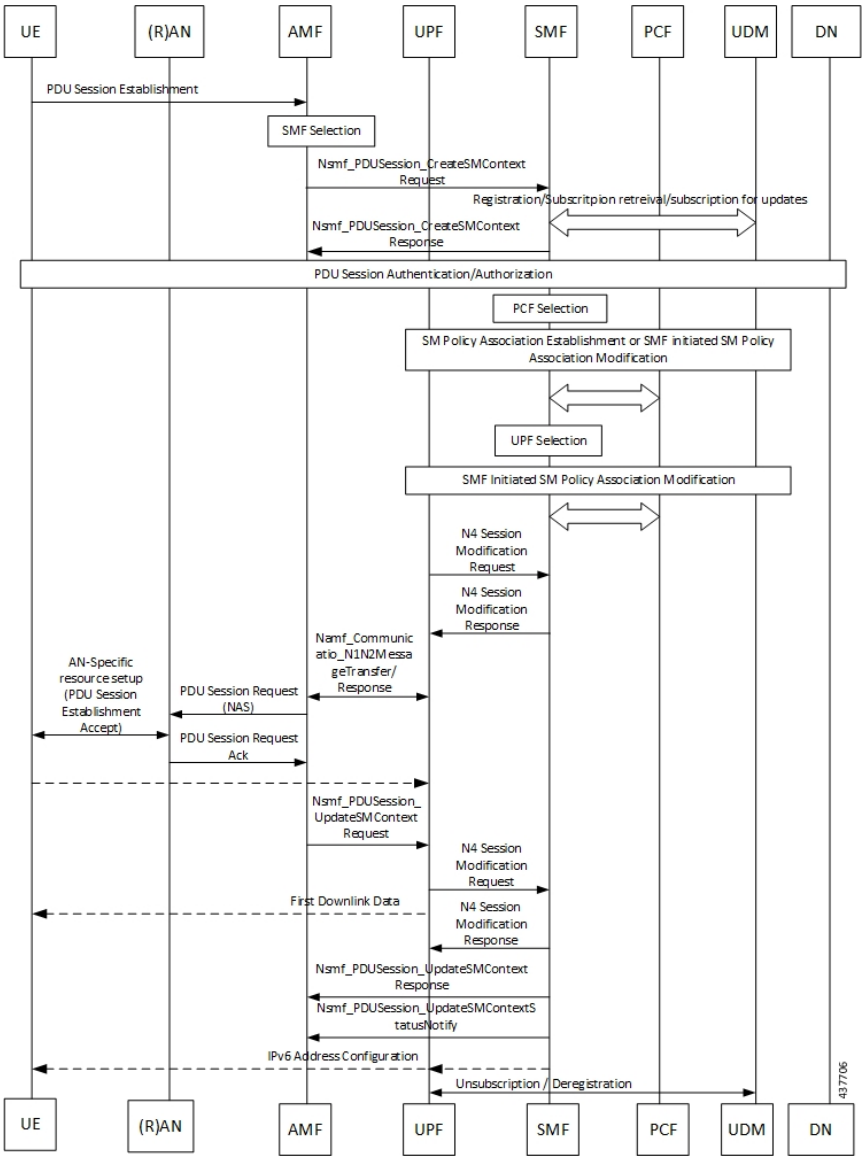


Table 59: PDU Session Creation Call Flow Description

Step	Description
1	The UE initiates the UE Requested PDU Session Establishment procedure by transmitting a NAS message containing a PDU Session Establishment Request within the N1 SM container. The PDU Session Establishment Request includes a PDU session ID, Requested PDU Session Type, a Requested SSC mode, 5GSM Capability PCO, SM PDU DN Request Container, Number of Packet Filters, and optionally Always-on PDU Session Requested.
2	The AMF performs SMF selection as described in 3GPP specification.

Step	Description
3	The AMF includes EPS Interworking Indication in the Nsmf_PDUSession_CreateSMContext Request message sent to the SMF. This parameter indicates whether the UE can perform 4G to 5G handover (and vice versa) and if it is allowed with or without the presence of the N26 interface between the AMF and MME.
4	If the EPS Interworking Indication received from the AMF indicates that the UE supports EPS interworking and the SMF determines (for example, if EPS interworking is allowed for this DNN and S-NSSAI based on UE subscription data) that the PDU session supports EPS interworking, the PGW-C+SMF FQDN for the S5/S8 interface is included in the Nudm_UECM_Registration Request message.
5	The SMF sends either Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID or N1 SM container (PDU Session Reject (Cause))) or an Nsmf_PDUSession_UpdateSMContext Response depending on the Request received in Step 3. If the SMF received Nsmf_PDUSession_CreateSMContext Request in Step 3 and the SMF can process the PDU Session Establishment Request, the SMF creates an SM context and responds to the AMF by providing an SM Context Identifier.
6	(Optional). If the Request Type in Step 3 indicates "Existing PDU Session", the SMF does not perform secondary authorization and authentication. If the Request Type received in Step 3 indicates "Emergency Request" or "Existing Emergency PDU Session", the SMF does not perform secondary authorization and authentication. If the SMF needs to perform secondary authorization and authentication during the establishment of the PDU Session by a DN-AAA server as described in 3GPP TS 23.501, Section 5.6.6, the SMF triggers the PDU session establishment authentication and authorization as described in 3GPP TS 23.501, Section 4.3.2.3.
7a	If dynamic PCC is to be used for the PDU Session, the SMF performs PCF selection as described in 3GPP TS 23.501, Section 6.3.7.1. If the Request Type indicates "Existing PDU Session" or "Existing Emergency PDU Session", the SMF uses the PCF already selected for the PDU Session. Otherwise, the SMF may apply local policy.
7b	The SMF performs the mapping of PCC rules and 5G QoS parameters to 4G TFTs and 4G QoS as described in the Generating EPS PDN Connection Parameters from 5G PDU Session Parameters section in this document. Based on the QoS flows, the SMF+PGW-C also determines the number of dedicated bearers required for the session when it hands off to EPS and the required flows (all non-GBR flows) in the default bearer. The SMF+PGW-C saves the mapping of 5G flows to 4G bearers.
8	If the Request Type in Step 3 indicates "Initial request", the SMF selects an SSC mode for the PDU Session as described in 3GPP TS 23.501, Section 5.6.9.3. The SMF also selects one or more UPFs as needed as described in 3GPP TS 23.501, Section 6.3.3.

Step	Description
9	The SMF performs an SMF-initiated SM Policy Association Modification procedure as defined in 3GPP TS 23.502, Section 4.16.5.1 to provide information on the Policy Control Request Trigger conditions that have been met. If Request Type is "initial request" and dynamic PCC is deployed and PDU Session Type is IPv4 or IPv6 or IPv4v6, the SMF notifies the PCF (if the Policy Control Request Trigger condition is met) with the allocated UE IP address/prefix(es). SMF+PGW-C initiates the EBI allocation procedure as defined in 3GPP TS 23.502, Section 4.11.1.4.
10	If the Request Type indicates "initial request", the SMF initiates an N4 Session Establishment procedure with the selected UPF. Otherwise, it initiates an N4 Session Modification procedure with the selected UPF. If multiple UPFs are selected for the PDU Session, the SMF initiates N4 Session Establishment/Modification procedure with each UPF of the PDU Session in this step.
11	In the non-roaming or LBO scenario, the PGW-C+SMF includes the mapped EPS bearer context(s) and the corresponding QoS flow(s) to be sent to the UE in the N1 SM container. The PGW-C+SMF also indicates the mapping between the QoS flow(s) and mapped EPS bearer context(s) in the N1 SM container. The PGW-C+SMF also includes the mapping between the received EBI(s) and QFI(s) in the N2 SM information to be sent to the NG-RAN. The PGW-C+SMF sends the N1 SM container and N2 SM information to the AMF through the Namf_Communication_N1N2MessageTransfer message.
12	The AMF sends N2 PDU Session Request (N2 SM information, NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept))) to the (R)AN. The AMF sends the NAS message containing PDU Session ID and PDU Session Establishment Accept targeted to the UE and the N2 SM information received from the SMF within the N2 PDU Session Request to the (R)AN.
13	The (R)AN may issue AN-specific signaling exchange with the UE that is related with the information received from the SMF. For example, in case of an NG-RAN, an RRC Connection Reconfiguration may take place with the UE establishing the necessary NG-RAN resources related to the QoS rules for the PDU Session Request received in Step 12.
14	(R)AN issues N2 PDU Session Response (PDU Session ID, Cause, N2 SM information (PDU Session ID, AN Tunnel Info, List of accepted/rejected QFI(s), User Plane Enforcement Policy Notification)) to the AMF.
15	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type) to the SMF. The AMF forwards the N2 SM information received from (R)AN to the SMF.
16a	The SMF initiates an N4 Session Modification procedure with the UPF. The SMF provides AN Tunnel Information and the corresponding forwarding rules to the UPF.

Step	Description
16b	The UPF provides an N4 Session Modification Response to the SMF. If multiple UPFs are used in the PDU session, the UPF in Step 16a refers to the UPF terminating N3. After this step, the UPF delivers any downlink packets to the UE that may have been buffered for this PDU session.
17	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (Cause) to the AMF.
18	(Conditional) The SMF sends Nsmf_PDUSession_SMContextStatusNotify (Release) to the AMF. If during the procedure, any time after Step 5, the PDU Session establishment is not successful, the SMF informs the AMF by invoking Nsmf_PDUSession_SMContextStatusNotify (Release). The SMF also releases any N4 session(s) created, any PDU session address if allocated (for example, IP address) and releases the association with PCF, if any.
19	If the PDU Session Type is IPv6 or IPv4v6, the SMF generates an IPv6 Router Advertisement and sends it to the UE via N4 and the UPF.
20	If the PDU Session Establishment failed after Step 4, the SMF performs the following: • The SMF unsubscribes to the modifications of Session Management Subscription data for the corresponding (SUPI, DNN, S-NSSAI), using Nudm_SDM_Unsubscribe (SUPI, Session Management Subscription data, DNN, S-NSSAI), if the SMF is no more handling a PDU session of the UE for this (DNN, S-NSSAI). The UDM may unsubscribe to the modification notification from UDR by Nudr_DM_Unsubscribe (SUPI, Subscription Data, Session Management Subscription data, S-NSSAI, DNN). • The SMF deregisters for the given PDU session using Nudm_UECM_Deregistration (SUPI, DNN, PDU Session ID). The UDM may update corresponding UE context by Nudr_DM_Update (SUPI, Subscription Data, UE context in SMF data).

PDU Session Modification Call Flow

This section describes the PDU session modification procedure as specified in 3GPP TS 23.502, Section 4.3.3.2.

Figure 49: PDU Session Modification Call Flow

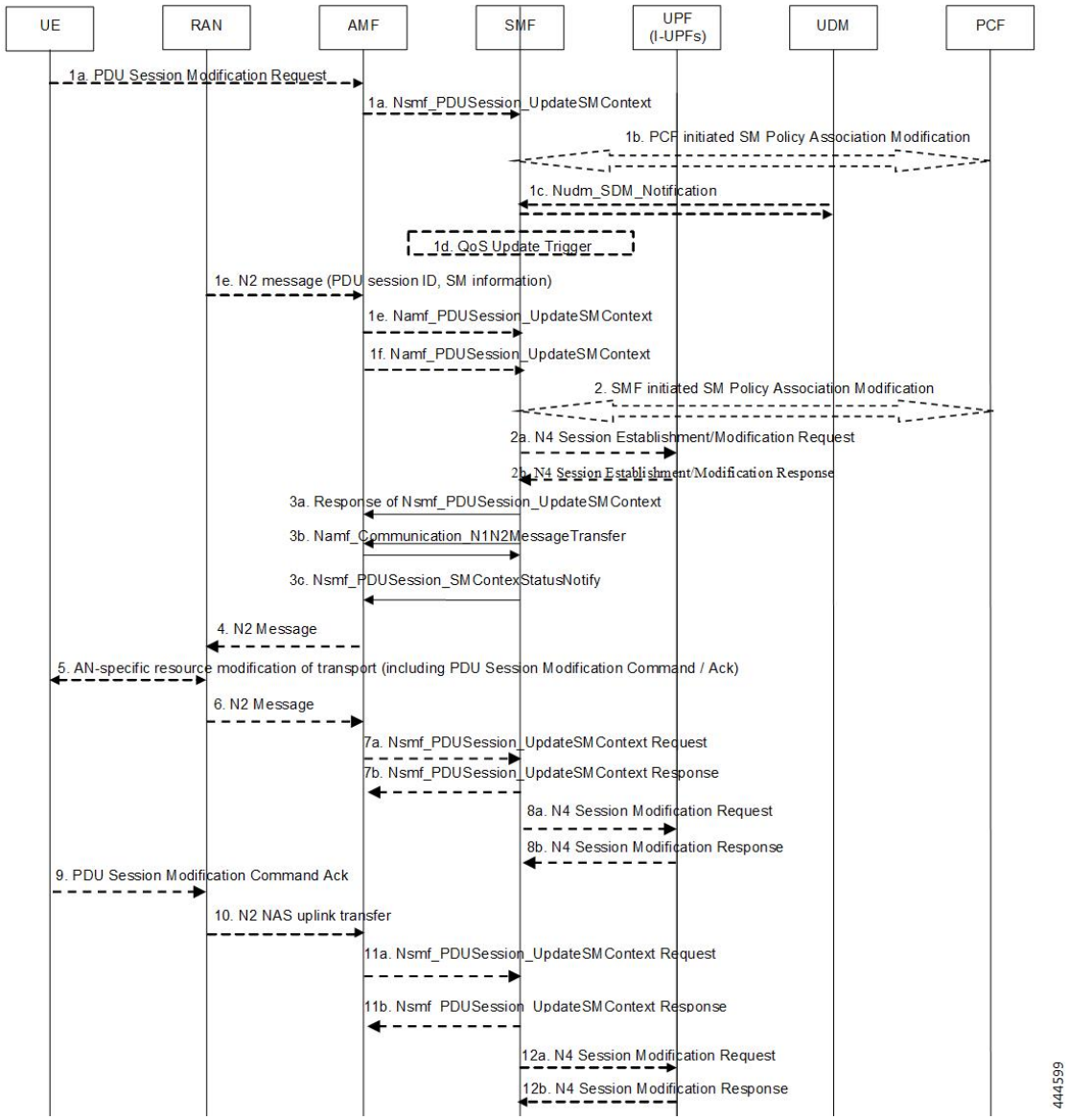


Table 60: PDU Session Modification Call Flow Description

Step	Description
1a	The UE initiates the UE Requested PDU Session Modification procedure by transmitting a NAS message containing a PDU Session Modification Request within the N1 SM container. The PDU Session Modification Request includes a PDU session ID, Packet Filters, Operation, Requested QoS, Segregation, and 5GSM Core Network Capability.
1b	(SMF-requested modification) The PCF performs a PCF-initiated SM Policy Association Modification procedure to notify the SMF about the modification of policies. The policy decision or upon AF requests, for example, Application Function influence on traffic routing, triggers this procedure.

Step	Description
1c	(SMF-requested modification) The UDM updates the subscription data of SMF by Nudm_SDM_Notification (SUPI, Session Management Subscription Data). The SMF updates the Session Management Subscription Data and acknowledges the UDM by returning an Ack with (SUPI).
1d	(SMF-requested modification) The SMF decides to modify PDU session. This procedure is also triggered based on locally configured policy or triggered from the (R)AN. If the SMF receives one of the triggers in step 1b to 1d, the SMF starts SMF-requested PDU Session Modification procedure.
1e	(AN-initiated modification) (R)AN indicates to the SMF when the AN resources onto which a QoS Flow is mapped are released irrespective of whether notification control is configured. (R)AN sends the N2 message (PDU Session ID, N2 SM information) to the AMF. The N2 SM information in the smf_PDU_Session_UpdateContext includes the following information: • QoS Flow Identifier (QFI) • User location Information • QoS Flow Release List IE - list of QoS flows which are released by NG-RAN node • QoS Flow Notify List IE and Notification Cause IE - list of GBR QoS flows that fulfilled a specific criteria, and the flows that missed fulfilling the criteria The SMF supports AN-initiated modification to release the QFI from RAN. For details on this support, see the following section.
2	The SMF reports the subscribed event to the PCF by performing an SMF-initiated SM Policy Association Modification procedure. The SMF skips this step if the PDU Session Modification procedure is triggered by step 1b or 1d. If the dynamic PCC is not deployed, the SMF may apply local policy to decide whether to change the QoS profile. The SMF does not invoke the steps 3 to 7 when the PDU Session Modification requires only action at a UPF (for example, gating).
3a	For UE or AN-initiated modification, the SMF responds to the AMF through Nsmf_PDUSession_UpdateSMContext including N2 SM information and N1 SM container. The N2 SM information carries information that the AMF provides to the (R)AN. It includes the QoS profiles and the corresponding QFIs to notify the (R)AN that one or more QoS flows were added, or modified. It includes only QFI(s) to notify the (R)AN that one or more QoS flows were removed. The N1 SM container carries the PDU Session Modification Command that the AMF provides to the UE. It includes the QoS rule(s), QoS rule operation, QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s), and Session-AMBR.

Step	Description
3b	For SMF-requested modification, the SMF invokes Namf_Communication_N1N2MessageTransfer including N2 SM information and N1 SM container. If the UE is in CM-IDLE state and an Asynchronous type communication (ATC) is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer, and skips the steps 4, 5, 6 and 7. When the UE is reachable, that is, when the UE enters CM-CONNECTED state, the AMF forwards the N1 message to synchronize the UE context with the UE.
4	The AMF sends N2 PDU Session Request (N2 SM information received from the SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) Message to the (R)AN.
5	The (R)AN issues AN-specific signalling exchange with the UE that is related with the information received from the SMF. For example, in an NG-RAN, an RRC Connection Reconfiguration takes place with the UE modifying the necessary (R)AN resources related to the PDU session.
6	The (R)AN acknowledges N2 PDU Session Request by sending a N2 PDU Session Ack Message to the AMF.
7	The AMF forwards the N2 SM information and the User location Information from the AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. The SMF sends Nsmf_PDUSession_UpdateSMContext Response. If the (R)AN rejects QFI(s), the SMF updates the QoS rules and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s) in the UE accordingly.
8	The SMF updates N4 session of the UPF(s) that are involved by the PDU Session Modification by sending N4 Session Modification Request message to the UPF.
9	The UE acknowledges the PDU Session Modification Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command Ack)).
10	The (R)AN forwards the NAS message to the AMF.
11	The AMF forwards the N1 SM container (PDU Session Modification Command Ack) and User Location Information from the AN to the SMF through Nsmf_PDUSession_UpdateSMContext service operation. The SMF sends Nsmf_PDUSession_UpdateSMContext Response.
12	The SMF updates N4 session of the UPF(s) that are involved by the PDU Session Modification by sending N4 Session Modification Request (N4 Session ID) message to the UPF. For a PDU Session of Ethernet PDU Session Type, the SMF notifies the UPF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s).

Step	Description
13	If the SMF interacts with the PCF in step 1b or 2, the SMF notifies the PCF whether the PCC decision is enforced or not by performing an SMF-initiated SM Policy Association Modification procedure. The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change. If the step 1b is triggered to perform Application Function influence on traffic routing, the SMF reconfigures the User Plane of the PDU session.

Releasing QFI During AN-initiated Modification Procedure

For the SMF to support AN-initiated modification to release the QFIs, perform the following steps:

1. If the EPS Interworking Indication is enabled for a given PDU session, the SMF initiates the EBI release towards the AMF.
2. The SMF sends N4 Modification to the UPF to delete the Packet Detection Rule (PDR), QoS Enforcement Rule (QER), and Usage Reporting Rule (URR) related to the flows being released.
3. The SMF initiates N1N2TransferMessage containing N1 PDU Session Modification command. This message includes information about the deleted flows, Mapped EPS Bearer Context.
4. Then, the SMF interacts with the PCF to report the flows released for the rules if “RES_RELEASE” trigger is set.

Note The "policy_pdu_flows_total" statistics is available to check the released flows.

EPS Interworking Indication in PDU Session Modification

The EpsInternetworkingIndication field denotes the possibility of handover between EPS and 5GC. This field holds the following values:

- NONE: The PDU session cannot be moved to EPS.
- WITH_N26: The PDU session is moved to EPS, with N26 interface supported during EPS interworking procedures.
- WITHOUT_N26: The PDU session is moved to EPS, without N26 interface supported during EPS interworking procedures.

The SMF allows the 4G to 5G handover and vice-versa only if the EpsInternetworkingIndication value is set to WITH_N26. For other values of EpsInternetworkingIndication, the SMF rejects the handovers.

During 4G and 5G PDU session establishment, if the EPS internetworking indication is received from the AMF, the SMF includes PGW-C+SMF FQDN for S5/S8 interface in the UDM Registration request.

With the EPS Interworking Indication Support Enabled:

If the EpsInternetworkingIndication value changes from NONE or WITHOUT_N26 to WITH_N26 for a created PDU session, follow these steps to support the EPS Interworking Indication change in the PDU modification procedure.

1. The AMF invokes the Nsmf_PDUSession_UpdateSMContext request with the changed EpsInterworkingIndication value.
2. The SMF receives the Nsmf_PDUSession_UpdateSMContext request from the AMF, and initiates the Namf_Communication_EbiAssignmentRequest. This request includes the PDU Session ID and Allocation/Retention Priority (ARP) List.
3. The AMF sends Namf_Communication_EbiAssignmentResponse to the SMF. The AMF sends the following through the response:
   - assignedEbiList containing the successfully assigned EBIs.
   - failedArpList containing the failed ARPs for which the EBI assignment failed.
   - 4XX/5XX error along with AssignEbiError representing the EBI assignment failure.
4. The SMF sends N1N2MessageTransfer request message if the EBIs are created successfully. This request includes the following:
   - N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Create])
   - N2:N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER (QoS Flow Add or Modify Request Item with EPS Radio Access Bearer (E-RAB) ID and QoS Flow ID)

Note If the UE is in Idle mode, the SMF skips sending the N2 message.

5. The SMF informs mapped EPS bearer context in the UE using N1 message. The SMF waits for N1: PDU SESSION MODIFICATION COMPLETE message.
6. The SMF informs EBI to QoS Flow Identifier (QFI) mapping to gNodeB using N2 message. The SMF waits for N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER message.
7. The SMF completes the PDU Session Modification procedure.

With the EPS Interworking Indication Support Disabled:

If the EpsInternetworkingIndication value changes from WITH_N26 to NONE or WITHOUT_N26 for a created PDU session, follow these steps to support the EPS Interworking Indication change in the PDU modification procedure.

1. The SMF receives the Nsmf_PDUSession_UpdateSMContext request with the changed EpsInterworkingIndication value from the AMF.
2. The SMF sends N1N2MessageTransfer request message. This request includes the following:
   - N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Delete])
   - N2:N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER

Note If the UE is in Idle mode, the SMF skips sending the N2 message.

3. The SMF deletes Mapped EPS bearer context in UE using N1 message. The SMF waits for N1: PDU SESSION MODIFICATION COMPLETE message.
4. The SMF deletes EBI to QFI mapping to gNodeB using N2 message. The SMF waits for N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER message.
5. The SMF completes the PDU Session Modification procedure.

Use the **show subscriber** command to determine the EPS interworking status of the PDU session, and the EBI mapping for the QoS flows.

PDU Session Release Call Flow

The PDU Session Release procedure is used to release all the resources associated with a PDU session, including:

- The IP address/prefixes allocated for an IP-based PDU session
- Any UPF resource that was used by the PDU session.
- Any access resource that was used by the PDU session.

The SMF notifies any entity associated with the PDU session: PCF, Data Network (DN) (for example, when DN authorization has taken place at PDU session establishment), and so on.

There are different ways to initiate the PDU session release. It can be from UE, network, AMF, or RAN.

UE-initiated PDU Session Release Call Flow

The UE-initiated PDU session release procedure allows the UE to request the release of the PDU session. In the case of Local Breakout (LBO), the procedure is as in the case of non-roaming with the difference that the AMF, the SMF, the UPF, and the PCF are located in the visited network.

The following figure depicts the UE-initiated PDU session release procedure to support EPS interworking on the SMF as specified in 3GPP TS 23.502, section 4.3.4.2.

Figure 50: UE-initiated PDU Session Release Call Flow

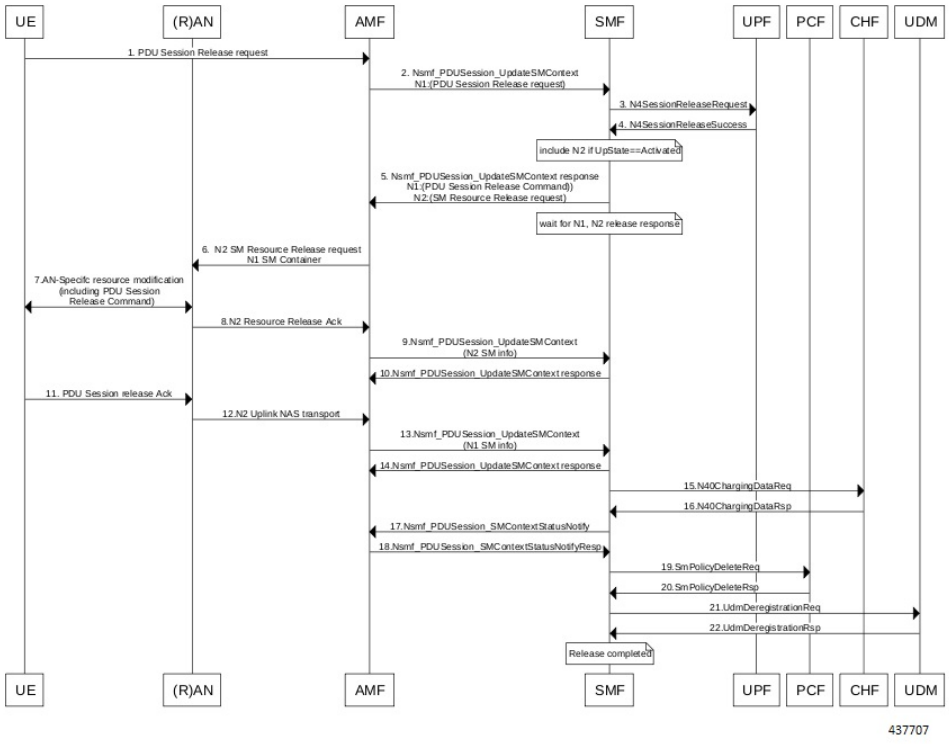


Table 61: UE-initiated PDU Session Creation Call Flow Description

Step	Description
1, 2	The UE sends PDU_SESSION_RELEASE_REQUEST in NAS message to the AMF through the RAN. The AMF sends the message to the SMF in SmContextUpdateRequest.
3, 4	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.
5	The SMF sends SmContextUpdateResponse message with N1 and N2 content. • N1: PDU_SESSION_RELEASE_COMMAND • N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 8, 9, and 10.
6, 7	The AMF exchanges the message with RAN. The RAN forwards it to the UE.
8, 9, 10	The RAN sends N2 release response to the AMF. The AMF sends N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.

Step	Description
11, 12, 13, 14	The UE sends N1 release response in NAS message to the AMF through the RAN. The AMF sends N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
15, 16	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
17, 18	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with SmContextStausNotifyResponse message.
19, 20	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response
21, 22	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

Network-initiated PDU Session Release Call Flow

The network-initiated PDU session release procedure allows the AMF, the SMF or the PCF to initiate the release of a PDU session.

The following figure depicts the network-initiated PDU session release call flow.

Figure 51: Network-initiated PDU Session Release Call Flow

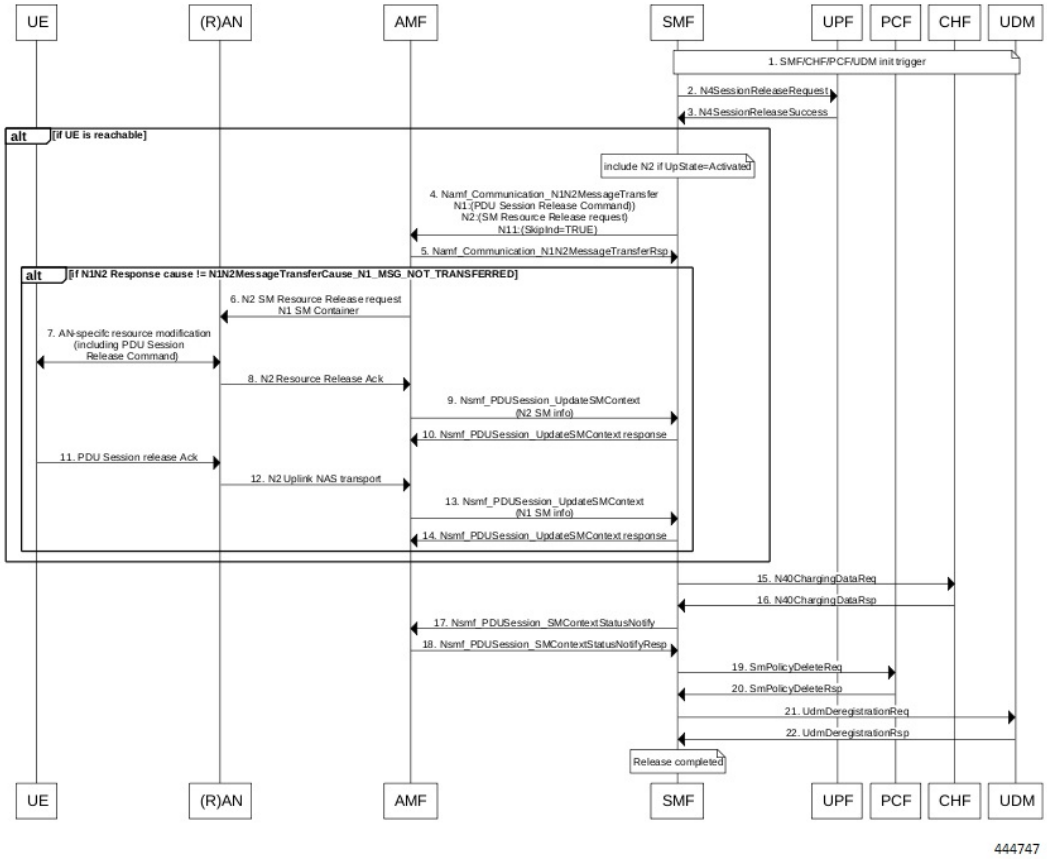


Table 62: Network-initiated PDU Session Creation Call Flow Description

Step	Description
1	This procedure can be triggered by PCF, CHF, UDM, UPF or CLI (clear subscriber) to initiate the release of a PDU session.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same. **Note** Skip the steps 4 to 14 if the AMF has notified that the UE is not reachable.
4	The SMF sends N1N2MessageTransfer message with N11, N1 and N2 content. • N11: SkipInd=True • N1: PDU_SESSION_RELEASE_COMMAND • N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 8, 9, and 10.

Step	Description
5	The AMF responds back to the SMF with the cause included in the N1N2MessageTransferRsp message. **Note** Skip the steps 6 to 14 if the AMF sends the cause as N1_MSG_NOT_TRANSFERRED in step 5.
6, 7	The AMF exchanges the message with RAN. The RAN forwards it to the UE.
8, 9, 10	The RAN sends N2 release response to the AMF. The AMF transfers N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
11, 12, 13, 14	The UE sends N1 release response in the NAS message to the AMF through the RAN. The AMF sends the N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
15, 16	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
17, 18	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with the SmContextStausNotifyResponse message.
19, 20	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
21, 22	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

AMF-initiated PDU Session Release

The AMF-initiated PDU session release procedure allows the AMF to initiate the release of a PDU session.

The following figure depicts the AMF-initiated PDU session release call flow.

Figure 52: AMF-initiated PDU Session Release Call Flow

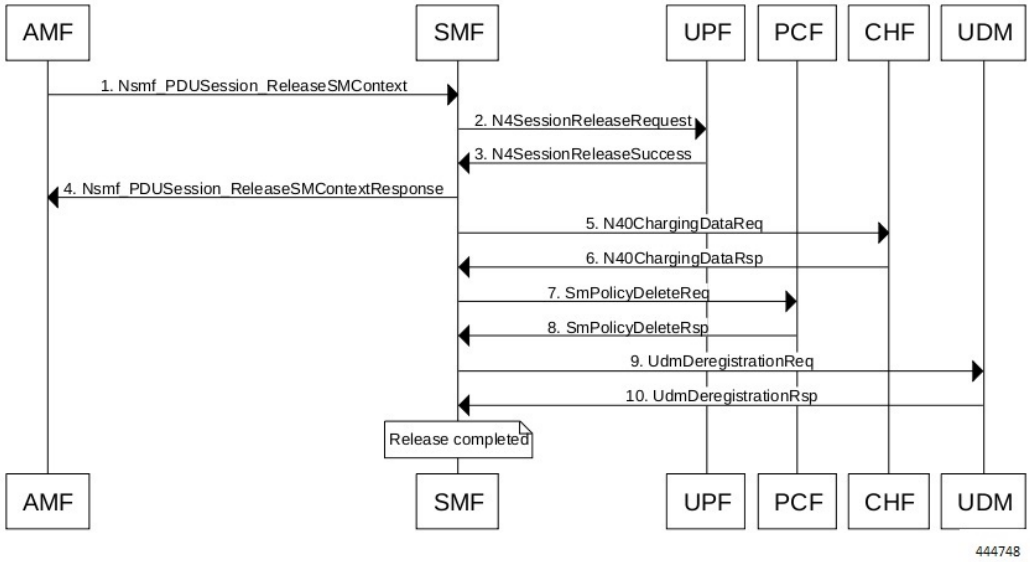


Table 63: AMF-initiated PDU Session Creation Call Flow Description

Step	Description
1	The AMF sends SmContextReleaseRequest.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.
4	The SMF sends SmContextReleaseResponse to the AMF.
5, 6	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
7, 8	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
9, 10	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

AMF-initiated PDU Session Release with N11 Release=True

The AMF-initiated PDU session release procedure allows the AMF to initiate the release of a PDU session with the N11 release in the SmContextModifyRequest being set to True.

The following figure depicts the AMF-initiated PDU session release call flow with the N11 release=True.

Figure 53: AMF-initiated PDU Session Release with N11 Release=True

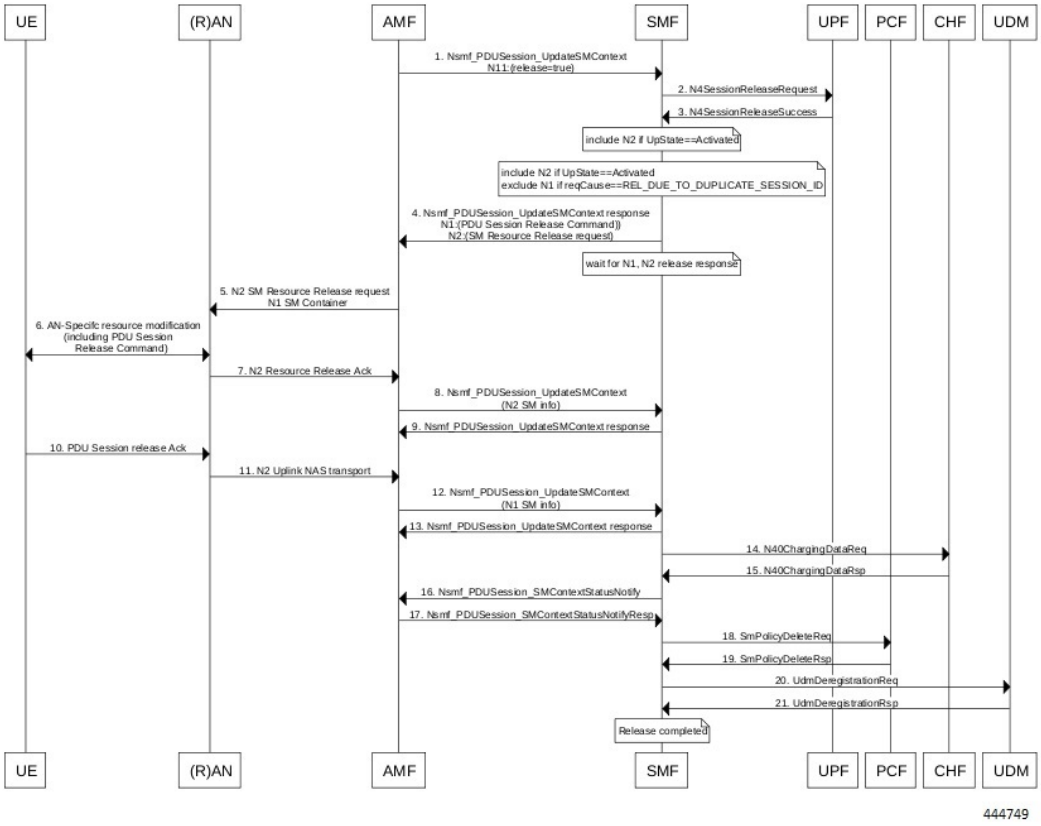


Table 64: AMF-initiated PDU Session Creation Call Flow (N11 release=true) Description

Step	Description
1	The AMF sends SmContextModifyRequest with release=True in 2 causes REL_DUE_TO_DUPLICATE_SESSION_ID or REL_DUE_TO_SLICE_NOT_AVAILABLE.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.
4	The SMF sends SmContextUpdateResponse message with N1 and N2 content. • N1: PDU_SESSION_RELEASE_COMMAND, exclude if cause is REL_DUE_TO_DUPLICATE_SESSION_ID, skip steps 10,11,12,13 • N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 7, 8, and 9.
5, 6	The AMF exchanges message with RAN. The RAN forwards it to the UE.

Step	Description
7, 8, 9	The RAN sends N2 release response to the AMF. The AMF sends N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
10, 11, 12, 13	The UE sends N1 release response in NAS message to the AMF through the RAN. The AMF sends N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
14, 15	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
16, 17	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with SmContextStausNotifyResponse message.
18, 19	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
20, 21	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

RAN-initiated PDU Session Release Call Flow

The RAN-initiated PDU session release procedure allows the RAN to initiate the release of a PDU session.

The following figure depicts the RAN-initiated PDU session release call flow.

Figure 54: RAN-initiated PDU Session Release Call Flow

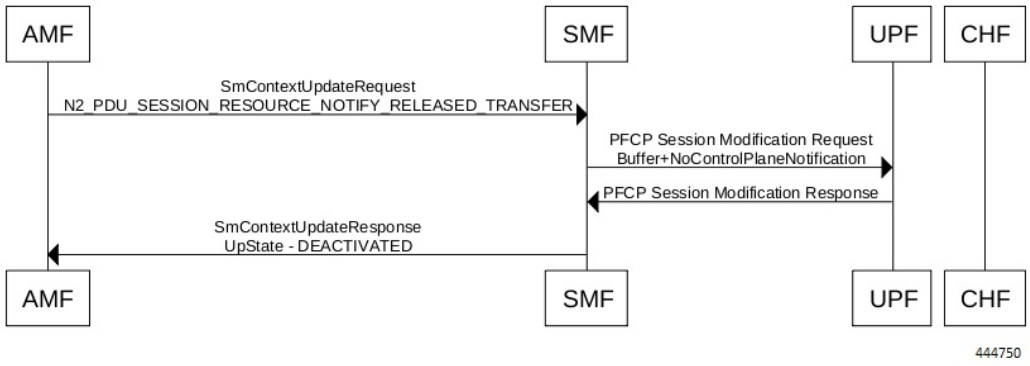


Table 65: AMF-initiated PDU Session Creation Call Flow Description

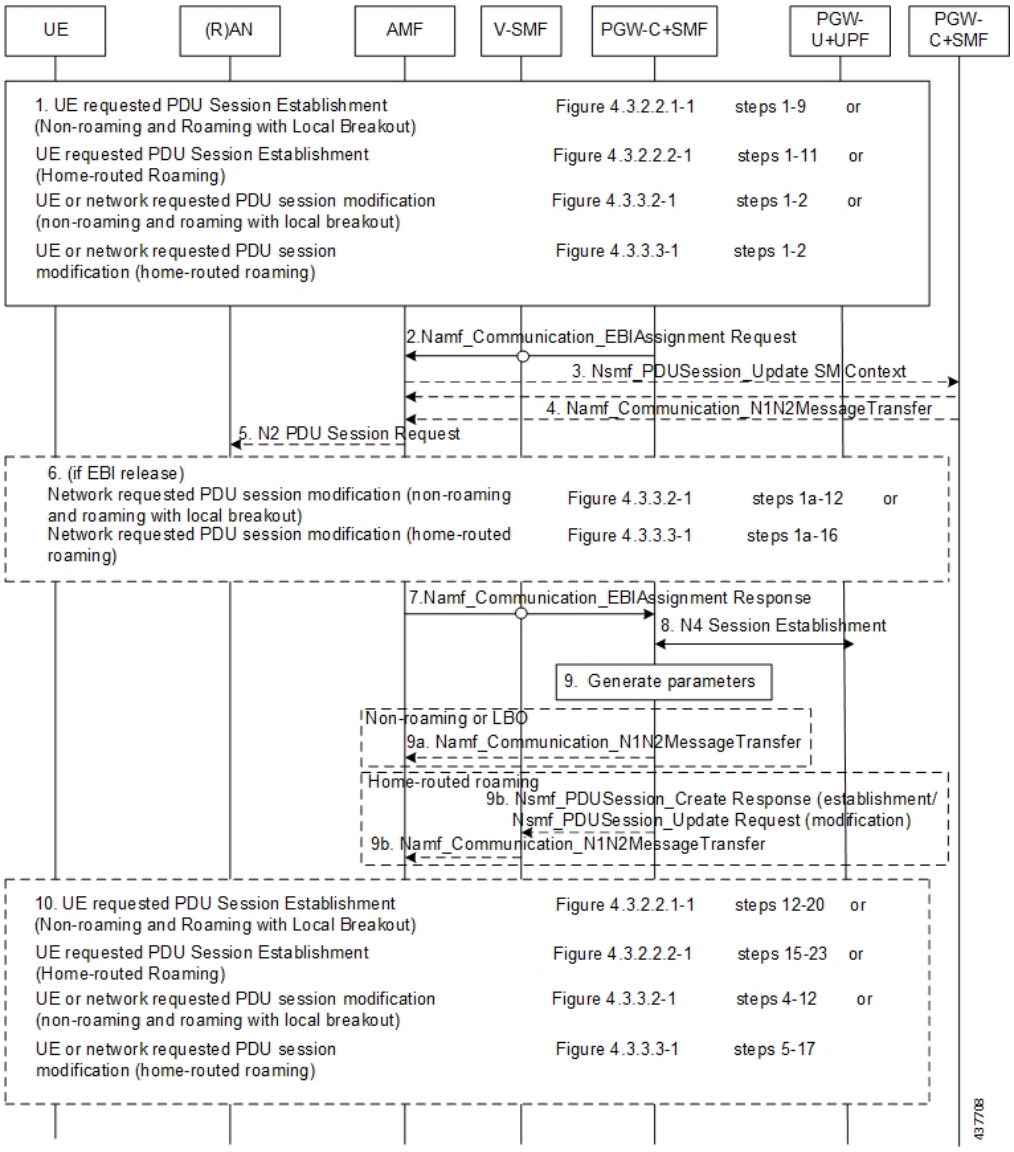
Step	Description
1	The AMF sends SmContextModifyRequest with N2 type: N2_PDU_SESSION_RESOURCE_NOTIFY_RELEASED_TRANSFER.

Step	Description
2, 3	The SMF sends N4SessionModificationRequest to the UPF with changing packet rule to Buffer from Forward. The UPF sends the response for the same, that is, the SMF moving to IDLE state.
4	The SMF sends SmContextUpdateResponse message with UpState as Deactivated.

EPS Bearer ID Allocation

This section describes the EPS Bearer ID Allocation procedure.

Figure 55: EPS Bearer ID Allocation Call Flow



Note Not all the steps in the preceding call flow are supported. For more details, see the descriptions in the following table.

Table 66: EPS Bearer ID Allocation Call Flow Description

Step	Description
1	The EBI Assignment procedure is initiated as specified in the relevant sections of 3GPP TS 23.502. The relevant steps of the procedure are executed as specified in the preceding call flow. **Note** Roaming scenarios are currently not supported.
2	If the PGW-C+SMF (or H-SMF for home-routed cases) determines that EPS bearer IDs (based on operator policies, S-NSSAI, User Plane Security Enforcement information) need to be assigned to the QoS flows in the PDU session, the PGW-C+SMF invokes Namf_Communication_EBIAssignment Request (PDU Session ID, ARP list).
Step 3 through Step 6 apply only when the AMF needs to revoke EBI that was previously allocated for a UE to serve a new SMF request of EBI for the same UE.	
3	(Conditional) If the AMF has no available EBIs, the AMF may revoke an EBI that was assigned to QoS flows based on the ARPs and S-NSSAI stored during PDU Session Establishment, EBI information in the UE context and local policies. If an assigned EBI is to be revoked, the AMF invokes Nsmf_PDUSession_UpdateSMContext (EBI(s) to be revoked) to request the related SMF (called “SMF serving the released resources”) to release the mapped EPS QoS parameters corresponding to the EBI to be revoked. The AMF stores the association of the assigned EBI, ARP pair to the corresponding PDU Session ID and SMF address.
4	The “SMF serving the released resources” that receives the request in Step 3 invokes Namf_Communication_N1N2Message Transfer (N2 SM information (PDU Session ID, EBI(s) to be revoked), N1 SM container (PDU Session Modification Command (PDU Session ID, EBI(s) to be revoked))) to inform the (R)AN and the UE to remove the mapped EPS QoS parameters corresponding to the EBI(s) to be revoked. In home-routed roaming scenario, the H-SMF includes EBI(s) to be revoked to V-SMF to inform V-SMF to remove the mapped EPS bearer context corresponding to the EBI(s) to be revoked. The SMF can also decide to remove the QoS flow if it is not acceptable to continue the service when no corresponding EPS QoS parameters can be assigned. For home-routed roaming scenario, the "SMF serving the released resources" sends an N4 Session Modification Request to request the PGW-U+UPF to release the N4 session corresponding to the revoked EBI(s). In home-routed roaming case, the V-SMF starts a VPLMN-initiated QoS Modification for the PDU session. The V-SMF invokes the Namf_Communication_N1N2Message Transfer based on the corresponding QoS modification message received from H-SMF.

Step	Description
5	If the UE is in CM-CONNECTED state, the AMF sends N2 PDU Session Request (N2 SM information received from SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) message to the (R)AN. If the UE is in CM-IDLE state and an ATC is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer and Step 5 and Step 6 are skipped. When the UE is reachable, for example, when the UE enters CM-CONNECTED state, the AMF forwards the N1 message to synchronize the UE context with the UE.
6	The relevant steps of the procedure are executed as specified in the preceding figure.
7	If the AMF successfully assigns EBI(s), it responds with the assigned EBI(s). Otherwise, it responds with a cause indicating EBI assignment failure. If a PDU session from another SMF already exists towards the same DNN, the AMF either rejects the EBI assignment request, or revokes the EBI(s) from the existing PDU session(s) to the same DNN but different SMF. The AMF makes the decision based on the operator policy. **Note** The preceding statement applies only when the S-NSSAI(s) for the PDU sessions are different, otherwise the same SMF is selected for PDU sessions to the same DNN.
8	The PGW-C+SMF sends an N4 Session Establishment/Modification Request to the PGW-U+UPF. For home-routed roaming scenario, if the EBI is assigned successfully, the PGW-C+SMF prepares the CN Tunnel Info for each EPS bearer. If the CN Tunnel info is allocated by the PGW-C+SMF, the PGW-U tunnel info for the EPS bearer may be provided to PGW-U+UPF. If the CN Tunnel info is allocated by PGW-U+UPF, the PGW-U+UPF sends the PGW-U tunnel info for the EPS bearer to the PGW-C+SMF. The PGW-U+UPF is ready to receive the uplink packets from E-UTRAN. **Note** In the home-routed roaming scenario, the PGW-C+SMF prepares the CN Tunnel Info for each EPS bearer and provides it to the V-SMF. Thus, when the UE moves to EPS network, the V-SMF does not need to interact with the PGW-C+SMF to get the EPS bearer context(s). **Note** If the CN Tunnel info is allocated by the PGW-C+SMF and not provided to PGW-U+UPF at PDU session establishment, when the UE moves to the target RAT the PGW-U+UPF cannot receive uplink (UL) data until the PGW-C+SMF has provided the Tunnel Info to the PGW-U+UPF in N4 Session Modification. This causes a short interruption to the UL data during the inter-system handover execution.

Step	Description
9	If the PGW-C+SMF receives any EBI(s) from the AMF, it adds the EBI(s) received into the mapped EPS bearer context(s). In home-routed roaming scenario, the PGW-C+SMF generates EPS bearer context, which includes per EPS bearer PGW-U tunnel information. In addition, if the default EPS bearer is generated for the corresponding PDN Connection of PDU Session (that is, during the PDU Session establishment procedure), the PGW-C+SMF generates the PGW-C tunnel information of the PDN connection and includes it in UE EPS PDN connection.
9a	(Conditional) In non-roaming or LBO scenario, the PGW-C+SMF includes the mapped EPS bearer context(s) and the corresponding QoS Flow(s) to be sent to the UE in the N1 SM container. PGW-C+SMF also indicates the mapping between the QoS flow(s) and mapped EPS bearer context(s) in the N1 SM container. PGW-C+SMF also includes the mapping between the received EBI(s) and QFI(s) in the N2 SM information to be sent to the NG-RAN. The PGW-C+SMF sends the N1 SM container and N2 SM information to the AMF via Namf_Communication_N1N2MessageTransfer.
9b	(Conditional) In home-routed roaming scenario, the PGW-C+SMF sends the mapped EPS bearer context(s), the mapping between the received EBI(s) and QFI(s), and EPS bearer context to the V-SMF via Nsmf_PDUSession_Create Response during PDU Session Establishment, or via Nsmf_PDUSession_Update Request during PDU Session Modification. The V-SMF stores the EPS bearer context, and generates N1 SM container and N2 SM information, and forwards them to the AMF via Namf_Communication_N1N2MessageTransfer.
10	The N1 SM container and N2 SM information are sent to the UE and NG-RAN respectively. The relevant steps of the procedure are executed as specified in the preceding figure.

Standards Compliance

This feature complies with the following standards:

- 3GPP TS 23.401, Version 15.6.0
- 3GPP TS 23.502, Version 15.4.0

Limitations

TFT IE in mapped EPS bearer context is currently not supported.

Generating EPS PDN Connection Parameters from 5G PDU Session Parameters

This section describes how to generate the EPS PDN connection parameters from the 5G PDU session parameters in the PGW-C+SMF.

When the PGW-C+SMF is requested to set up or modify a PDN connection or a PDU session that supports interworking between EPS and 5GC, the PGW-C+SMF generates the PDN connection parameters from the PDU session parameters.

When the PGW-C+SMF generates the PDN connection parameters based on the PDU session parameters, the following rules hold:

- PDN Type: The PDN type is set to IPv4 or IPv6 if the PDU Session Type is IPv4 or IPv6 respectively. The PDN type is set to Non-IP for Ethernet and Unstructured PDU Session Types.
- EPS Bearer ID: The EBI is requested from the AMF during the establishment of a QoS Flow as described in 3GPP TS 23.502, Section 4.11.1.4.1, for PDU sessions that support interworking between EPS and 5GC. The EBI is obtained from MME during the establishment of an EPS bearer (that is triggered by an establishment of the QoS Flow) as defined in 3GPP TS 23.401 for PDN connections hosted by PGW-C+SMF. The association between EBI and QoS Flow is stored by the SMF.
- APN-AMBR: APN-AMBR is set according to the operator policy. For example, taking the session AMBR into account.
- EPS QoS parameters (including ARP, QCI, GBR, and MBR):
  - If the QoS Flow is mapped to one EPS bearer: ARP, GBR, and MBR of the EPS bearer is set to the respective ARP, GFBR, and MFBR of the corresponding QoS Flow.
  - For standardized 5QIs, the QCI is mapped 1:1 to the 5QI. For non-standardized 5QIs, the PGW-C+SMF derives the QCI based on the 5QI and operator policy.

Note A GBR QoS flow is mapped 1:1 to a GBR dedicated EPS Bearer if an EBI has been assigned. All other GBR QoS flows will be terminated during interworking. If multiple QoS flows are mapped to one EPS bearer, the EPS bearer parameters are set based on the operator policy. For example, EPS bearer QoS parameters are set according to the highest QoS of all mapped QoS flows.

Note Non-GBR QoS flows for which no EBI has been assigned are mapped to the default EPS bearer.

5G to EPS Handover Using N26 Interface

Feature Description

The SMF supports handover of PDU sessions to EPS on 5GC when the N26 interface is present between the MME and the AMF. The handover supports the creation of applicable default and dedicated bearers.

How it Works

This section describes the 5G to EPS handover procedure and the 5G to EPS handover cancellation procedure.

Call Flows

This section describes the following call flows:

- 5G to EPS Handover Call Flow
- 5G to EPS Handover Cancellation Flow

5G to EPS Handover Call Flow

This section describes the 5G to EPS handover call flow with N26 interface.

The 5G to EPS Handover procedure for the EPS session is compliant with 3GPP 23.502, section 4.11.1.2.1.

1. The AMF requests the SMF to provide the SM Context using Nsmf_PDUSession_ContextRequest.
2. The SMF sends N4 Session Modification to the UPF to establish the CN tunnel for each EPS bearer. The bearer mapping to the 5G QoS and PCC rules received from PCC must already be present with the SMF. The SMF must also have the bearer IDs obtained from the Bearer ID Allocation procedure. The SMF creates new PDRs for the N4 session and gets TEID allocated for each bearer as required by the 4G system.
3. The SMF provides EPS bearer contexts to the AMF. The SMF also provides the CN tunnel information to AMF for all bearers for the uplink traffic from E-UTRAN.
4. If indirect data forwarding applies, the AMF sends the Nsmf_PDUSession_UpdateSMContext Request (S-GW address(es) and S-GW DL TEID(s) for data forwarding) to the SMF, for creating the indirect data forwarding tunnel.
5. The SMF sends N4 Modification Request to the UPF to create additional PDRs and FARs to receive the redirected DL data over the indirect tunnel from NG RAN and forwards them to eNodeB. The uplink PDRs must have QFI to match the forwarded DL data from NG-RAN and the associated QER will not have QFI as data needs to be forwarded to the eNodeB. The FAR redirects the received data to the eNodeB over appropriate tunnel based on the QFI.
6. The S-GW sends Modify Bearer Request to the SMF with DL TEIDs on the SMF for the bearers.
7. The SMF sends N4 Modification Request to the UPF to activate the DL data path to E-UTRAN. At this time, both the indirect tunnel and the direct DL path are activated towards the eNodeB.
8. The SMF sends the Modify Bearer Response to S-GW.
9. The AMF initiates Nsmf_PDUSession_UpdateSMContext Request service operation with an indication to release the forwarding tunnels.
10. The SMF sends N4 Modification Request to the UPF to remove the PDRs and FARs for the indirect tunnels. The PDRs and FARs for the 5G session which are not required are also removed.

5G to EPS Handover Cancellation Call Flow

When the Source Radio Access Network (RAN) triggers a handover cancellation after the preparation phase, the AMF invokes the "Nsmf_PDUSession_UpdateSMContext request (SUPI, Relocation Cancel Indication) toward the SMF. Based on the Relocation Cancel Indication, the SMF deletes the session resources established during the handover preparation phase. That is, the SMF removes all the Packet Detection Rules (PDRs), Forwarding Action Rules (FARs), and other rules that were allocated in preparation of handoff for indirect tunnel and the 5G session.

The following call flow depicts the 5GS to EPS handover cancellation procedure.

Figure 56: 5GS to EPS Handover Cancellation Call Flow

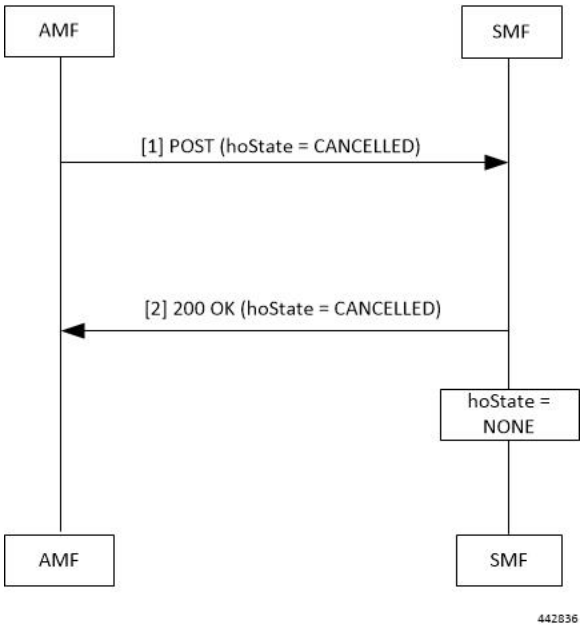


Table 67: 5GS to EPS Handover Cancellation Call Flow Description

Step	Description
1	The AMF requests the SMF to cancel the handover of an existing PDU session by sending a POST request for Sm Context Update service, with the following information: • updating the hoState attribute of the individual SM Context resource in the SMF to CANCELLED • cause information
2	The SMF returns a 200 OK response message including the following information: • hoState attribute set to CANCELLED The SMF cancels the execution of the handover, for example, releases the resources reserved for the handover to the target RAN. Then, the SMF sets the hoState to NONE and deletes any stored targetServingNfId.

Standards Compliance

The 5G to EPS Handover feature complies with the 3GPP TS 23.502, version 15.3.0.

Create Dedicated Bearer Delay and Retry Support

Feature Description

The Create Dedicated Bearer Delay and Retry Support feature facilitates the following:

- Delays the creation of the dedicated bearer that is based on the configured time after handover is complete.
- Retries the creation of the dedicated bearer for the IMS bearer in either of the following scenarios:
  - When the MME fails with the handover in progress.
  - When the IMS bearer is temporarily unreachable.
- After the handover is complete, the SMF service starts with the configured timer. Then, the dedicated bearer creation begins.
- If the IMS dedicated bearer creation fails, the maximum retries configuration determines the number of retries the creation process attempts. The configured timeout determines the delay of each retry attempt.

How It Works

This section provides a brief of how the Create Dedicated Bearer Delay and Retry Support feature works.

Call Flows

This section includes the following call flow.

Figure 57: EPS Fallback Guard Timer Call Flow

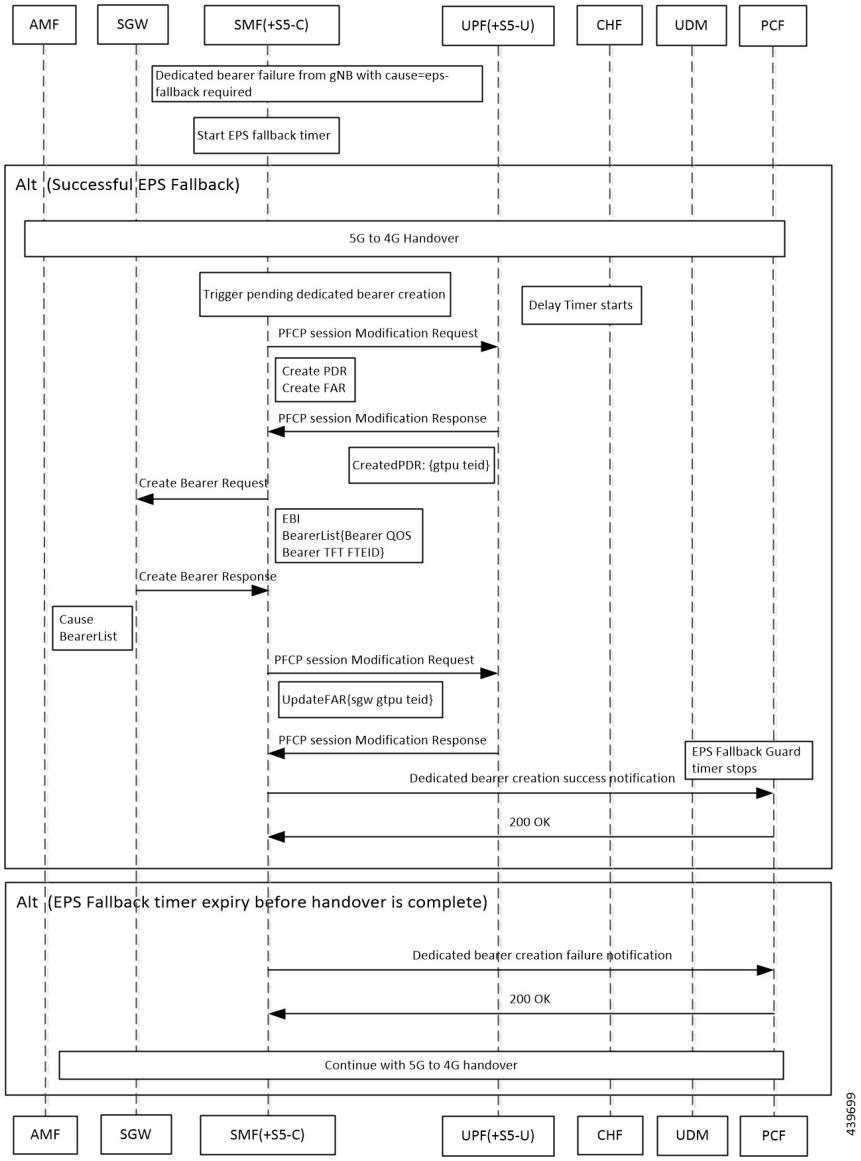


Table 68: EPS Fallback Guard Timer Call Flow Description

Step	Description
1	gNB sends the dedicated bearer creation failure information with the fallback cause through AMF.
2	EPS fallback timer starts.
With the successful EPS fallback following the 5G to 4G handover, steps 3 to12 occur.	
3	EPS triggers pending dedicated bearer creation.
4	Delay timer starts.

Step	Description
5	SMF (+S5-C) sends the PFCP session modification request to UPF (+S5-U).
6	PDR and FAR are created.
7	UPF (+S5-U) sends the PFCP session modification response to SMF (+S5-C).
8	The information on the created PDR with the GTP-U TEID is available.
9	SMF (+S5-C) sends the Create Bearer Request to S-GW.
10	S-GW sends the Create Bearer Response to SMF (+S5-C).
11	SMF (+S5-C) sends the PFCP Session Modification Request to UPF (+S5-U).
12	UPF (+S5-U) sends the notification of the successful dedicated bearer creation to PCF.
13	EPS Fallback Guard Timer stops.
14	PCF sends the “200 OK” acknowledgment to SMF (+S5-C).
In the EPS fallback timer expiry before handover completion scenario, steps 13 to15 occur.	
15	SMF (+S5-C) sends the failure notification of the dedicated bearer creation to PCF.
16	PCF sends the “200 OK” acknowledgment to SMF (+S5-C).
17	The 5G to 4G handover procedure continues.

Configuring Create Dedicated Bearer Delay and Retry Support

This section describes how to configure the Create Dedicated Bearer Delay and Retry Support feature.

```
configure
  profile access accesstemp
    eps-fallback cbr delay delay_time max-retryretry_counttimeouttimeout_value
    end
```

NOTES:

- **delay** *delay_time*: Specifies the time delay in milliseconds for the creation of the dedicated bearer. The valid values range 0 through10000 milliseconds. The default is 0.
- **max-retry** *retry_count*: Specifies the number of times to retry the creation of the dedicated bearer. The valid values range from 0 through 10. The default is 0.
- **timeout** *timeout_value*: Specifies the time gap in seconds before retrying the creation of the dedicated bearer. The valid values range from 1 through 3 seconds. The default is 1.

Verifying the Create Dedicated Bearer Delay and Retry Support Configuration

This section describes how to verify the Create Dedicated Bearer Delay and Retry Support configuration.

Use the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```
profile smf smf1
service name smf-service
  access-profile access1
```

```
!
!
profile access access1
eps-fallback cbr delay 100 max-retry 5 timeout 2
```

Handling GTP-U Error Indication for 4G Sessions

Feature Description

This section describes how the SMF handles GPRS tunneling protocol, user plane (GTP-U) error indication for the 4G sessions.

Serving Gateway (S-GW) sends GTP-U error indication message including the tunnel IDs to UPF when it receives a GTP-U message with an unknown Tunnel Endpoint Identifier (TEID). The UPF on receiving GTP-U error indication sends N4SessionReportRequest towards SMF including error indication (ERIR). The SMF retrieves EBI based on Fteid included in the N4SessionReportRequest, and initiates deletion of the session or bearer. The SMF sends Delete Bearer Request towards S-GW. On receiving the response from S-GW, the SMF sends either an N4 session modification request or N4 session release request to the UPF based on the bearer type, that is, dedicated or default bearer. CHF and PCF are also notified based on the bearer type.

Note When the SMF receives PFCPSessionReportRequest, the IntSelfTxnN4SessRptReq message is displayed as part of the debug message.

Standards Compliance

The GTP-U Error Indication Handling feature complies with the following standards:

- 3GPP TS 29.244, Version 15.6.0
- 3GPP TS 23.527, Version 15.3.0

How it Works

GTP-U Error Handling Procedure

This section describes the call flow associated with the GTP-U error handling procedure for the 4G sessions.

Figure 58: GTP-U Error Indication Handling Call Flow

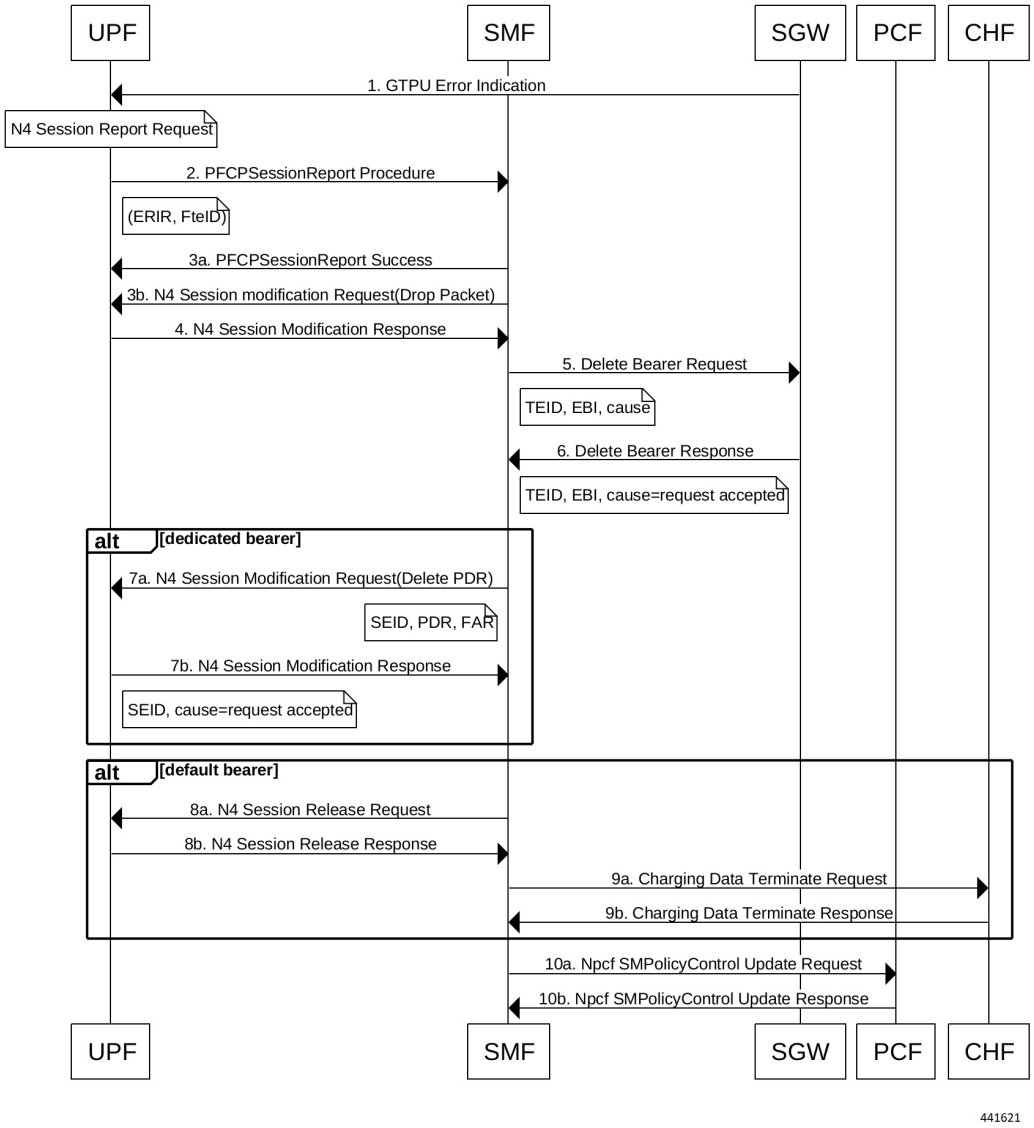


Table 69: GTP-U Error Handling Call Flow Description

Step	Description
1	S-GW sends GTP-U Error Indication towards UPF, indicating the bearer with the failed bearer ID.
2	After receiving GTP-U error indication, the UPF sends PFCPSessionReport towards SMF along with the failed bearer ID.
3a and 3b	The SMF sends PFCPSessionReport Success message and N4 Session Modification Request for dropped packet towards the UPF.

Step	Description
4	The UPF sends N4 Session Modification Response to the SMF.
5	The SMF sends Delete Bearer Request towards S-GW along with TEID, EBI, and cause.
6	The S-GW sends Delete Bearer Response towards SMF along with TEID, EBI, and cause as request accepted.
7a	If the TEID is a dedicated bearer, then the SMF sends N4 Session Modification Request with Delete PDR.
7b	The UPF sends N4 Session Modification Response.
8a	If it is a default bearer, the SMF sends N4 Session Release Request.
8b	The UPF sends N4 Session Release Response.
9a	The SMF sends Charging Data Terminate Request towards CHF.
9b	The CHF responds with Charging Data Terminate Response.
10a	The SMF sends SMPolicyControl Update Request towards PCF.
10b	The PCF sends SMPolicyControl Update Response to the SMF.

GTP Path Failure Handling, Restoration, and Recovery

Feature Description

SMF now supports:

- Handling of the following GTP-C path management messages as per 3GPP TS 29.274
  - Echo Request
  - Echo Response
- Sending Echo Request message to the newly discovered GTP-C peer as per the configuration.
- Sending Echo Response message as a reply if it receives Echo Request message from GTP-C peer.
- Retransmitting Echo Request message to GTP-C peer for configured number of times if no response is received.
- Clearing all the subscribers associated to a GTP-C peer if no response is received for Echo Request message for configured number of times for that GTP-C peer.
- Clearing all the subscribers associated to a GTP-C peer if a different recovery value is received from that GTP-C peer.

The feature complies with the following standards:

- 3GPP TS 29.274
- 3GPP TS 23.007

Call Flows

The following call flows captures information specific to how GTP-C path management and GTP-C restoration messages are handled.

GTP-C Path Management

Figure 59: GTP-C Path Management

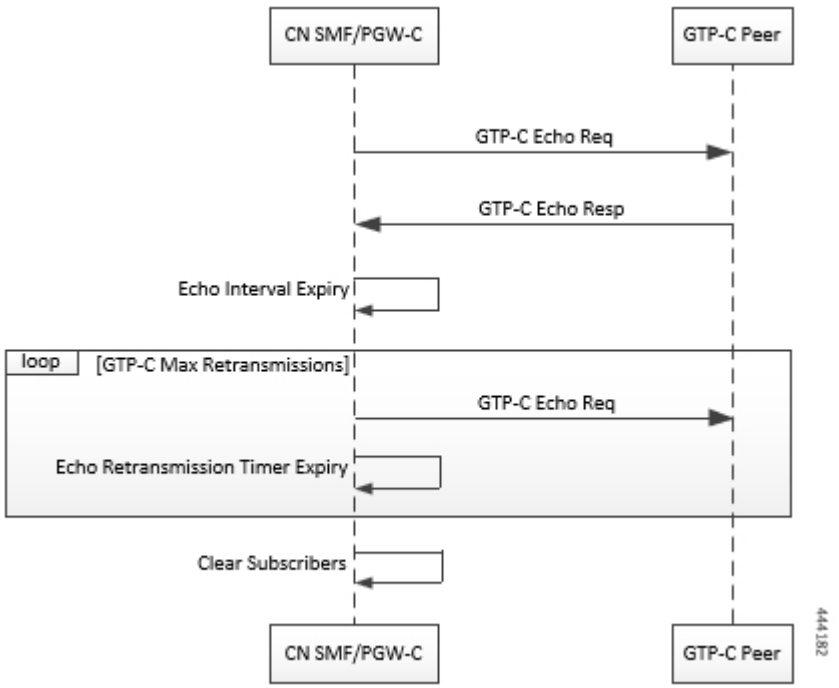


Table 70: GTP-C Path Management

Step	Description
1	Once the GTP-C peer is discovered (an Initial GTP-C Create Session Request or an GTP-C Modify Bearer Request message is received), CN SMF/PGW-C starts sending GTP-C Echo Request Messages periodically to the new GTP-C Peer as per configuration.
2	If GTP-C Echo response is not received, CN SMF/PGW-C retries sending GTP-C Echo Request (configured) N3 times for every configured T3 timer expiry.
3	Once all retries are exhausted, CN SMF/PGW-C clears all the sessions associated to that GTP-C peer.

GTP-C Echo Request Handling

Figure 60: GTP-C Echo Request Handling

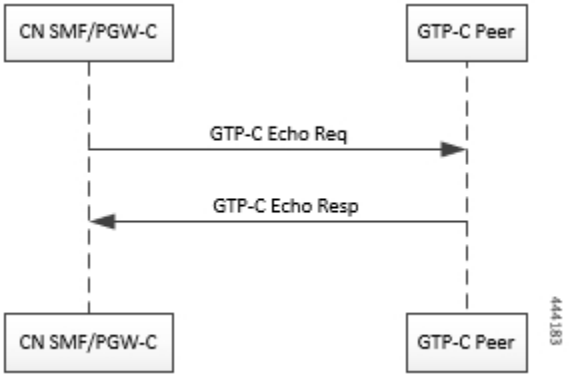


Table 71: GTP-C Echo Request Handling

Step	Description
1	Whenever a GTP-C Echo Request message is received from a GTP-C peer, CN SMF/PGW-C sends GTP-C Echo Response message as a reply.

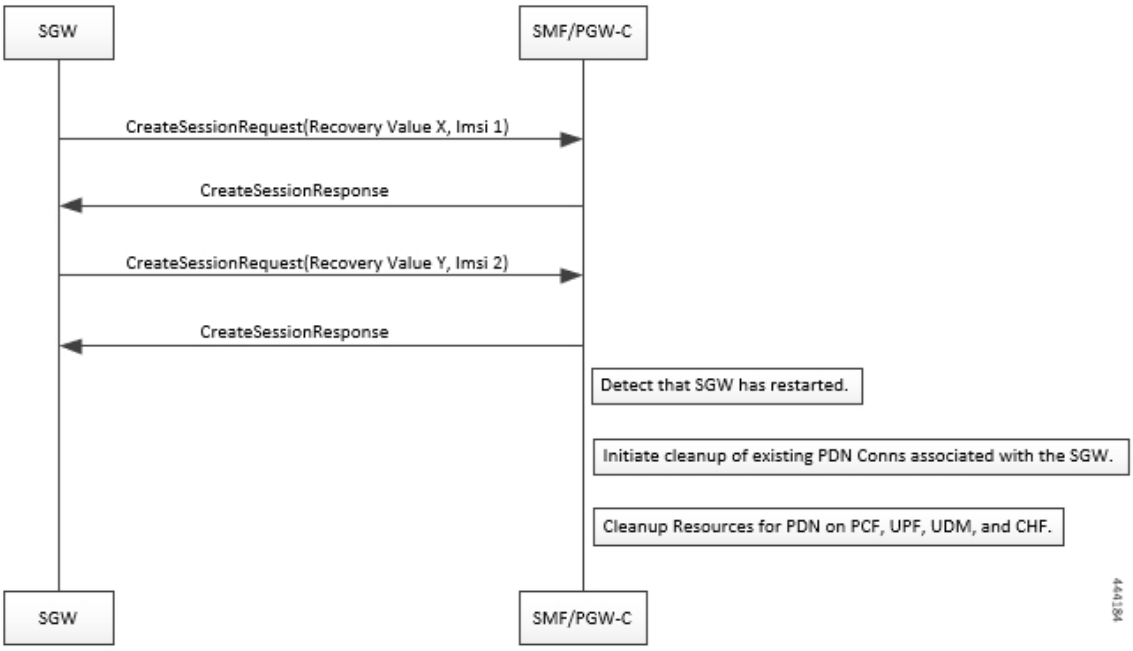
GTP-C Restoration on PGW-C/SMF

PGW-C/SMF can detect that there is a change in recovery value of SGW. PGW-C/SMF can detect this value from the following messages:

- Create Session Request
- Modify Bearer Request
- Create Bearer Response
- Echo Response

If PGW-C/SMF detects that there is a change in recovery value, then it initiates the cleanup of all the PDN connections associated with the SGW.

Figure 61: GTP Restoration due to SGW Restart



Memory and Performance Impact

The Node Manager pod to GTP-C peer path mapping is maintained in etcd and also in the local cache of NodeMgr and GTP-C Pods.

Configuration

The following echo sending related parameters need to be configured at GTP endpoint.

```
config
        endpoint gtp
        interface <s2b s5 s8>
                echo interval <val>
                echo retransmission-timeout <val>
                echo max-retransmissions <val>
```

Sample Configuration

```
[unknown] smf# config
Entering configuration mode terminal
[unknown] smf(config)# endpoint gtp
[unknown] smf(config-endpoint-gtp)#
[unknown] smf(config-endpoint-gtp)# interface
s2b s5 s8
[unknown] smf(config-endpoint-gtp)# interface s5
[unknown] smf(config-interface-s5)# echo interval 60
echo - Enable gtpc path management
interval - Configure echo interval in seconds, ranging from <60-360>
```

```
[unknown] smf(config-interface-s5)# echo retransmission-timeout 3
retransmission-timeout - Configure the echo retransmission timeout in seconds, ranging from
 <1-20>
[unknown] smf(config-interface-s5)# echo max-retransmissions 10
max-retransmissions  - Configure maximum retries for GTP echo request, ranging from <0-10>
[unknown] smf(config-interface-s5)#
```

show Command

The `show peers gtp` command can be used to display all the connected GTP peers and their node information.

Example:

```
[unknown] smf# show peers gtp

Ip Address    Recovery Value
============================
1.1.1.2          10
1.1.1.3          21
```

Bulk Statistics

The following dedicated disconnect reason is used for PDN connections cleared due to peer GTP-C restart or path failure.

- disc_pdnrel_gtpc_peer_restart
- disc_pdnrel_gtpc_peer_pathfail

The following statistics are added in smf-nodemgr pod.

```
# HELP nodemgr_gtpc_msg_stats Gtpc Msg Stats
# TYPE nodemgr_gtpc_msg_stats counter
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_rx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="smf-nodemgr"}
 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_tx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="smf-nodemgr"}
 4
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_res_rx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="smf-nodemgr"}
 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_res_tx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="smf-nodemgr"}
 1
# HELP nodemgr_gtpc_peer_status Gtpc Peer Status
# TYPE nodemgr_gtpc_peer_status counter
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="10.105.35.209",gtpc_peer_status="gtpc_peer_path_down",instance_id="0",service_name="smf-nodemgr"}
 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="10.105.35.209",gtpc_peer_status="gtpc_peer_path_up",instance_id="0",service_name="smf-nodemgr"}
 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="10.105.35.209",gtpc_peer_status="gtpc_peer_restarted",instance_id="0",service_name="smf-nodemgr"}
 1
```

Limitations

From 3GPP TS 23.007, Section 20: It is recommended that GTPv2 Echo Request should be sent only when a GTP-C entity has not received any GTP response message for a previously sent request message on the GTP-C path for, an implementation dependent time period.

Currently, this is not supported.

Even if SMF receives GTPC echo req from peer, it is considered as path is up. The subsequent Echo Req from SMF is received after the echo interval expiry.

Configuration Support for Rejecting 4G-only Devices

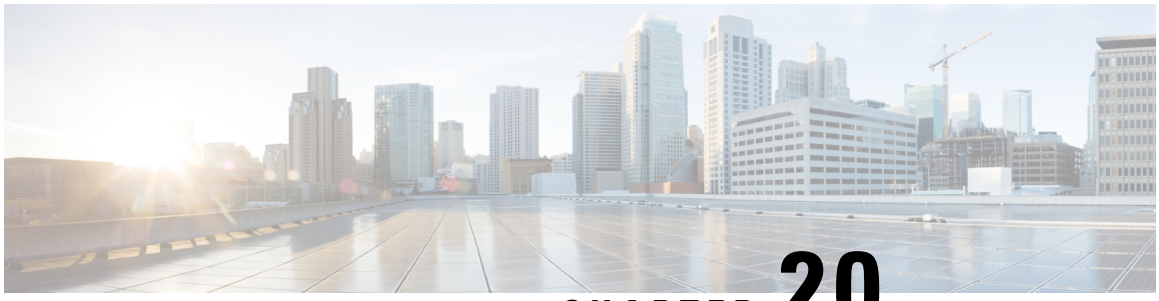
The SMF provides configuration support to reject calls from 4G-only UE devices.

To reject calls from 4G-only UE devices, use the following configuration:

```
configure
   profile dnn dnnprofile_name
      only-nr-capable-ue true
      end
```

NOTES:

- **only-nr-capable-ue true**: Enable this command to reject any new call attempt for PDN session creation from a 4G only capable UE device.



CHAPTER 20

Flow Failure Handling for Access and Mobility Procedures

Feature Summary and Revision History

Summary Data

Table 72: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 73: Revision History

Revision Details	Release
First introduced	Pre-2020.02.0

Feature Description

The SMF supports the QoS flow failures for access and mobility procedures. The SMF receives the QoS flow failure details as part of the following call flows from NG-RAN to N2 messages.

- Xn handover
- Service request procedures (UE and network-initiated)
- N2 handover with or without changing AMF
- N26 4G to 5G handover
- N26 5G to 4G handover

How it Works

The SMF processes N11 messages with N2 message details to determine the accepted and failed QoS flow IDs. For failed QoS flow IDs, the SMF excludes the resources locally and communicates the following information to the external interfaces:

- Sends the N4 Session Modification Request to UPF to delete the QERs, URRs, UL or DL PDRs, UL or DL FARs which are applicable to the QoS flow IDs.
- Sends the Charging Data Update Request to CHF by including multi-unit usage details for the removed URRs. If SMF receives a usage report from UPF, SMF sends this report to CHF.
- Sends the N1 N2 transfer message with N1 message details to UE as the PDU Session Modification Command.
- Based on the received Policy Control Request Triggers and SM Policy Decision last Request Rule Data, SMF sends the Rule Reports SM Policy Control Update to PCF.

Call Flows

This section describes the following call flows:

- QoS flow failure handling for Xn handover call flow
- QoS flow failure handling for N2 handover call flow
- QoS Flow failure handling for N26 4G to 5G handover call flow
- QoS flow failures for service request procedures
- PDU UE synchronization procedure
- Flow Failure Management Call Flows

QoS Flow Failure Handling During Xn Handover

This section describes the QoS flow failure handling during the Xn handover.

Figure 62: QoS Flow Failure Handling during Xn Handover

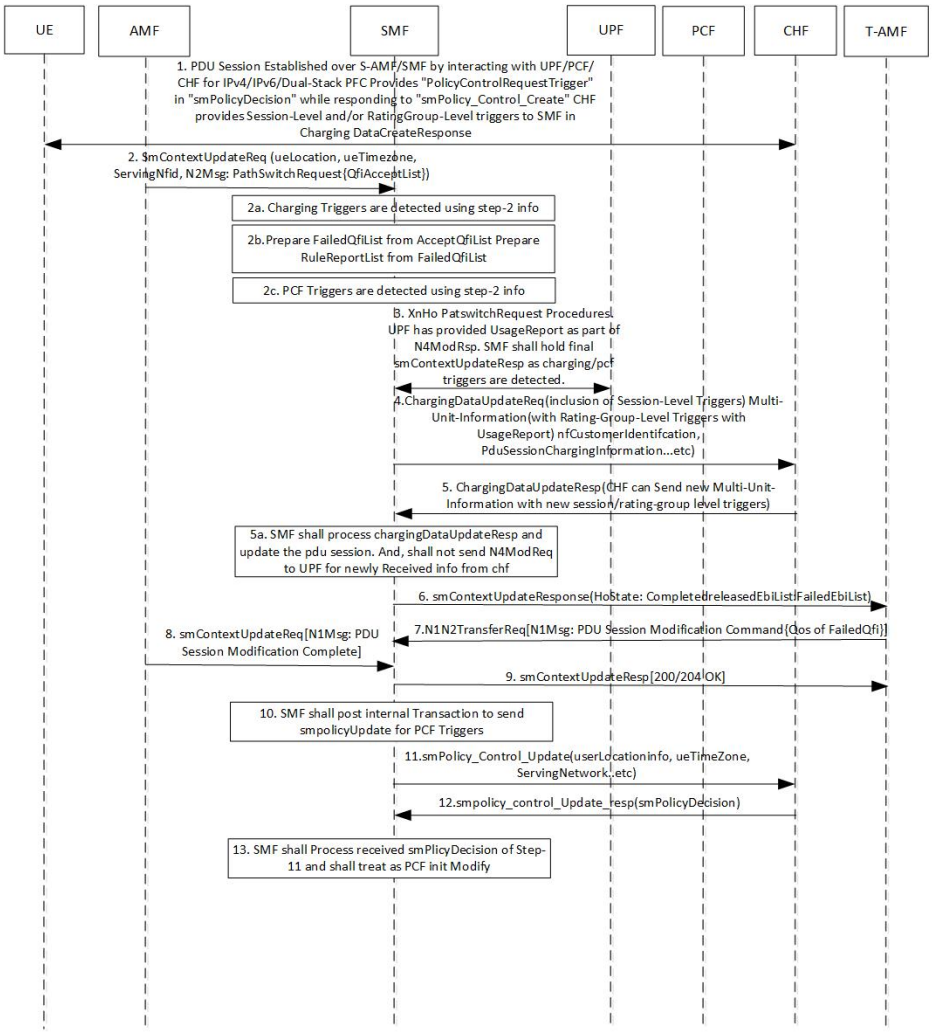


Table 74: QoS Flow Failure Handling Call Flow Description

Step	Description
1	The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.
2	The AMF sends SM Context Update Request to SMF. This request includes the information on UE location, UE time zone, and N2 message path switch request with the list of the accepted QoS Flow Identifier (QFI).

Step	Description
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The SMF extracts the list of failed QFI, failed rule report, and failed EPS bearer ID (EBI) from the received list of the accepted QFIs.
2c	The PCF triggers are identified through the information that is received in Step 2.
3	For Xn handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 modification response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
4	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
5	The CHF sends the Charging Data Update Response to the SMF. This response may include the multi-unit information with new session or rating-group-level triggers.
5a	The SMF processes the Charging Data Update Response and updates the PDU session. SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
6	The SMF sends the SM Context Update Response by including the N2 message path switch request acknowledgment and the list of failed EBI list.
7	The SMF and T-AMF process the N1 N2 Transfer Request for the PDU Session modification for the QoS about failed QFIs. The SMF includes the PDU Session Modification command to communicate the information on the QoS flow failure list to the UE.
8	The AMF sends the SM Context Update Request N1 message to the SMF to communicate about the handover completion.
9	The SMF sends the SM Context Update Response as “200/204 OK” to T-AMF. The SMF does not process the received N1 message from UE.
10	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers to send to the PCF. The SMF posts this information to communicate Rule Report for the failed QFIs or any identified armed access-side triggers.
11	The SMF sends the SM Policy Control Update to the PCF. This update includes details, such as user location information and UE time zone.
12	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
13	The SMF processes the received SM policy decision and initiates the PCF modify procedures.

QoS Flow Failure Handling During N2 Handover

This section describes the flow failure handling procedure during the N2 handover.

Figure 63: Flow Failure Handling During N2 Handover

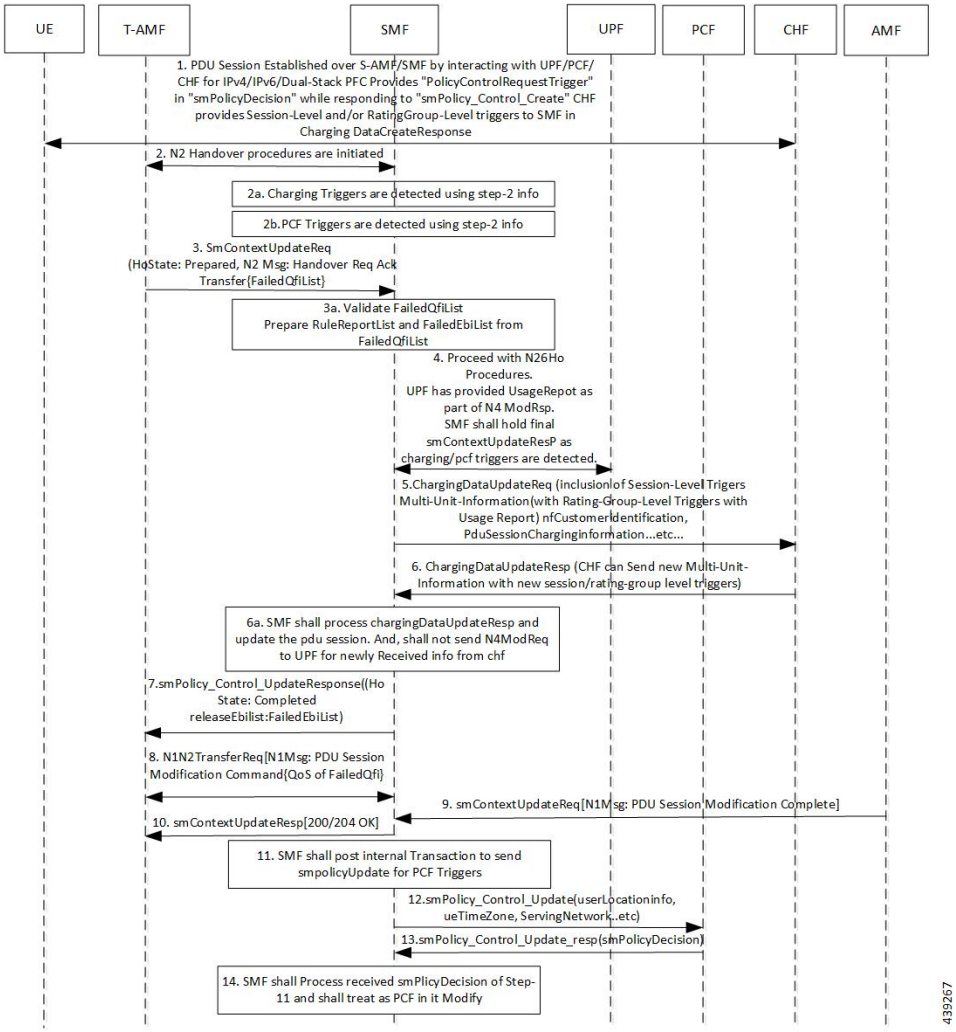


Table 75: Description for Flow Failure Handling During N2 Handover

Step	Description
1	The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.

Step	Description
2	The T-AMF sends SM Context Update Request to the SMF. This request includes the information on handover state as preparing, UE location, UE time zone, target serving NF ID, and serving network. In case of inter-AMF handoff, the AMF includes the target serving NF ID.
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The PCF triggers are identified through the information that is received in Step 2.
3	The T-AMF sends the SM Context Update Request to the SMF. This request includes the information on handover state as prepared along with N2 message on Handover Required Transfer Request. The transfer request includes the list of failed QFIs.
3a	The SMF validates the list of failed QFIs to extract the list of failed rule report and failed EBIs.
4	For N2 handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 modification response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
6	The CHF sends the Charging Data Update Response to the SMF. This response contains the multi-unit information along with new session-level or rating-group level triggers.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
7	The SMF sends the SM Context Update Response to the T-AMF with handover state as completed. This response also includes list of the released EBIs and the failed EBIs.
8	The SMF and T-AMF process the N1 N2 Transfer Request. This request includes the N1 message as PDU Session Modification Command to communicate the information on the QoS flow failure list to the UE.
9	The CHF sends the SM Context Update Request with an N1 message for the completion of the PDU session modification.
10	The SMF sends the SM Context Update Response as “200/204 OK” to the T-AMF. The SMF does not process the received N1 message from the UE.

Step	Description
11	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers. The SMF sends this update to communicate the rule report about the failed QFIs or any armed access-side triggers.
12	The SMF sends the SM Policy Control Update to the PCF. This update includes the details on the user location and UE time zone.
13	The PCF sends the SM Policy Control Update response, which is the SM policy decision, to the SMF.
14	The SMF processes the SM policy decision and treats it as the PCF-initiated PDU Session Modification procedure.

QoS Flow Failure Handling During N26 4G to 5G Handover

This section describes the flow failure handling procedure during the N26 4G to 5G handover.

Figure 64: QoS Flow Failure Handling During N26 4G to 5G Handover

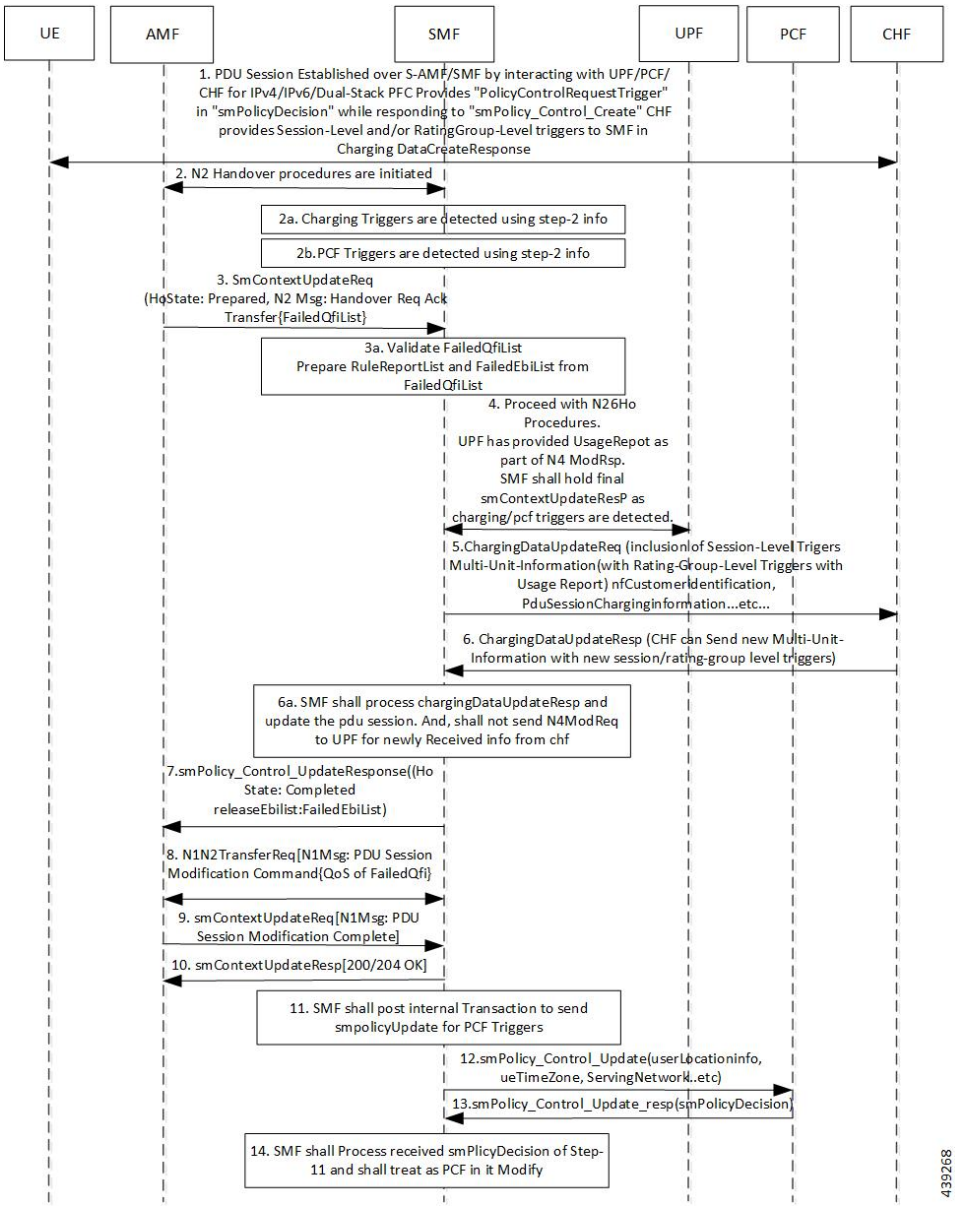


Table 76: Description for QoS Flow Failure Handling During N26 4G to 5G Handover

Step	Description
1	The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.

Step	Description
2	The T-AMF sends SM Context Update Request to the SMF. This request includes the information on handover state as prepared, UE location, UE time zone, target serving NF ID, serving network. In case of inter-AMF handoff, the AMF includes the target serving NF ID and the N2 message path switch request with the list of the accepted QFIs to the SMF.
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The PCF triggers are identified through the information that is received in Step 2.
3	The T-AMF sends the SM Context Update Request to the SMF. This request includes the information on handover state as prepared along with N2 message on Handover Required Transfer Request. The transfer request includes the list of failed QFIs.
3a	The SMF validates the list of failed QFIs to extract the list of failed rule report and failed EBIs.
4	For N26 handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 Modification Response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
6	The CHF sends the Charging Data Update Response to the SMF. This response contains the multi-unit information along with new session-level or rating-group level triggers.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
7	The SMF sends the SM Context Update Response to the T-AMF with the handover state as completed. This response also includes list of the released EBIs and the failed EBIs.
8	The SMF and T-AMF process the N1 N2 Transfer Request. This request includes the N1 message as PDU Session Modification Command to communicate the information on the QoS flow failure list to the UE.
9	The CHF sends the SM Context Update Request with an N1 message for the completion of the PDU session modification.
10	the SMF sends the SM Context Update Response as “200/204 OK” to the T-AMF. The SMF does not process the received N1 message from the UE.
11	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers. The SMF sends this update to communicate the rule report about the failed QFIs or any armed access-side triggers.

Step	Description
12	The SMF sends the SM Policy Control Update to the PCF. This update includes the details on the user location and UE time zone.
13	The PCF sends the SM Policy Control Update response, which is the SM policy decision, to the SMF.
14	The SMF processes the SM policy decision and treats it as the PCF-initiated PDU Session Modification procedure.

QoS Flow Failures for Service Request Procedures

The SMF supports both UE and Network Service Request procedures. For these procedures, the SMF processes the received SM Context Update Request to update the N3 tunnel path from idle to active state.

The QoS flow failures for service request procedures are handled in the same way as described in the 3GPP 23.502, Section 4.2.3.2. However, QoS flow failure list is handled with the PDU Session Setup Response Transfer N2 message, which is received as SM Context Update Response when subscriber moves from Idle to Active State.

Figure 65: PDUIM Idle to Active Mode

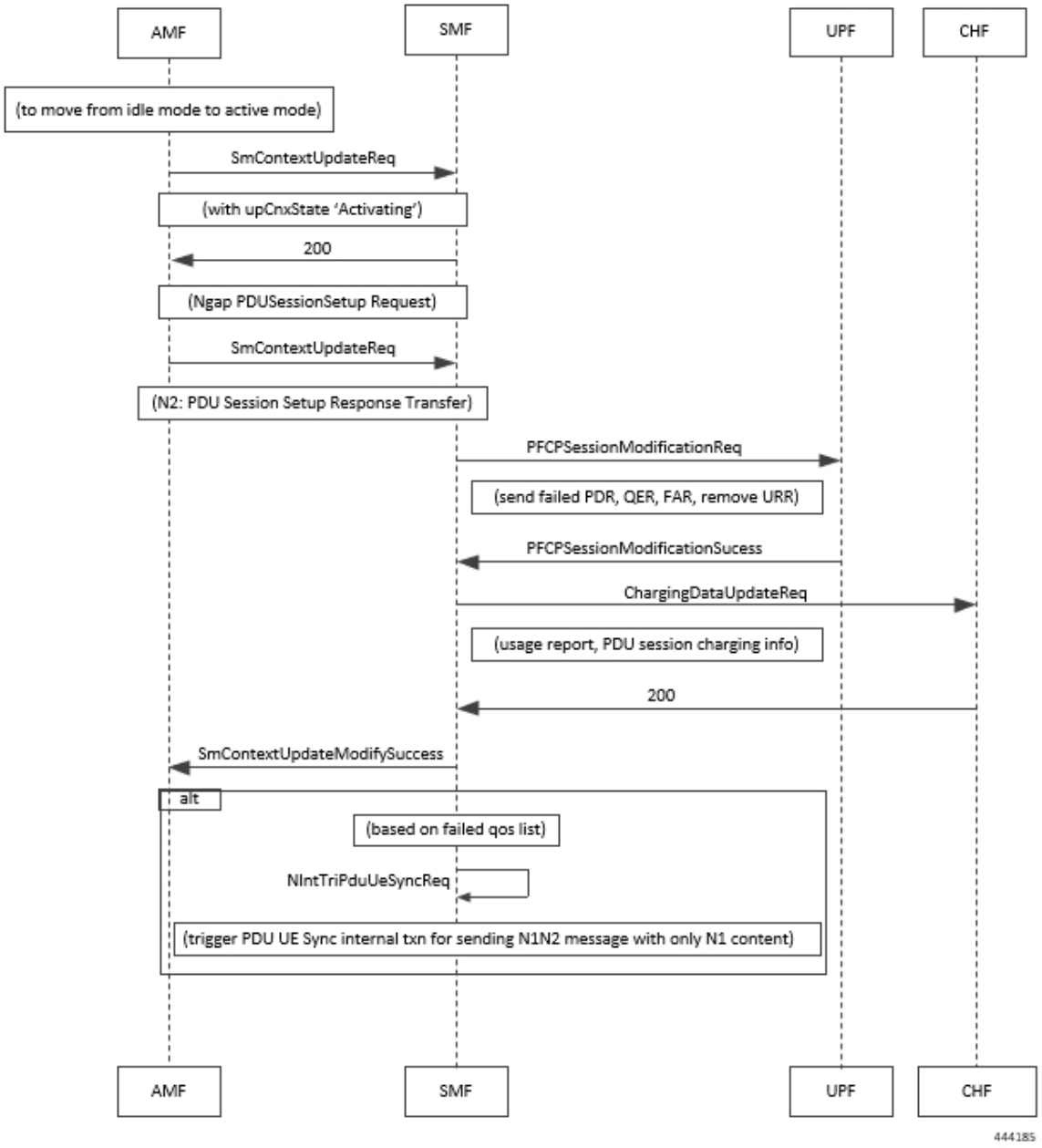


Table 77: QoS Flow Failures for Service Request Procedure

Step	Description
1	The SMF sends the SM Context Update Request message for the User Plane Connection State as Activated.

Step	Description
2	SMF sends 200 response along with PDU Session Setup Request towards AMF. AMF sends N2 message **PDU Session Setup Response Transfer** which contains QoS flow faliure list.
3	SMF validates failed QFIs to extract failed PCC rules and failed flows.
4	SMF updates received DL tunnel information (gNB, delete PDRs, delete QERs). After the tunnel information is updated, SMF removes URR based on failed flows and sends N4 Session Modification Request towards UPF.
5	UPF provides usage report as part of N4 Session Modification Response. SMF sends SM Context Update Response for User Plane Connection State as Activated along with released EBIs as failed EBIs and triggers internal transaction to process charging and PCF triggers.
6	SMF sends Charging Data Update Request to CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
7	SMF sends internal transaction based on failed QFIs to initiate PDU UE Sync Procedure to send N1/NAS signalling. Refer to PDU UE Sync Procedure call flow diagram for N1N2 message transfer

PDU UE Synchronization Procedure

This section describes the UE synchronization procedure.

1. PDU UE synchronization procedure in idle mode receives the failed QFIs, QoS rules and EBIs.
2. UE synchronization procedure fills N1 message PDU Session Modification command with QoS Descriptions, QoS Rules, and EPS Bearer Context from received QFI, QoS rule ID, and EBI respectively.
3. The SMF includes the created N1 container to N11 message without any N2 content.
4. The SMF sends N1N2 Transfer Request message towards AMF and starts the N1N2 retransmission timer. The SMF waits for N1N2 Transfer Response.
5. If N1N2 Transfer Success is received, the SMF waits for SM Context Update Request with N1 update. The N1 update includes resource modify success/resource modify reject information.

Statistics

This procedure creates statistics for the following events:

- N1N2TransferRequest Attempt
- N1 modify success
- N1 modify failure
- UE sync procedure suspend
- On resuming UE sync procedure if it was suspended by other procedure

N1N2 Retransmission

Once N1N2 retransmission timer expires, following action is taken:

1. SMF increments the N1N2 retry counter
2. SMF sends N11N1N2 Transfer Request message towards AMF and restarts the N1N2 retransmission timer. SMF waits for N1N2 Transfer Response.
3. If N1N2 Transfer Success is received, SMF waits for SM Context Update Request with N1 update. The N1 update includes resource modify success/resource modify reject information.
4. Once the N1N2 retry counter reaches the configured maximum number, the procedure is aborted.

Collision Case

AMF informs SMF about HO procedure by rejecting the N1N2 Transfer Request with temporary reject cause. Also any other procedure can pre-empt the UE synchronization procedure while it is awaiting N1 update from the UE.

Figure 66: Collision Case

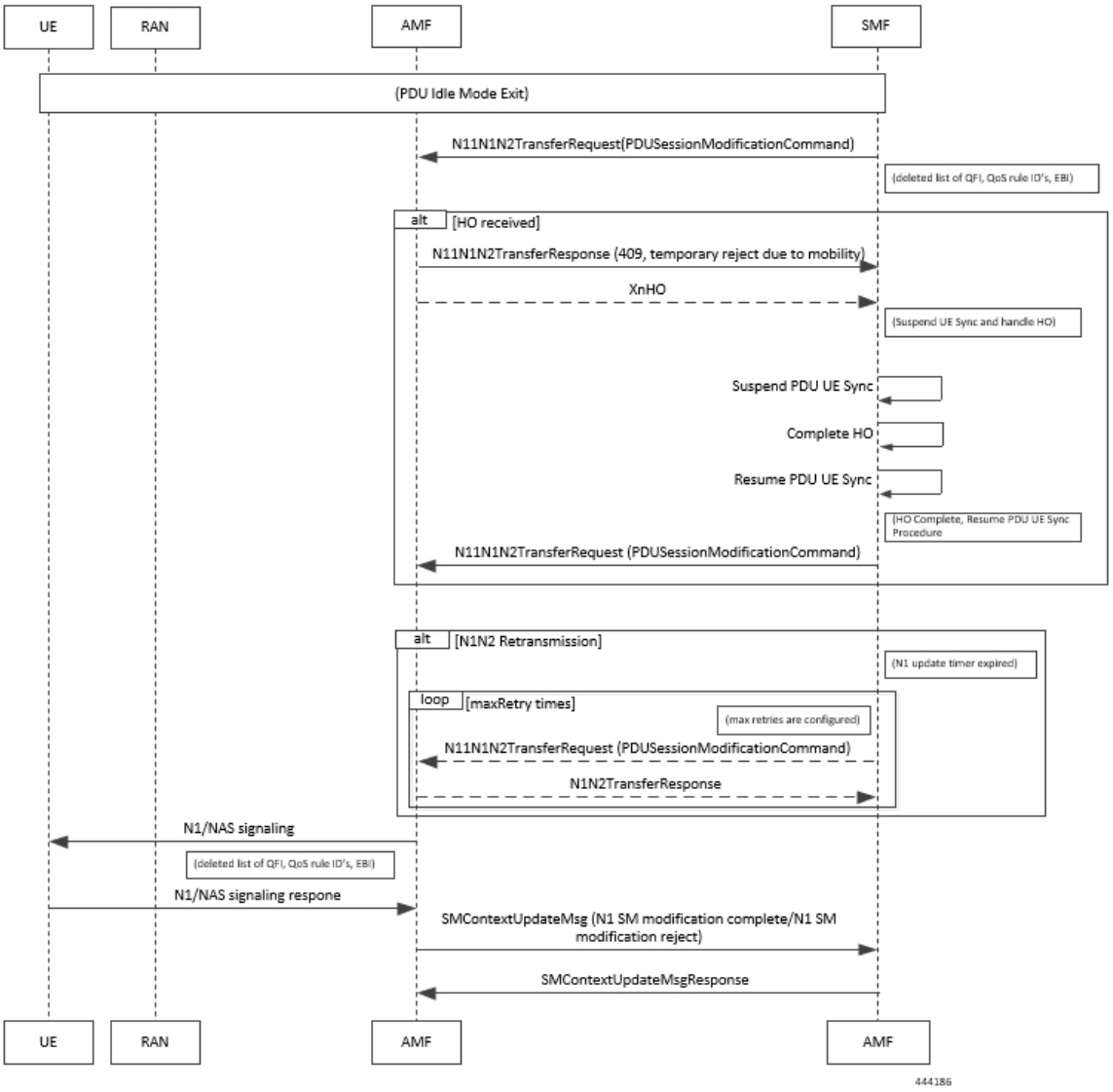


Table 78: Collision Case

Step	Description
1	If N1N2 Transfer Failure with cause as **Temporary Reject Handover Ongoing** is received, SMF awaits HO procedure to pre-empt PDU UE Sync Procedure.
2	While awaiting N1 Update or handover from UE, if any procedure (including handover) is triggered then: • If suspended by the handover procedure, it starts the N1N2 retry timer. • If aborted by PDU release or PDU setup procedure, it cleans up all the timers and aborts the N1N2 retry.

Step	Description
3	In case UE sync procedure is suspended by handover then on expiry of N1N2 Retry Timer, UE sync resumes after handover is processed.
4	On resuming if the UE sync procedure finds that the RAT has changed then it aborts the procedure and stop any timers.
5	On resuming the procedure in the same RAT the UE sync procedure reinitiates N11N1N2Transfer request message.

Handling Failed QoS Flow Identifier During PDU Setup Procedure

The SMF supports handling of the failed QoS Flow Identifier (QFI) during the PDU setup procedure.

NG-RAN rejects a QoS flow due to various reasons. When the NG-RAN node reports unsuccessful establishment of a QoS flow, the SMF uses cause value to identify the reason for the unsuccessful establishment.

Figure 67: Handling Failed QFIs During PDU Setup

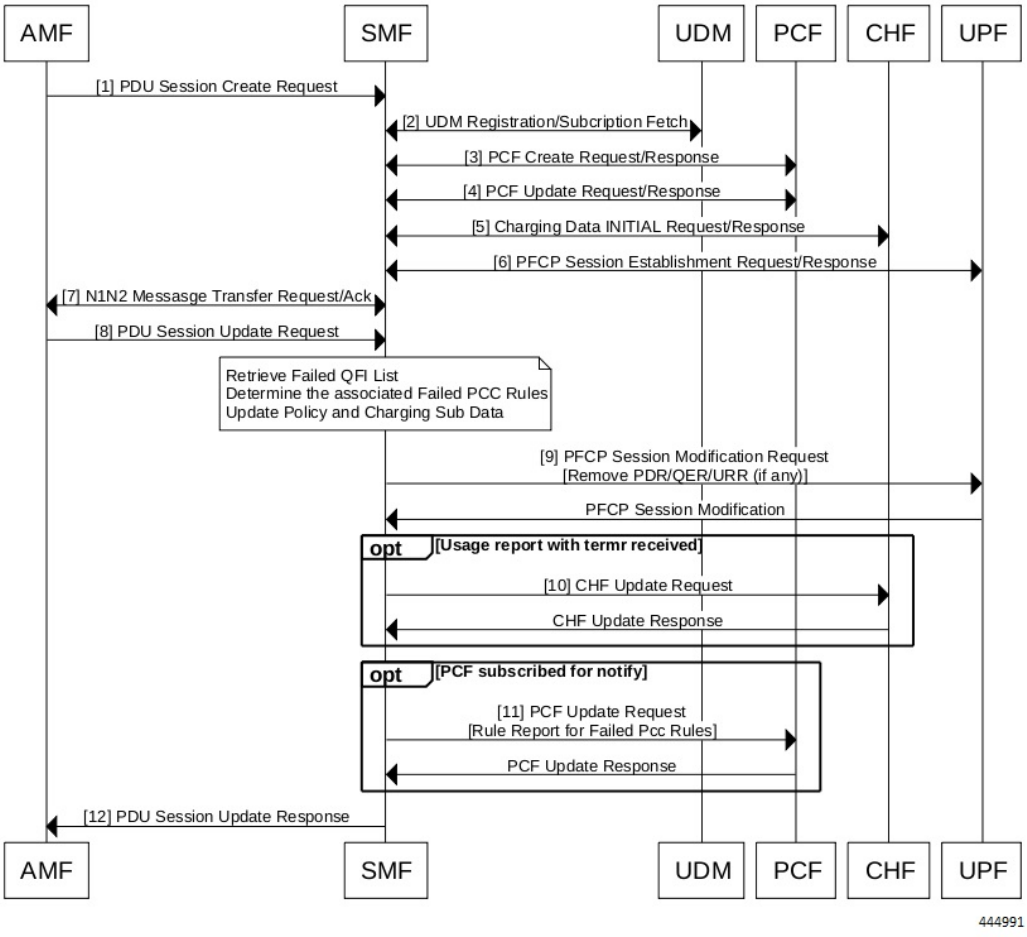


Table 79: Description for Failed QFI Handling During PDU Setup

Step	Description
1-7	The SMF, AMF, UDM, PCF, CHF, and UPF communicate with each other to perform the PDU setup procedure as defined in the 3GPP specification.
8	The AMF sends SM Context Update Request to the SMF. This request carries N2 payload “PDU Session Resource Setup Response Transfer”. This message includes the list of QoS flows failed to be established, if any, in the QoS Flow Failed to Setup List IE. The SMF marks the failed PCC rules and the charging descriptors associated with them for deletion.
9	The SMF sends PFCP Session Modification message to the UPF. This message carries Remove Packet Detection Rules (PDR), Remove QoS Enforcement Rules (QER), and Remove Usage Reporting Rules (URR) for the failed PCC rules in addition to the existing Update FAR for Downlink (DL) Tunnel Endpoint Identifier (TEID) of the successful PCC rules.
10	The SMF sends the CHF Update Request message to the CHF upon receiving a termination request. The CHF sends the CHF Update Response as an acknowledgment.
11	If the PCF has subscribed for notification on failed PCC rules, the SMF sends PCF Update Request with rule report containing the failed PCC rules dropped by the NG-RAN.
12	The SMF sends the PDU Session Update Response to the AMF. The SMF triggers internal transaction based on the failed QFI list. Then, the SMF initiates PDU UE Sync Procedure to send N1/NAS signalling. The SMF notifies the UE about the failed QoS flows using N1 messaging, and the UPF and PCF nodes about the associated failed PCC rules.

Handling Failed QoS Flow Identifier During PDU Session Modification

The SMF supports handling of the failed QoS flows over N2 interface during the PDU session modification.

If the modification of a PDU session or a QoS flow fails, the NG-RAN node falls back to the older configuration. That is, it falls back to the configuration of the session or the flow that was available before receiving the PDU SESSION RESOURCE MODIFY REQUEST message.

The SMF receives the QoS Flow Identifier for which the flow add/modify failed during the PDU SESSION RESOURCE MODIFY REQUEST.

If the new flow addition fails, the SMF performs the following:

- Removes the failed flow towards N1 (UE)
- Stops sending the failed flow-related information towards N4 (UPF)
- Stops sending the failed flow-related information towards N40 (CHF)
- Checks if the triggers are enabled and then sends the rule report for the failed flow towards N7 (PCF).

If the modification of flow fails, the SMF performs the following:

- Replaces the old information for the failed flow towards N1 (UE)
- Stops sending the modified flow-related information towards N4 (UPF)
- Stops sending the modified flow-related information towards N40 (CHF)
- Checks if the triggers are enabled and then sends the Rule Report for the failed flow towards N7 (PCF).

The following table captures the SMF behavior for the cause values included in the PDU Session Resource Modify Unsuccessful Transfer IE. These cause values are applicable for the PDU session modification procedure.

Cause Group	Cause Value	SMF Behavior	Comment
Radio Network Layer Cause			
	Unspecified		General
	Unknown PDU Session ID	Delete the session	N1 FiveGSM Cause reactivation requested
	Unknown QoS Flow ID	Send delete details to N1 Send PCF report about rule(s)	
	Multiple PDU Session ID Instances	Delete the session	
	Multiple QoS Flow ID Instances	Delete the session	N1 FiveGSM Cause reactivation requested
	Xn handover triggered	Act based on collision handling	
	Not supported 5QI value	Send delete details to N1 Send PCF report about rule(s)	
	IMS voice EPS fallback or RAT fallback triggered	Already supported	
Transport Layer Cause			
	Transport resource unavailable	Send delete details to N1 Send PCF report about rule(s)	
	Unspecified		
NAS Cause			
	Normal release	Delete the session	
	Authentication failure	Delete the session	

Cause Group	Cause Value	SMF Behavior	Comment
	Deregister	Delete the session	
	Unspecified	Delete the session	
Protocol Cause			
	Transfer syntax error	N1 rollback Error log fail procedure	
	Abstract syntax error (reject)	N1 rollback Error log fail procedure	
	Abstract syntax error (ignore and notify)	N1 rollback Error log fail procedure	
	Message not compatible with receiver state	N1 rollback Error log fail procedure	
	Semantic error	N1 rollback Error log fail procedure	
	Abstract syntax error (falsely constructed message)	N1 rollback Error log fail procedure	
	Unspecified	N1 rollback Error log fail procedure	
Miscellaneous Cause			
	Control processing overload	N1 rollback Error log fail procedure	
	Not enough user plane processing resources	N1 rollback Error log fail procedure	
	Hardware failure	Delete the session	
	O&M intervention	N1 rollback Error log fail procedure	
	Unknown PLMN	Delete the session	

Bulk Statistics

The following statistics provide details about the failed QoS flows over the N2 interface.

- policy_pdu_flows_total

- total attempted
- total succeeded
- total failed

- policy_pdu_flows_current
  - current attempted
  - current succeeded
  - current failed

Flow Failure Management Call Flows

The following call flow provides the details of the different flow failure scenarios during the EPS to 5GS handover. This call flow also describes how the SMF manages these failures and keeps the flows intact across 5GS network elements and the subscriber.

- Flow failure from source in EPS to 5GS Handover
- Flow failure from target in EPS to 5GS Handover

Figure 68: Flow Failure Management Call Flow

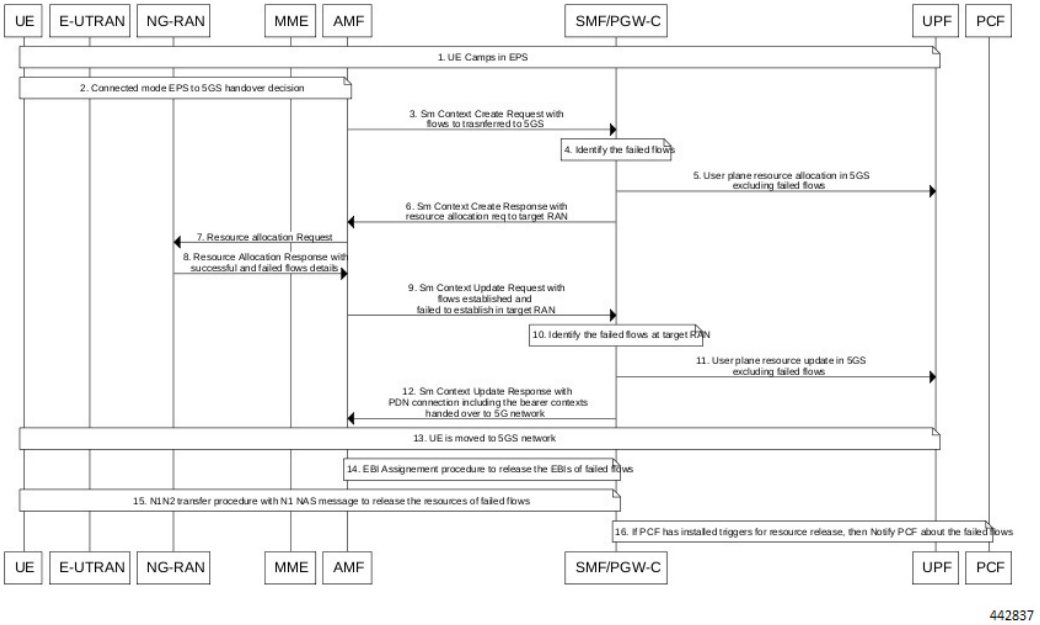


Table 80: Flow Failure Management Call Flow Description

Step	Description
1	The EPS interworking capable UE initially camps on the EPS network.
2	This step involves taking the connected mode EPS to 5GS handover decision.

Step	Description
3	During the EPS to 5GS handover procedure, the PDN Connection in the Sm Context Create request from the AMF carries the EPS bearer contexts to be handed over to 5GS network.
4	The SMF identifies the bearer contexts that were established in EPS and missing in PDN connection as failed flows.
5	The SMF performs the resource allocation in 5GS network and sends it to the UPF excluding the failed flows.
6	The SMF sends the Sm Context Create Response with resource allocation request to the target RAN.
7	The AMF forwards the resource allocation request to the NG-RAN.
8	The NG-RAN sends the resource allocation response with the details of successful and failed flows to the AMF. The target RAN node may not be able to allocate the resources for all the requested flows during EPS to 5GS handover procedure. The target RAN shares information about such failed flows in the resource allocation response.
9	The AMF sends the Sm Context Update Request with flows established and failed to establish in the target RAN.
10	The SMF identifies the failed flows at the target RAN.
11	The SMF performs the user plane resource update in 5G network excluding the failed flows.
12	The SMF sends the Sm Context Update Response with PDN connection including the bearer contexts handed over to the 5GS network.
13	The UE is moved to the 5GS network.
14	The SMF uses the EBI assignment procedure to release the EBIs of failed flows.
15	The SMF sends the N1N2 transfer request with the N1 NAS message to the UE to remove the resources of failed flows.
16	If the PCF has installed triggers to release the resources, then the SMF notifies the PCF about the failed flows.

Handling of Flow Failures from Source in EPS to 5GS Handover

The following call flow depicts the handling of flow failure from source RAN in EPS to the 5GS handover.

Figure 69: Flow Failure Handling Call Flow (From Source in EPS to 5GS Handover)

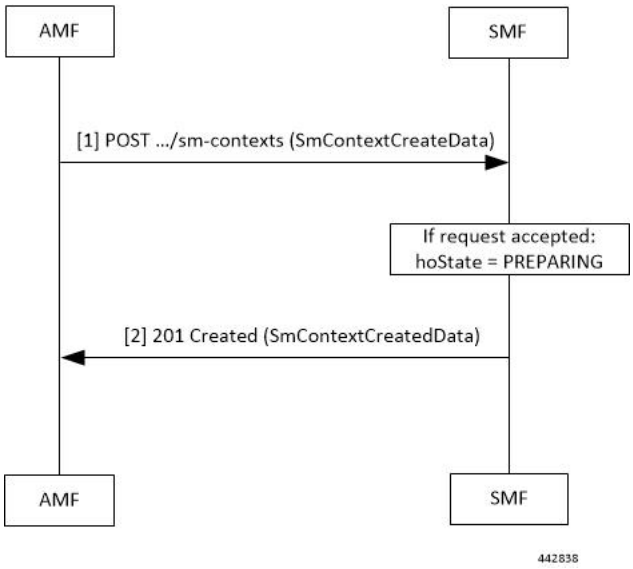


Table 81: Flow Failure Handling Call Flow Description (From Source in EPS to 5GS Handover)

Step	Description
1	The AMF sends a POST request for Sm Context Create Service, with the following additional information: • UE EPS PDN connection, including the EPS bearer contexts, representing the individual SM context resource to be created. The UE EPS PDN connection may not carry the flows which source does not want to establish in the 5GS network. • hoState attribute set to PREPARING • targetId identifying the target RAN Node ID and TAI based on the Target ID IE received in the Forward Relocation Request message from the source MME.

Step	Description
2	If the corresponding PDU session is detected based on the EPS bearer contexts and the handover of the PDN connection to 5GS network is possible, then the SMF returns a 201 Created response including the following information: • hoState attribute set to PREPARING and N2 SM information to request the target RAN to assign resources to the PDU session, excluding the flows which are not received in the UE EPS PDN connection. • PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection. • allocatedEbiList containing the EBIs allocated to the PDU session. The POST response includes the Location header and the URI of the created SM context resource. The AMF stores the association of the PDU Session ID and the SMF ID, and the allocated EBIs associated to the PDU Session ID.

Handling of Flow Failures from Target in EPS to 5GS Handover

The following call flow depicts the handling of flow failure from target RAN in EPS to the 5GS handover.

Figure 70: Flow Failure Handling Call Flow (From Target in EPS to 5GS Handover)

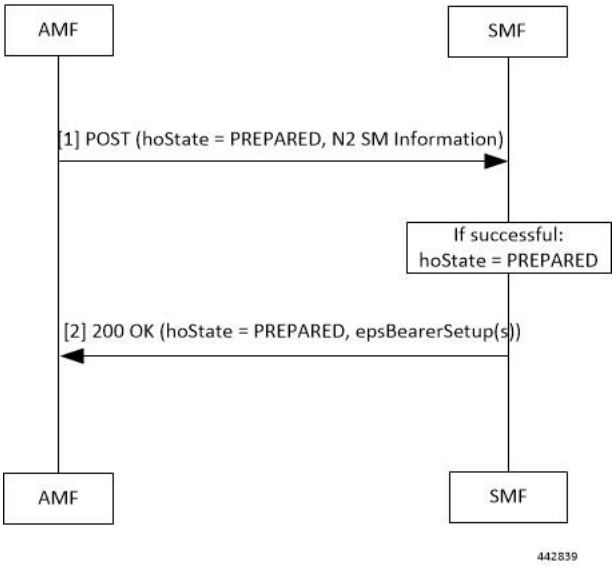


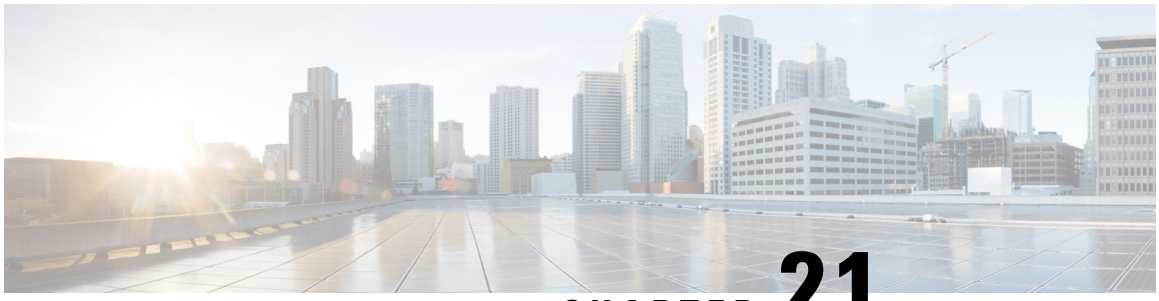
Table 82: Flow Failure Handling Call Flow Description (From Target in EPS to 5GS Handover)

Step	Description
1	The AMF updates the SM context in the SMF by sending POST request with the following information: • hoState attribute set to PREPARED • N2 SM information received from the target RAN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session (that is, GTP-U F-TEID of the target RAN for downlink traffic), if the target RAN succeeded in establishing resources for the PDU session; the target RAN may not be able to establish resources for all the flows; the target RAN includes such failed flows information
2	If the target RAN succeeded in establishing resources for the PDU sessions, the SMF sets the hoState attribute to PREPARED and returns a 200 OK response including the following information: • hoState attribute set to PREPARED • the epsBearerSetup IEs containing the list of EPS bearer contexts successfully handed over to the 5GS and the CN tunnel information for data forwarding, generated based on the list of accepted QFIs received from the RAN; This is the final list of flows handed over to the 5GS network.

Standards Compliance

The QoS Flow Failure Handling for Access and Mobility Procedures feature complies with the following standards:

- 3GPP TS 23.502 V16.1.1 (2019-06)



CHAPTER 21

Inter gNodeB Handover

This chapter covers the following topics:

Feature Summary and Revision History

Summary Data

Table 83: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the Xn-based and N2-based handover procedures to hand over a UE from a source NG-RAN node to a target NG-RAN node using the Xn or N2 reference points. Initiation of this procedure can be due to new radio conditions, load balancing or due to a specific service.

The SMF releases the QoS flows that failed to set up on the target NG-RAN during Xn and N2 handovers on the respective interfaces N4 (UPF) and N1 (UE). The SMF sends appropriate notification to N7 (PCF) based on the triggers if armed. The SMF also sends the usage report to N40 (CHF) for the released QoS flows.

How it Works

Call Flows

The following sections explain the execution of Xn-based and N2-based handover procedures.

Xn-based Inter NG-RAN Handover

This section provides details regarding the Xn-based inter NG-RAN handover without UPF reallocation.

The handover preparation and the execution stages are implemented as specified in 3GPP TS 38.300. When performing the handover in a shared network, the source NG-RAN determines a PLMN to be used in the target network as specified in 3GPP TS 23.501. If the serving PLMN changes during the Xn handover, the source NG-RAN node indicates the selected PLMN ID to the target NG-RAN node.

If the AMF generates the N2 downlink signalling and receives a rejection to an N2 interface procedure due to the ongoing Xn handover procedure, the AMF reattempts the same N2 interface procedure either when the handover is complete or the handover is deemed to have failed. The failure is known by expiry of the timer guarding the N2 interface procedure.

Upon reception of an SMF-initiated N1 and/or N2 request(s) with an indication that the request has been temporarily rejected due to the ongoing Xn handover procedure, the SMF starts a locally configured guard timer. The SMF holds signalling messages targeted towards the AMF during the handover preparation phase unless it detects that the handover is completed or the handover has failed or cancelled. The SMF reattempts, up to a pre-configured number of times, when either it detects that the handover is completed or has failed using message reception or at expiry of the guard timer.

The Xn-based inter NG-RAN handover is used to hand over a UE from a source NG-RAN to target NG-RAN using Xn when the AMF is unchanged and the SMF decides to keep the existing UPF.

The following figure depicts the call flow of the Xn-based inter NG-RAN handover without the UPF reallocation.

Figure 71: Xn-based Inter NG-RAN Handover without UPF Reallocation

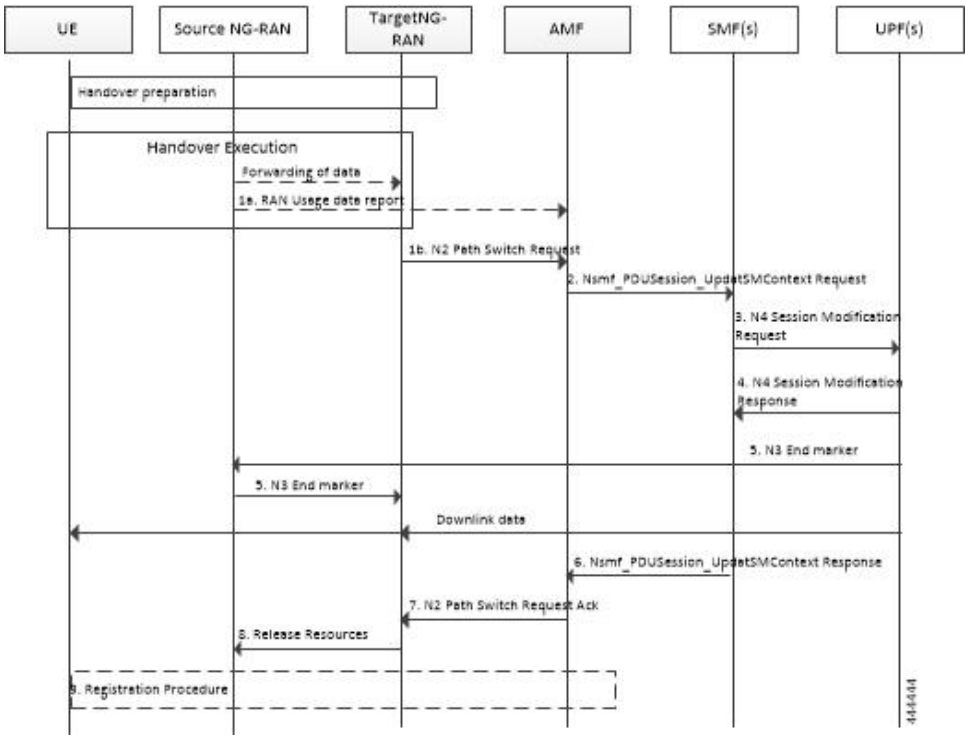


Table 84: Xn-based Inter NG-RAN Handover Call Flow Description (Without UPF Reallocation)

Step	Description
1a	During the handover execution, the source NG-RAN node provides RAN usage data Report to the AMF. The source NG-RAN node provides this report only when the target NG-RAN has confirmed handover over Xn interface. This report includes N2 SM Information (Secondary RAT usage data), Handover Flag, and Source to Target transparent container. The Handover Flag indicates that the report needs to be buffered by the SMF.
1b	The target NG-RAN sends an N2 Path Switch Request message to the AMF to inform that the UE has moved to a new target cell. The NG-RAN provides a List Of PDU Sessions To Be Switched. The N2 SM Information includes the AN Tunnel Info for each PDU Session to be switched.
2	The AMF sends N2 SM information by invoking the Nsmf_PDUSession_UpdateSMContext request service operation for each PDU session in the lists of PDU Sessions received in the N2 Path Switch Request.
3	The SMF sends an N4 Session Modification Request message to the UPF. The SMF may notify the UPF that originated the Data Notification to discard downlink data for the PDU Sessions and/or to not provide further Data Notification messages.
4	The UPF returns an N4 Session Modification Response message to the SMF after the requested PDU sessions are switched.

Step	Description
5	The UPF sends one or more "end marker" packets for each N3 tunnel on the old path immediately after switching the path. The UPF starts sending downlink packets to the target NG-RAN.
6	The SMF sends an Nsmf_PDUSession_UpdateSMContext response (CN Tunnel Info) to the AMF for PDU sessions which have been switched successfully. **Important** Step 6 can occur any time after the receipt of N4 Session Modification Response at the SMF.
7	Once the Nsmf_PDUSession_UpdateSMContext response is received from all the SMFs, the AMF aggregates the received CN Tunnel Info and sends this aggregated information as a part of N2 SM Information along with the Failed PDU Sessions in N2 Path Switch Request Ack to the target NG-RAN. If none of the requested PDU sessions have been switched successfully, the AMF sends an N2 Path Switch Request Failure message to the target NG-RAN.
8	The target NG-RAN confirms success of the handover by sending Release Resources message to the source NG-RAN.
9	The UE initiates Mobility Registration Update procedure if one of the triggers of registration procedure applies.

The following figure shows the detailed call flow of the Xn handover without UPF reallocation.

Figure 72: Xn Handover Without UPF Relocation Call Flow

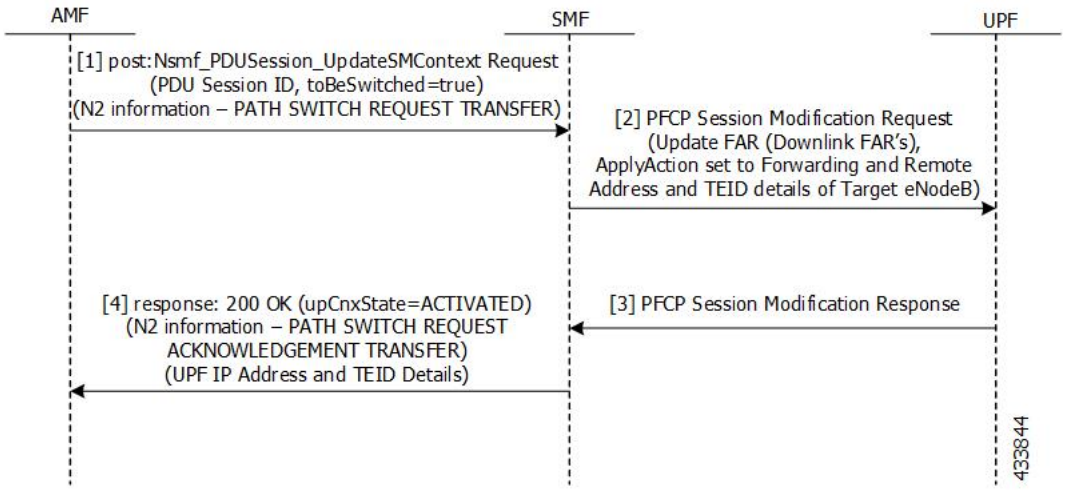


Table 85: Detailed Call Flow Description for the Xn Handover Without UPF Relocation

Step	Description
1	The NF Service Consumer (AMF) requests the SMF to switch the user plane connection of the PDU session. The AMF sends a POST request with the following information: • The toBeSwitched indication. • N2 SM information received from the 5G-AN (PDU session path switch request transfer IE), including the new transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session. • User location and user location timestamp. • Other information, if necessary.
2	The SMF switches the N3 tunnel of the PDU session after receiving the request. The SMF initiates PFCP session modification procedure toward the UPF with downlink FAR updated with the following option: • Forwarding Action is enabled with the remote node "forwarding parameters" details, such as the IP address and GTP-U F-TEID.
3	The SMF marks the PDU handover as successful after receiving the successful response from the UPF node.
4	The SMF initiates the 200 OK response. This response includes the N2 SM information, which has the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session, that is UPFs GTP-U F-TEID for the uplink traffic.

N2-based Inter NG-RAN Handover

The source NG-RAN decides to initiate an N2-based handover (HO) to the target NG-RAN. Initiation of this procedure could be due to any of the following reasons:

- New radio conditions
- Load balancing
- If there is no Xn connectivity to the target NG-RAN
- An error indication from the target NG-RAN after an unsuccessful Xn-based handover (that is, no IP connectivity between Target RAN (T-RAN) and Source UPF (S-UPF))
- Based on dynamic information learnt by the Source RAN (S-RAN)

The source NG-RAN determines the availability of a direct forwarding path and indicates the same to the SMFs. If the IP connectivity is available between the source and target NG-RAN and security association is in place between them, a direct forwarding path is available. If a direct forwarding path is not available, use the indirect forwarding. The SMFs use the indication from the source NG-RAN to choose the data forwarding path.

When performing the handover in a shared network, the source NG-RAN determines a PLMN for use in the target network as specified by 3GPP TS 23.501. The source NG-RAN indicates the selected PLMN ID to the AMF as part of the Tracking Area sent in the HO Required message.

If the AMF generates the N2 downlink signalling and receives a rejection to a N2 interface procedure due to the ongoing N2 handover, the AMF reattempts the same N2 interface procedure either when the handover is complete or the handover is deemed to have failed. If the Inter NG-RAN node handover changes the serving AMF, the source AMF terminates any other ongoing N2 interface procedures except the handover procedure.

If the AMF is still the serving AMF, the AMF pauses non-handover related N2 interface procedures and resumes them after the N2 handover is complete.

If the AMF detects that it needs to be changed, the AMF rejects any SMF-initiated N2 request and includes an indication that the request has been temporarily rejected due to the ongoing N2 handover procedure.

The following figure depicts the call flow for the preparation phase of the N2-based inter NG-RAN handover procedure.

Figure 73: Inter NG-RAN Node N2-based Handover - Preparation Phase

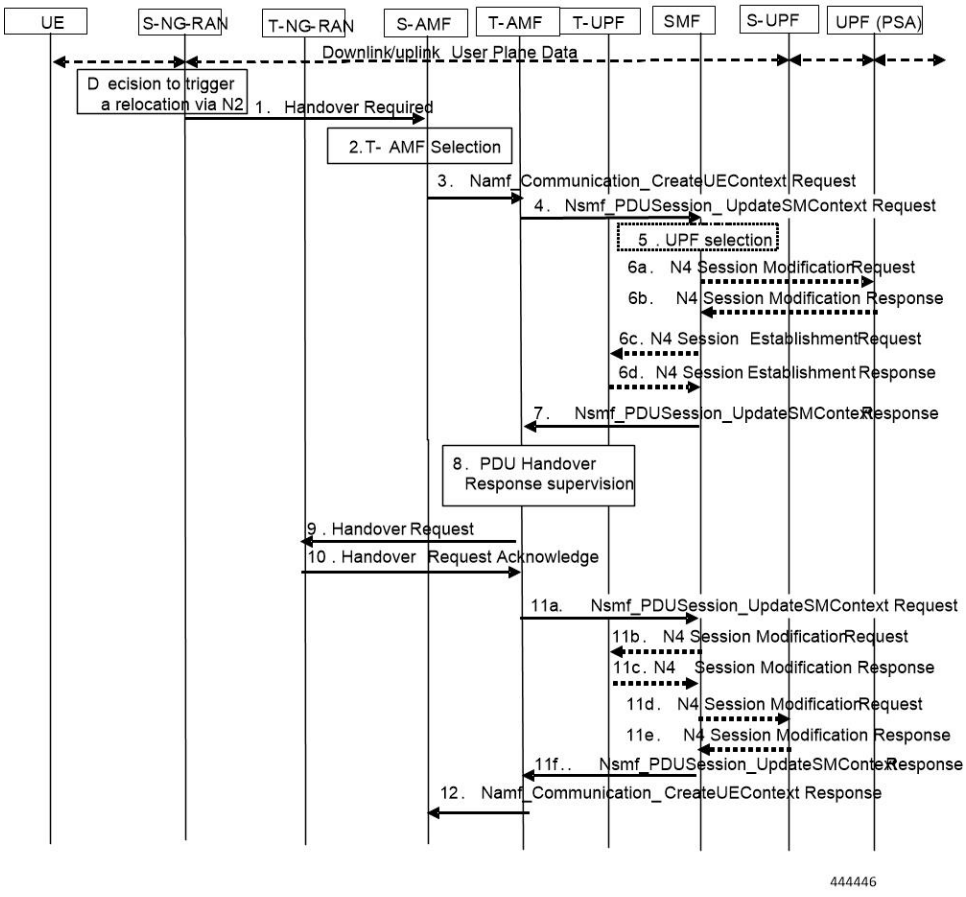


Table 86: Inter NG-RAN Node N2-based Handover Call Flow Description - Preparation Phase

Step	Description
1	The Source NG-RAN (S-RAN) sends the Handover Required message to the Source AMF (S-AMF). This message includes the following: • Target ID • Source to Target transparent container • SM N2 info list • PDU Session IDs • Intra system handover indication The Source to Target transparent container includes NG-RAN information for use in Target RAN (T-RAN), and is transparent to 5GC. It also contains the corresponding User Plane Security Enforcement information, QoS flows/DRBs information subject to data forwarding. If direct data forwarding is available, the SM N2 info includes Direct Forwarding Path Availability. Direct Forwarding Path Availability indicates whether direct forwarding is available from the S-RAN to the T-RAN. This indication from S-RAN is based on the presence of IP connectivity and security association between the S-RAN and the T-RAN.
2	When the S-AMF cannot serve the UE anymore, the S-AMF selects the T-AMF as described in clause 6.3.5 on "AMF Selection Function" in TS 23.501.

Step	Description

3	The S-AMF initiates Handover resource allocation procedure by invoking the Namf_Communication_CreateUEContext service operation towards the T-AMF.
	The Namf_Communication_CreateUEContext Request includes the following:
	• N2 Information
	  • Target ID
	  • Source to Target transparent container
	  • SM N2 information list
	  • PDU Session IDs
	• UE context information
	  • SUPI
	  • Service area restriction
	  • Allowed NSSAI for each Access Type if available
	  • Tracing Requirements
	  • The list of PDU Session IDs along with the corresponding SMF information and the corresponding S-NSSAI(s), PCF ID(s), and DNN
	When the S-AMF can still serve the UE, this step and step 12 are not needed.

4	For each PDU session indicated by S-RAN, the AMF invokes the Nsmf_PDUSession_UpdateSMContext Request to the associated SMF. However, if the S-NSSAI associated with PDU session is not available in the T-AMF, the T-AMF does not invoke Nsmf_PDUSession_UpdateSMContext for this PDU session. If the T-AMF detects that the UE moves into a restricted area based on Service area restrictions, the T-AMF notifies that the UE is only reachable for regulatory prioritized services to each NF consumer which has subscribed for UE reachability event.
5	Based on the Target ID, the SMF checks the acceptance of N2 handover for the indicated PDU session. The SMF also checks the UPF Selection Criteria. If the UE has moved out of the service area of the UPF connecting to NG-RAN, the SMF selects a new intermediate UPF.
6a	If the SMF selects a new UPF to act as intermediate UPF for the PDU session, and the different CN Tunnel Info need to be used, the SMF sends N4 Session Modification Request message to UPF (PDU Session Anchor (PSA)). If the SMF allocates the CN Tunnel Info, it provides the CN Tunnel Info on N9, and the UPF (PSA) associates CN Tunnel Info with UL Packet detection rules.

Step	Description
6b	The UPF (PSA) sends an N4 Session Establishment Response message to the SMF. If the UPF (PSA) allocates CN Tunnel Info (on N9) of UPF (PSA), it provides CN Tunnel Info (on N9) to the SMF. The UPF (PSA) associates the CN Tunnel Info (on N9) with UL Packet detection rules provided by the SMF.
6c	If the SMF selects a new intermediate UPF (T-UPF) and if the T-UPF allocates the CN Tunnel Info, the SMF sends an N4 Session Establishment Request message to the T-UPF. This request enables the Packet detection, enforcement, and reporting rules to be installed on the T-UPF. The T-UPF receives the CN Tunnel Info (on N9) of UPF (PSA) for this PDU session, which is used to set up N9 tunnel.
6d	The T-UPF sends an N4 Session Establishment Response message to the SMF with DL CN Tunnel Info and UL CN Tunnel Info (that is, N3 tunnel info). The SMF starts a timer to release the resource of S-UPF, which is to be used in step 13a of the Execution Phase.
7	If N2 handover for the PDU session is accepted, the SMF includes the N2 SM Information in the Nsmf_PDUSession_UpdateSMContext response. The N2 SM Information contains the N3 UP address and the UL CN Tunnel ID of the UPF and the QoS parameters indicating that the N2 SM Information is for the Target NG-RAN. If the N2 SM information received at step 4 does not include the Direct Forwarding Path Availability and the SMF knows that there is no indirect data forwarding connectivity between source and target, the N2 SM Information includes a Data forwarding not possible indication. If the N2 handover for the PDU session is not accepted as described in step 5, the SMF does not include the N2 SM Information to avoid establishment of radio resources at the target NG-RAN. The SMF provides a reason for non-acceptance. If the SMF receives notification from T-AMF that UE is only reachable for regulatory prioritized service, the SMF deactivates the PDU session.
8	The AMF supervises the Nsmf_PDUSession_UpdateSMContext Response messages from the involved SMFs. At the expiry of maximum wait time or when all Nsmf_PDUSession_UpdateSMContext Response messages are received, the AMF continues with the N2 Handover procedure (Handover Request message in step 9).
9	If the subscription information includes Tracing Requirements, the target AMF provides the target RAN with Tracing Requirements in the Handover Request. The Handover request includes Source to Target transparent container, N2 MM Information, N2 SM Information list, and Tracing Requirements. The T-AMF determines T-RAN based on Target ID. T-AMF allocates a 5G-GUTI valid for the UE in the AMF and target TAI. N2 MM Information includes, for example, security information and Mobility Restriction List if available in the T-AMF. N2 SM Information list includes N2 SM Information for the T-RAN in the Nsmf_PDUSession_UpdateSMContext Response messages received within allowed max delay supervised by the T-AMF in step 8.

Step	Description
10	The T-RAN sends Handover Request Acknowledge to the T-AMF. The Acknowledge message includes Target to Source transparent container, List of PDU Sessions to Hand-over with N2 SM information, List of PDU Sessions that failed to be established with the failure cause given in the N2 SM information element.
11a	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID, N2 SM response) to the SMF. For each N2 SM response received from the T-RAN, the AMF sends the N2 SM response to the SMF indicated by the respective PDU Session ID. If no new T-UPF is selected, the SMF stores the N3 tunnel info of T-RAN from the N2 SM response if N2 handover is accepted by T-RAN. The SMF/UPF allocates the N3 UP address and Tunnel IDs for indirect data forwarding corresponding to the data forwarding tunnel endpoints established by T-RAN. If a PDU session is indicated as a rejected PDU session by the Target NG-RAN, the SMF triggers the release of this PDU session. In all other cases of PDU Session rejection, the SMF decides whether to release the PDU session or to deactivate the UP connection of this PDU session. If some of the QoS Flows of a PDU Session are not accepted by the Target NG-RAN, the SMF initiates the PDU Session Modification procedure to remove the non-accepted QoS Flows from the PDU Session(s) after the handover is completed.
11b	The SMF sends N4 Session Modification Request to the T-UPF. This request includes T-RAN SM N3 forwarding Information list, and indication to allocate DL forwarding tunnel(s) for indirect forwarding.
11c	The T-UPF allocates Tunnel Info and returns an N4 Session Modification Response message to the SMF. The T-UPF SM N3 forwarding info list includes T-UPF N3 address, T-UPF N3 Tunnel identifiers for forwarding data.
11d	The SMF sends N4 Session Modification Request to the S-UPF. This request includes T-RAN SM N3 forwarding Information list or T-UPF SM N3 forwarding Information list, and an indication to allocate DL forwarding tunnel(s) for indirect forwarding.
11e	The S-UPF allocates Tunnel Info and returns an N4 Session establishment Response message to the SMF. The S-UPF SM N3 forwarding Information list includes S-UPF N3 address and S-UPF N3 Tunnel identifiers for DL data forwarding.
11f	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response message per PDU session to the T-AMF.

Step	Description
12	The AMF supervises the Nsmf_PDUSession_UpdateSMContext Response message from the involved SMFs. At the expiry of maximum wait time or when all Nsmf_PDUSession_UpdateSMContext Response messages are received, the T-AMF sends the Namf_Communication_CreateUEContext Response to the S-AMF.

The following figure depicts the call flow for the execution phase of the N2-based inter NG-RAN handover procedure.

Figure 74: Inter NG-RAN Node N2-based Handover - Execution Phase

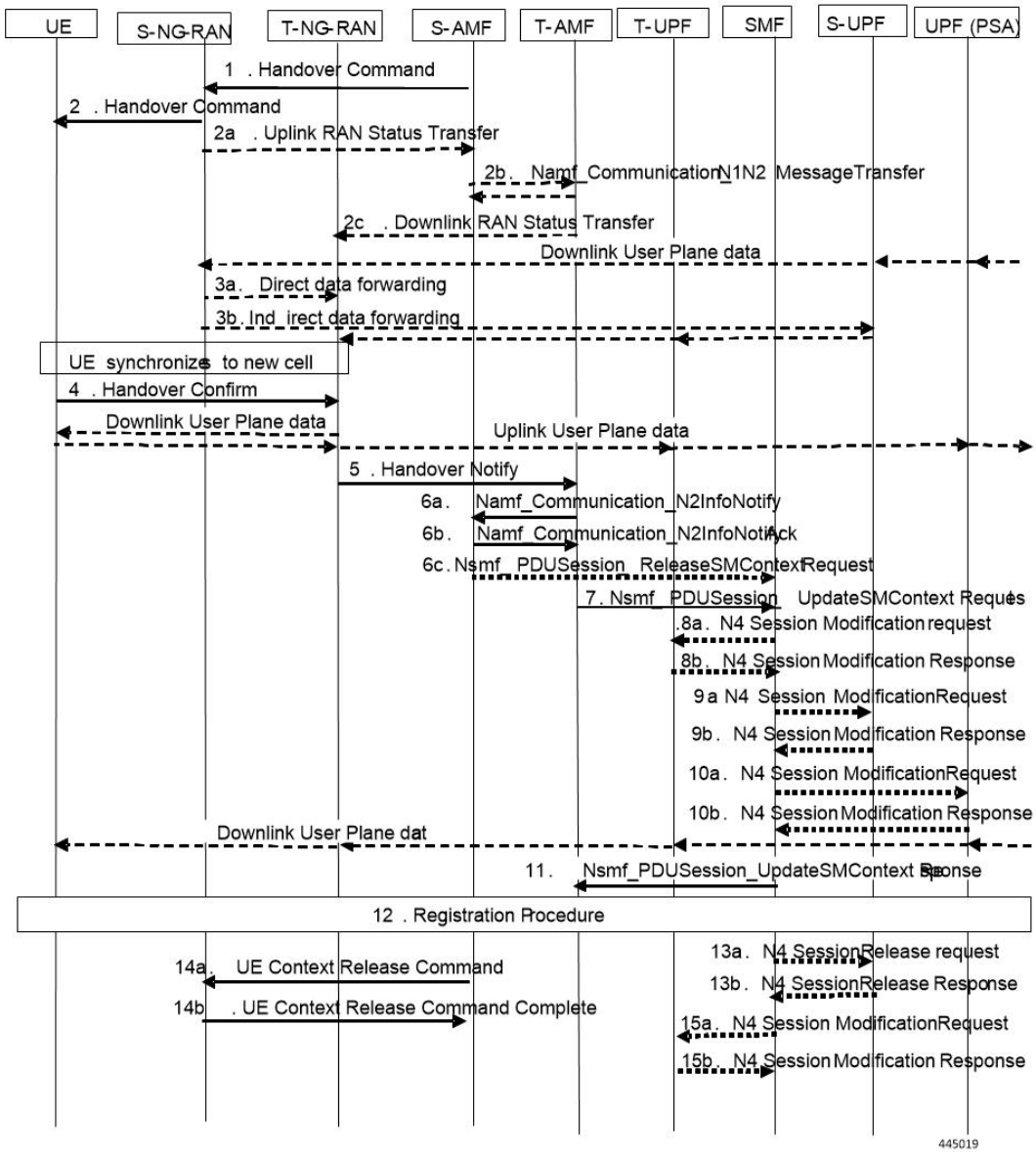


Table 87: Inter NG-RAN Node N2-based Handover Call Flow Description - Execution Phase

Step	Description
1	The Source AMF (S-AMF) sends the Handover Command to the Source NG-RAN (S-RAN). The Handover Command includes Target to Source transparent container, List Of PDU Sessions to be handed-over with N2 SM information containing information received from T-RAN during the handover preparation phase, and List Of PDU Sessions failed to be set up. The SM forwarding info list includes T-RAN SM N3 forwarding info list for direct forwarding or S-UPF SM N3 forwarding info list for indirect data forwarding. The S-RAN uses the PDU Sessions failed to be setup list and the indicated reason for failure to decide whether to proceed with the N2 handover procedure.
2	The S-RAN sends Handover Command (UE container) to the UE. The UE container is a UE part of the Target to Source transparent container which is sent transparently from T-RAN via AMF to S-RAN and is provided to the UE by the S-RAN.
2a - 2c	The S-RAN sends the Uplink RAN Status Transfer message to the S-AMF. The S-RAN refrains from sending this message if none of the radio bearers of the UE are treated with Packet Data Convergence Protocol (PDCP) status preservation.
3	The T-RAN sends the uplink packets to the T-UPF and UPF (PSA). The UPF (PSA) sends the downlink packets to the S-RAN via S-UPF. The S-RAN forwards the downlink data towards the T-RAN for QoS flows or Data Radio Bearers (DRBs) subject to data forwarding. The data forwarding path is either direct (step 3a) or indirect forwarding (step 3b).
4	After the UE has successfully synchronized to the target cell, it sends a Handover Confirm message to the T-RAN.
5	The T-RAN sends Handover Notify message to the T-AMF. This message is sent to indicate that the handover is successful.
6a.	The T-AMF notifies to the S-AMF about the N2 handover notify received from the T-RAN by invoking the Namf_Communication_N2InfoNotify. The S-AMF uses a timer to supervise the release of resources in S-RAN.
6b	The S-AMF acknowledges by sending the Namf_Communication_N2InfoNotify ACK to the T-AMF.
6c	The S-AMF sends Nsmf_PDUSession_ReleaseSMContext Request to the SMF. This request includes SUPI, PDU Session ID, and N2 SM Information (Secondary RAT Usage Data). If the PDU Session(s) is not accepted by the T-AMF, the S-AMF triggers PDU Session Release procedure after the reception of N2 Handover Notify.

Step	Description
7	The T-AMF sends Nsmf_PDUSession_UpdateSMContext Request to the SMF. This request includes Handover Complete indication for PDU Session ID, UE presence in LADN service area, and N2 SM Information (Secondary RAT usage data). The T-AMF sends Handover Complete indication per each PDU Session to the corresponding SMF to indicate the success of the N2 handover.
8a	If a new T-UPF is inserted or an existing intermediate S-UPF is reallocated, the SMF sends N4 Session Modification Request indicating DL AN Tunnel Info of T-RAN to the T-UPF.
8b	The T-UPF acknowledges by sending N4 Session Modification Response message to the SMF.
9a	If the UPF is not reallocated, the SMF sends N4 Session Modification Request indicating DL AN Tunnel Info of T-RAN to the S-UPF.
9b	The S-UPF acknowledges by sending N4 Session Modification Response message to SMF.
10a	For non-roaming or local breakout roaming scenario, the SMF sends N4 Session Modification Request message to PDU Session Anchor UPF, UPF (PSA). If a new T-UPF is inserted or an existing intermediate S-UPF is reallocated, the SMF provides N3 AN Tunnel Info of T-RAN or the DL CN Tunnel Info of T-UPF. If the T-UPF is not inserted or an existing intermediate S-UPF is not reallocated, skip the step 10a and step 10b.
10b	The UPF (PSA) sends N4 Session Modification Response message to the SMF. When there are multiple UPFs (PSA), perform step 10a and step 10b for each UPF (PSA).
11	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (PDU Session ID) to the T-AMF. The SMF confirms reception of Handover Complete.
12	The UE initiates Mobility Registration Update procedure as defined in 3GPP TS 23.502.
13a	If there is a source intermediate UPF, the SMF initiates resource release by sending an N4 Session Release Request (Release Cause) to the source UPF. This message is also used to release the indirect data forwarding resource in the S-UPF.
13b	The S-UPF acknowledges with an N4 Session Release Response message to confirm the release of resources. In case of indirect data forwarding, the resource of indirect data forwarding is also released.
14a	After the expiry of timer (defined in step 6a), the AMF sends UE Context Release Command.

Step	Description
14b	The source NG-RAN releases its resources related to the UE and responds with a UE Context Release Complete () message.
15a	If indirect forwarding applies and the UPF is reallocated, after the timer of indirect data forwarding expires, the SMF sends N4 Session Modification Request to the T-UPF. Then, the T-UPF releases the indirect data forwarding resources.
15b	The T-UPF acknowledges with an N4 Session Modification Response message to confirm the release of indirect data forwarding resources.

Limitations

The Xn-based handover with UPF reallocation is currently not supported.

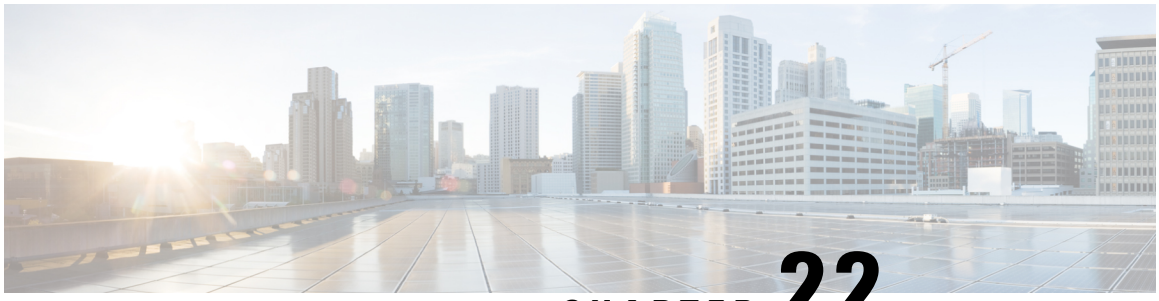
OAM Support

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

Statistics Support

The "smf_ran_failed_flows" metric is added to identify the number of QoS flows released by RAN as part of various call flow procedures including the Xn and N2 handover procedures.

The SMF uses the "xn_handover" label to account for Xn handovers. Similarly for the N2 handovers, the SMF uses the "n2_handover" label.



CHAPTER 22

IP Address Management

Feature Summary and Revision History

Summary Data

Table 88: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 89: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

IP Address Management (IPAM) is a method of tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. Traditional IPAM functionalities are insufficient in Cloud-Native network deployments. Hence, IPAM requires additional functionalities to work with the Cloud-Native subscriber management system. The Cloud-Native IPAM system is used in various network functions, such as SMF and PCF.

The IPAM system includes the following functionalities to serve the Cloud Native and Control and User Plane Separation (CUPS) architecture:

- **Centralized IP resource management** —Based on the needs of the Internet Service Provider (ISP), the Control Plane (CP) is deployed either on a single (centralized) cluster or multiple (distributed) clusters. For multiple cluster deployments, the IPAM automatically manages the single IP address space across the multiple CPs that are deployed in the distributed environment.
- **IP address-range reservation per user-plane**—For subscribers connecting to the Internet core, the User Plane (UP) provides the physical connectivity. The UP uses the summary-routes to advertise subscriber routes to the Internet core. For CPs that are managing multiple UPs, the CP reserves a converged IP subnet to the UPs. In such a scenario, the IPAM splits the available address space into smaller address-ranges and assigns it to different UPs.
- **IP address assignment from pre-reserved address-ranges**—When subscribers request for an IP address, the IPAM assigns addresses from the pre-reserved address range of their respective UP.

How it Works

IPAM uses the following sub-modules for the Cloud-Native subscriber management system:

- IPAM Server—This module manages the complete list of pools and address-space configurations. The IPAM server splits the configured address ranges into smaller address-ranges statically or dynamically to distribute them to IPAM cache modules. The IPAM server is deployed as a centralized entity to serve group of Cloud-Native clusters or can be an integrated entity within a single cluster.
- IPAM Cache—This module receives the free address-ranges from the IPAM server and allocates the individual IP addresses to the IPAM clients. Usually, the IPAM cache is deployed in a distributed mode running within each cluster to communicate with the co-located or remotely-located IPAM server. The IPAM cache also handles address-range reservation per UP and pool threshold monitoring. The IPAM server and cache modules can run as an integrated mode.
- IPAM Client—This module handles the request and release of an individual IP address from the IPAM cache for each IP managed end-device. The IPAM client is tightly coupled with a respective network-function.

IPAM Integration in SMF

Feature Description

The IP Address Management (IPAM) is a technique for tracking and managing the IP address space of a network. A core component of the subscriber management system, the IPAM provides all the functionalities necessary for working with the Cloud-Native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions such as the SMF, Policy Control Function (PCF), and so on.

The IPAM is integrated with the SMF in the Application Services layer.

Architecture

This section describes the IPAM integration in the SMF architecture.

IPAM Integration in SMF

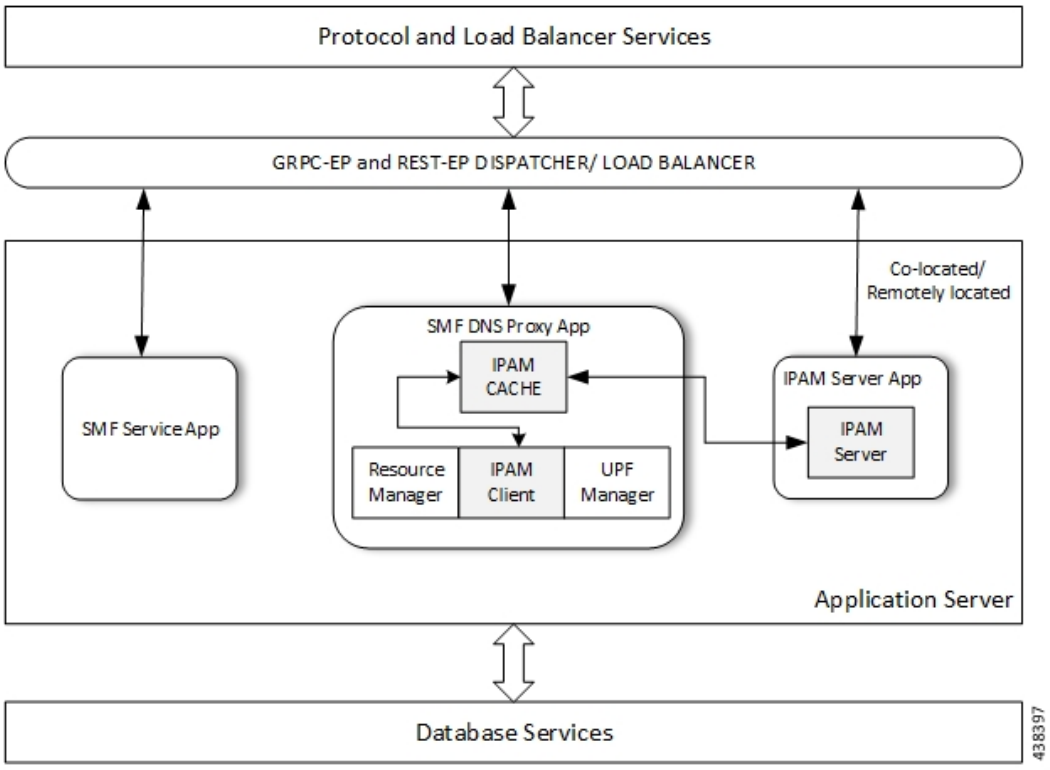
The SMF comprises of loosely coupled microservices that enables the SMF to perform session management (session establishment, modification, and release) and other associated functions. The decomposition of these microservices is based on the following three-layered architecture:

1. Layer 1: Protocol and Load Balancer Services (Stateless)
2. Layer 2: Application services (Stateless)
3. Layer 3: Database Services (Stateful)

The IPAM and SMF integration happens in the Application Services layer.

The following describes the SMF and IPAM integration architecture in the Application Services layer.

Figure 75: IPAM Integration in SMF



- **SMF Node-Manager Application** – The SMF Node-Manager application takes care of the UPF, ID resource, and IP address management. Therefore, the SMF Node-Manager application integrates IPAM Cache and IPAM client modules. The UPF Manager uses the IPAM Client module for address-range-reservation per UPF.
- **SMF Service Application** – The SMF Service application provides PDU session services. During session establishment and termination, the IP addresses are requested and released back. The SMF Service application invokes the IPC to RMGR in Node Manager, which receives (free) the IP from the IPAM module.
- **IPAM Server Application** – Based on the deployment model, the IPAM Server application can run as an independent microservice, as a part of the same cluster, or in a remote-cluster. For standalone deployments, the IPAM Servers are an integral part of the IPAM cache.

Components

This section describes the different components of the IPAM system.

IPAM Sub-Modules

The IPAM system includes the following sub-modules:

- **IPAM Server** – The IPAM Server module manages the complete list of pools and address-space configuration. It splits the configured address-ranges into smaller address-ranges (statically and dynamically) and distributes it to the IPAM Cache modules. You can deploy the IPAM Server either as

a centralized entity to serve a group of cloud native clusters or as an integrated entity within a single cluster.

- **IPAM Cache** – The IPAM Cache acquires free address-ranges from the IPAM Server and allocates individual IP addresses to the IPAM clients. Deployed in a distributed mode running within each cluster, the IPAM Cache communicates with co-located and remotely located IPAM Servers. Additionally, the IPAM Cache takes care of the address-range reservation per Data-Plane and pool threshold monitoring.
- **IPAM Client** – The IPAM Client module handles the request and release of the individual IP addresses from the IPAM Cache for each IP managed end-device. Based on the use cases, the IPAM Client module caters the needs of specific network functions (such as SMF, PCF, and so on).

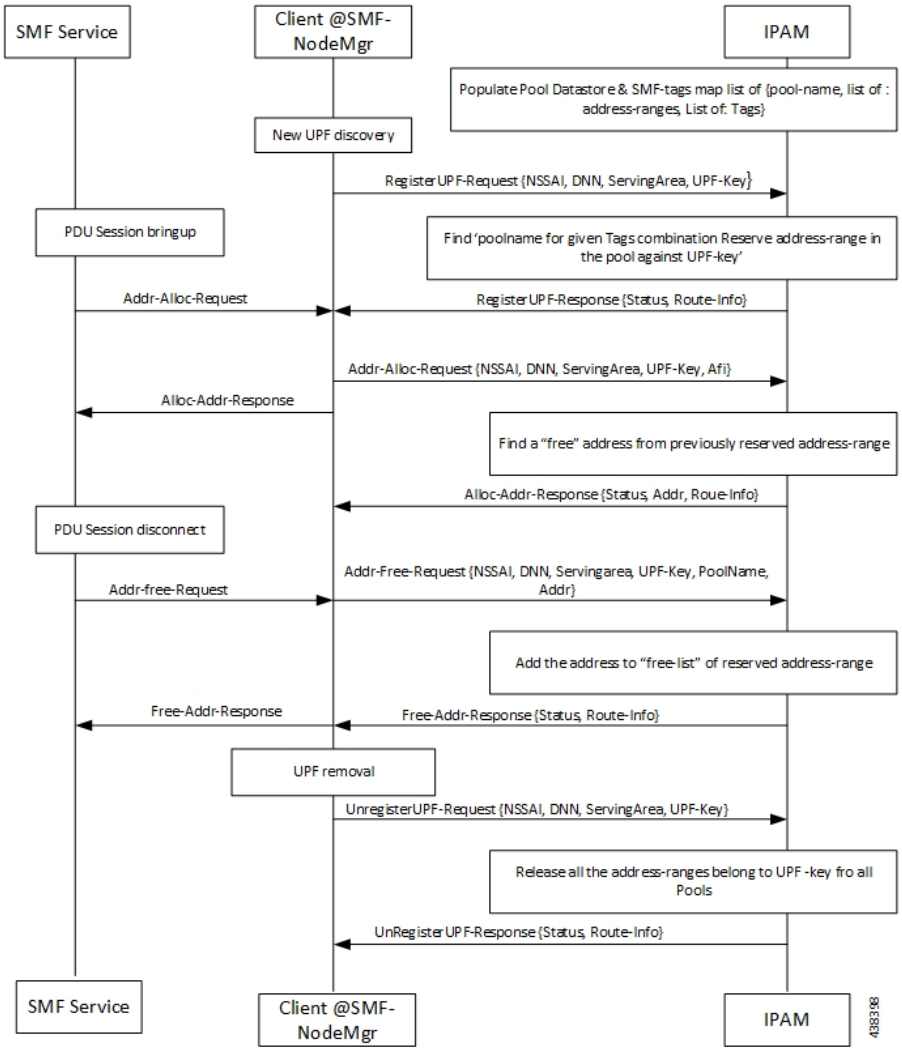
How it Works

This section describes the call flows pertaining to the integration of the IPAM in the SMF.

Call Flows

The following call flow depicts the integration of the IPAM in the SMF.

Figure 76: Integration of IPAM in SMF Call Flow



Configuring the IPAM Feature

This section describes how to configure the IPAM in the SMF.

Configuring the IPAM in the SMF involves the following steps:

1. Configuring IPv4 address ranges.
2. Configuring IPv6 address ranges.
3. Configuring IPv6 prefix ranges.
4. Configuring SMF tags.
5. Configuring IPv4 threshold.
6. Configuring IPv6 address range threshold.

7. Configuring IPv6 prefix range threshold.
8. Configuring IPv4 address range split.
9. Configuring IPv6 address and prefix address range split.
10. Configuring global threshold.
11. Configuring IPAM source.

Configuring IPv4 Address Ranges

Use the following configuration to configure the IPv4 address ranges.

```
configure
   ipam
      address-pool pool_name
         vrf-name string
         ipv4
            address-range start_ipv4_address end_ipv4_address
            commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **vrf-name** *string*: Configures the Virtual routing and forwarding (VRF) name of the pool.
- **ipv4**: Enters the IPv4 mode of the pool.
- **address-range** *start_ipv4_address end_ipv4_address*: Configures the IPv4 range. *start_ipv4_address* specifies the starting IPv4 address. *end_ipv4_address* specifies the ending IPv4 address.

The following is a sample configuration:

```
configure
   ipam
      address-pool p1
         vrf-name one
         ipv4
            address-range 1.1.1.10 1.1.1.255
            address-range 2.2.2.1 2.2.2.255
```

Configuring IPv6 Address Ranges

Use the following configuration to configure the IPv6 address ranges:

```
configure
   ipam
      address-pool pool_name
         vrf-name string
         ipv6
            address-range start_ipv6_address end_ipv6_address
            commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **vrf-name** *string*: Configures the VRF name of the pool.
- **ipv6**: Enters the IPv6 mode of the pool.
- **address-range** *start_ipv6_address end_ipv6_address*: Configures the IPv6 range. *start_ipv6_address* specifies the starting IPv6 address. *end_ipv6_address* specifies the ending IPv6 address.

The following is a sample configuration:

```
configure
   ipam
      address-pool p1
         vrf-name one
         ipv6
            address-range 1::1 1::1000
            address-range 2::1 2::1000
```

Configuring IPv6 Prefix Ranges

Use the following configuration to configure the IPv6 prefix ranges:

```
configure
   ipam
      address-pool pool_name
         vrf-name string
         ipv6
            prefix-ranges
               prefix-range prefix_value prefix-length length
               commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **vrf-name** *string*: Configures the VRF name of the pool.
- **ipv6**: Enters the IPv6 mode of the pool.
- **prefix-ranges**: Enters the prefix ranges mode.
- **prefix-range** *prefix_value* **prefix-length** *length* : Configures the IPv6 prefix range. **prefix-range** *prefix_value* specifies the IPv6 prefix range. **prefix-length** *length* specifies the IPv6 prefix length.

The following is a sample configuration:

```
configure
   ipam
      address-pool p3
         vrf-name three
         ipv6
```

```
prefix-ranges
   prefix-range 1:1:: prefix-length 48
   prefix-range 2:1:: prefix-length 48
```

Configuring SMF Tags

Use the following configuration to configure the SMF tags.

```
configure
   ipam
      address-pool pool_name
         tags
            nssai string
            dnn string
            serving-area string
            commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **tag** : Enters the tag section of the pool.
- **nssai** *string*: Specifies the NSSAI value.
- **dnn** *string* : Specifies the DNN value.
- **serving-area** *string*: Specifies the serving-area value.

The following is a sample configuration:

```
configure
   ipam
      address-pool p1
         tags
            nssai one
            dnn two
            serving-area three
```

Configuring IPv4 Threshold

Use the following configuration to configure the IPv4 threshold:

```
configure
   ipam
      address-pool pool_name
         ipv4
            threshold
               upper-threshold percentage
               commit
```

NOTES:

- **ipam**: Enters the IPAM Configuration mode.

- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **ipv4** : Enters the IPv4 mode of the pool.
- **threshold** : Enters the threshold sub-mode.
- **upper-threshold** *percentage*: Specifies the IPv4 upper threshold value in percentage.

The following is a sample configuration:

```
configure
   ipam
      address-pool p1
         ipv4
            threshold
               upper-threshold 80
```

Configuring IPv6 Address Range Threshold

Use the following configuration to configure the IPv6 address range threshold.

```
configure
   ipam
      address-pool pool_name
         ipv6
            address-ranges
               threshold
                  upper-threshold percentage
                  commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **ipv6** : Enters the IPv6 mode of the pool.
- **address-ranges**: Enters the IPv6 address ranges sub-mode.
- **threshold** : Enters the threshold sub-mode.
- **upper-threshold** *percentage*: Specifies the IPv6 upper-threshold value in percentage.

The following is an example configuration:

```
configure
   ipam
      address-pool p2
         ipv6
            address-ranges
               threshold
                  upper-threshold 75
```

Configuring IPv6 Prefix-Range Threshold

Use the following configuration to configure the IPv6 prefix-range threshold.

```
configure
   ipam
      address-pool pool_name
         ipv6
            prefix-ranges
               threshold
                  upper-threshold percentage
                  commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **ipv6** : Enters the IPv6 mode of the pool.
- **prefix-ranges**: Enters the IPv6 prefix ranges sub-mode.
- **threshold** : Enters the threshold sub-mode.
- **upper-threshold** *percentage*: Specifies the IPv6 upper-threshold value in percentage.

The following is an example configuration:

```
configure
   ipam
      address-pool p3
         ipv6
            prefix-ranges
               threshold
                  upper-threshold 78
```

Configuring IPv4 Address Range Spilt

Use the following configuration to configure the IPv4 address range spilt.

```
configure
   ipam
      address-pool pool_name
         ipv4
            spilt-size per-cache integer
            spilt-size per-dp integer
            commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **ipv4** : Enters the IPv4 mode of the pool.
- **spilt-size per-cache** *integer*: Specifies the size of the IPv4 range to be split for each IPAM cache allocation. The IPAM server consumes this configuration.

- **spilt-size-per-dp** *integer*: Specifies the size of the IPv4 range to be spilt for each Data-Plane (User-Plane) allocation. The IPAM cache consumes this configuration.

The following is a sample configuration:

```
configure
   ipam
      address-pool p1
         ipv4
            split-size per-cache 1024
            split-size per-dp 256
```

Configuring IPv6 Address and Prefix Address-Range-Spilt

Use the following configuration to configure the IPv6 address and prefix address range spilt.

```
configure
   ipam
      address-pool pool_name
         ipv6
            address-ranges
               spilt-size per-cache integer
               spilt-size per-dp integer
               commit
            prefix-ranges
               spilt-size per-cache integer
               spilt-size per-dp integer
               commit
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Configures the address pool configuration. *pool_name* must be the name of the address pool.
- **ipv6** : Enters the IPv6 mode of the pool.
- **address-ranges**: Enters the IPv6 address-ranges sub-mode.
- **spilt-size per-cache** *integer*: Specifies the size of the IPv6 adress-ranges or prefix-ranges to be split for each IPAM cache allocation. The IPAM server consumes this configuration.
- **spilt-size-per-dp** *integer*: Specifies the size of the IPv6 adress-ranges or prefix-ranges to be spilt for each Data-Plane (User-Plane) allocation. The IPAM cache consumes this configuration.
- **prefix-ranges**: Enters the IPv6 prefix ranges sub-mode.

The following is a sample configuration:

```
configure
   ipam
      address-pool p1
         ipv6
            address-ranges
               split-size per-cache 4096
               split-size per-dp 1024
               !
            prefix-ranges
```

```
split-size per-cache 8192
split-size per-dp 2048
```

Configuring Global Threshold

Use the following configuration to configure the global threshold.

```
configure
   ipam
      threshold
         ipv4-addr percentage
         ipv6-addr percentage
         ipv6-prefix percentage
         commit
```

NOTES:

- **ipam**: Enters the IPAM Configuration mode.
- **threshold**: Enters the threshold sub-mode.
- **ipv4-addr** *percentage* : Specifies the IPv4 threshold value in percentage.
- **ipv6-addr** *percentage* : Specifies the IPv6 threshold value in percentage.
- **ipv6-prefix** *percentage* : Specifies the IPv6 prefix threshold value in percentage.

The following is a sample configuration:

```
configure
   ipam
      threshold
         ipv4-addr 80
         ipv6-addr 75
         ipv6-prefix 70
```

Configuring IPAM Source

Use the following configuration to configure the IPAM source.

```
configure
   ipam
      source local
         source external ipam
            host ip_address
            port integer
            vendor type
            commit
```

NOTES:

- **ipam**: Enters the IPAM Configuration mode.
- **source local**: Enters the local datastore as the pool source.
- **source external ipam** : Enters the external IPAM server as the pool source.
- **host** *ip_address* : Specifies the host name of the external IPAM server.
- **port** *integer* : Specifies the port of the external IPAM server.

- **vendor** *type*: Specifies the vendor type of the external IPAM server.

The following is a sample configuration:

```
ipam
 source external ipam
  host 1.1.1.1
  port 10000
  vendor cisco
```

Verifying the IPAM Integration Configuration

This section describes how to verify the IPAM integration in the SMF feature configuration.

Use the **show ipam pool** command to view the summary of current threshold of each pool.

The following is a sample output of the **show ipam pool** command.

```
show ipam pool
=================================================================
PoolName   Ipv4Threshold  Ipv6AddrThreshold  Ipv6PrefixThreshold
=================================================================
  p1               80%            80%              0%
  p2               75%            0%               70%
=================================================================
```

Use the **show ipam pool** *pool_name* command to view more details of a specific pool name.

The following is a sample output of the **show ipam pool** *pool_name* command.

```
show ipam pool p1
-----------------------------------------------------
Ipv4Addr   [Total/Used/Threshold] = 7680 / 7680 / 80%
Ipv6Addr   [Total/Used/Threshold] = 512 / 512 / 80%
Ipv6Prefix [Total/Used/Threshold] = 0 / 0 / 0%
-----------------------------------------------------
```

Use the **show ipam** *pool_name* **ipv4-addr** command to view the IPv4-address ranges for the given pool-name. Based on the configuration, the address ranges are dynamically split. You can also view whether the address range is free or allocated to a Data Plane (User Plane) using this command.

The following is a sample output of the **show ipam** *pool_name* **ipv4-addr** command.

```
show ipam pool p1 ipv4-addr
=========================================
StartAddress     EndAddress    AllocContext
=========================================
  1.1.1.0        1.1.3.255     Upf-100
  1.1.4.0        1.1.7.255     Upf-200
  1.1.8.0        1.1.10.255    Free
  2.2.1.0        2.2.3.255     Upf-100
  2.2.4.0        2.2.7.255     Upf-300
  2.2.8.0        2.2.10.255    Free
  3.3.1.0        3.3.3.255     Free
  3.3.4.0        3.3.7.255     Free
  3.3.8.0        3.3.10.255    Free
=========================================
```

Use the **show ipam pool** *pool_name* **ipv6-perfix** command to view the prefix-ranges for the given pool-name. Based on the configuration, the address ranges are dynamically split. You can also view whether the address range is free or allocated to a Data Plane (User Plane) using this command.

The following is a sample output of the **show ipam pool** *pool_name* **ipv6-perfix** command.

```
show ipam pool p2 ipv6-prefix
==============================================
Prefix                          AllocContext
==============================================
 aaaa:bbbb:ccc0::/64            Upf-100
 aaaa:bbbb:ccc1::/64            Free
 aaaa:bbbb:dd00::/64            Upf-200
==============================================
```

Use the **show ipam dp** command to view the summary of the current threshold for each Data Plane (User Plane).

The following is a sample output of the **show ipam dp** command.

```
show ipam dp
================================================================
DpName     Ipv4Threshold  Ipv6AddrThreshold  Ipv6PrefixThreshold
================================================================
UPF-100           20%             40%               70%
UPF-200           40%             20%               20%
================================================================
```

Use the **show ipam dp** *dataplane_name* command to view more details of a specific Data Plane (User Plane).

The following is a sample output of the **show ipam dp** *dataplane_name* command.

```
show ipam dp UPF-100
-------------------------------------------------------
Ipv4Addr   [Total/Used/Threshold] = 512 / 100 / 20%
Ipv6Addr   [Total/Used/Threshold] = 512 / 200 / 40%
Ipv6Prefix [Total/Used/Threshold] = 512 / 300 / 70%
-------------------------------------------------------
```

Use the **show ipam dp** *dataplane_name* **ipv4-addr** command to view the IPv4-address ranges assigned to a data plane.

The following is a sample output of the **show ipam dp** *dataplane_name* **ipv4-addr** command.

```
show ipam dp UPF-100 ipv4-addr
=====================================================
StartAddress   EndAddress    AllocContext   Route
=====================================================
1.1.1.1        1.1.1.255      Pool-1        1.1.1.0/24
2.2.1.1        2.2.1.255      Pool-2        2.2.1.0/24
=====================================================
```

Use the **show ipam dp** *dataplane_name* **ipv6-addr** command to view the IPv6-address ranges assigned to a data plane.

The following is a sample output of the **show ipam dp** *dataplane_name* **ipv6-addr** command.

```
show ipam dp UPF-100 ipv6-addr
=======================================================
```

```
StartAddress     EndAddress    AllocContext   Route
=========================================================
100::1           100::100         Pool-1      100::/120
00::1            200::100         Pool-2      200::/120
=========================================================
```

Use the **show ipam dp** *dataplane_name* **ipv6-prefix** command to view the IPv6-address ranges assigned to a data plane.

The following is a sample output of the **show ipam dp** *dataplane_name* **ipv6-prefix** command.

```
show ipam dp UPF-100 ipv6-prefix
=============================================================
Prefix                AllocContext      Route
=============================================================
aaaa:bbbb:cccc::/64   Pool-1            aaaa:bbbb:cccc::/48
aaaa:bbbb:dd00::/64   Pool-1            aaaa:bbbb:dd00::/40
=============================================================
```

Static IP Support

Feature Description

IPAM is the core component of the subscriber management system. Traditional IPAM functionalities prove insufficient in the Cloud Native network deployments. Hence, IPAM requires additional functionalities to work with the Cloud Native subscriber management system.

The Static IP Support feature enables the support of static IP on the SMF using IPAM. This feature supports the following functionalities:

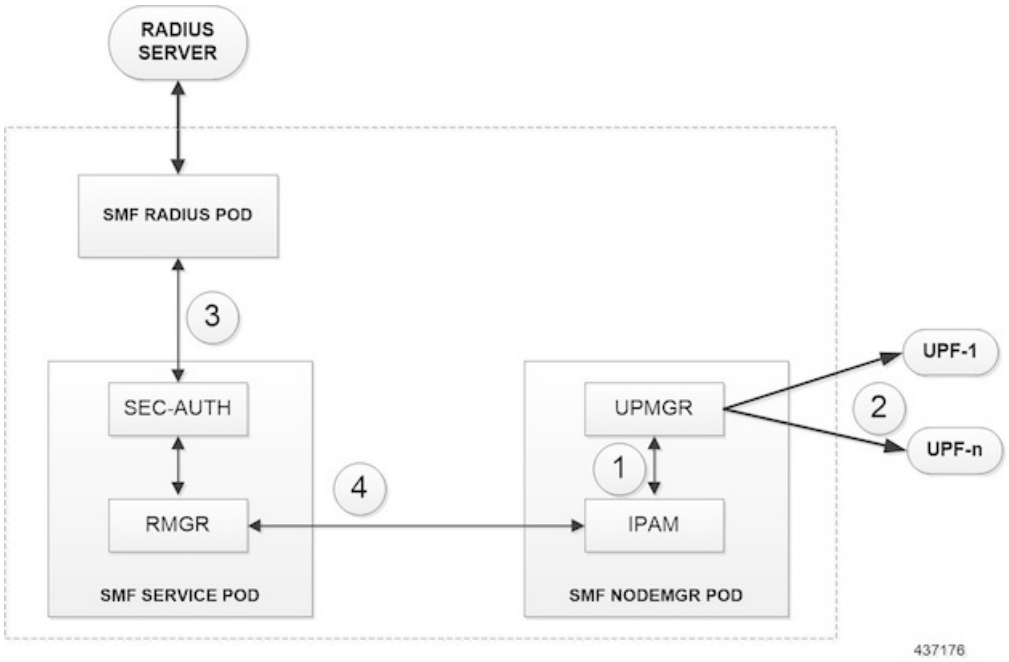
- Supports static pool configuration.
- Splits static address-ranges into smaller chunks and associates them with the configured UPFs.
- Enables program routes according to static address-range reservation during UPF association.
- Enables secondary authentication under the DNN profile.
- Selects UPF based on reserved address-range and Framed-IP received from the Authentication response.

How it Works

This section provides a brief of how the Static IP Support feature feature works.

The SMF receives a framed-IP address of the subscriber from external AAA servers such as RADIUS. While IPAM is not involved in individual IP address management in this scenario, it still handles the route management and UPF management for static address-ranges.

IPAM splits the ‘static’ address-ranges equally according to number of UPFs present in the SMF configuration. Unlike dynamic IP, IPAM splits all static-IP address-ranges and assigns them for all configured UPFs. IPAM involves and selects an UPF when the external AAA server returns the framed-IP of the subscriber. IPAM looks for the route which includes this static-IP and then selects the UPF where the route is already configured.



Procedure

1. IPAM splits the static ranges into equal number of address-ranges based on number of configured UPFs.
2. The UPMGR programs the corresponding static routes on the associated UPFs.
3. Subscribers get static IP from Radius server authorize response.
4. SMF service selects the right UPF based on ADDR ranges and UPF map allocation from the Node Manager.

Address-Range Split

Splitting a given address-range into smaller address-ranges is a key functionality of the IPAM server and IPAM cache. The following guidelines determine address-range split:

1. Size of a split address-range depends upon the ‘configured’ value or the ‘default’ value as per the AFI type.
2. Size of a split address-range must be a ‘power-of-2’ or at least to the closest of it. That is, it should be able to represent the split range in “subnet/mask” notation such that a route can be added in the Data Plane (User Plane) if required.
3. ‘Configured’ or ‘default’ address-range-size must be at the ‘power-of-2’.

The address-range must be split into smaller ranges immediately on configuration or initial start-up. This helps in better sorting of address-ranges based on size and faster allocation during actual address-range-allocation requests. The address-range exchange between modules is always in the mentioned size.

Table 90: Examples of IPv4 Address-Range Split

Address-Range	Split-Size (number of addresses per range)	Split-ranges (* Odd sized ranges)	Route Notation
1.1.1.0 - 1.1.1.255	128	[1] 1.1.1.0 – 1.1.1.127 [2] 1.1.1.128 – 1.1.1.255	[1] 1.1.1.0/25 [2] 1.1.1.128/25
1.1.0.0 – 1.1.10.255	256	[1] 1.1.0.0 – 1.1.0.255 [2] 1.1.1.0 – 1.1.1.255 [3] 1.1.2.0 – 1.1.2.255 ... [n] 1.1.10.0 – 1.1.10.255	[1] 1.1.0.0/24 [2] 1.1.1.0/24 [3] 1.1.2.0/24 ... [n] 1.1.10.0/24
1.1.0.5 – 1.1.2.200	256	[1] 1.1.0.5 – 1.1.0.255 * [2] 1.1.1.0 – 1.1.1.255 [3] 1.1.2.0 – 1.1.2.200 *	[1] 1.1.0.0/24 [2] 1.1.1.0/24 [3] 1.1.2.0/24

Table 91: Examples of IPv6 Address-Range Split

Address-Range	Split-Size (number of addresses per range)	Split-ranges (* Odd sized ranges)	Route Notation
1:: - 1::1000	1024	[1] 1:: – 1::3FF [2] 1::400 – 1::7FF [3] 1::800 – 1::BFF [4] 1::C00 – 1::FFF	[1] 1::/118 [2] 1::400/118 [3] 1::800/118 [4] 1::C00/118
1::3 - 1::1DEF	1024	[1] 1::3 – 1::3FF * [2] 1::400 – 1::7FF [3] 1::800 – 1::BFF … [n] 1::1C00 – 1::1DEF *	[1] 1::/118 [2] 1::400/118 [3] 1::800/118 … [n] 1::1C00/118

Examples of IPv6 Address-Range Split

Prefix split needs two length fields for performing the split.

- Network length
- Host length

Prefixes are split between these and a new route is calculated.

Example 1: network-length = 48, prefix-length = 64

Total (64-48) = 16 bits (that is, 65536 prefixes are available for the split)

Example 2: network-length = 32, prefix-length = 56

Total (56-32) = 24 bits (that is, 16 million prefixes available for the split)

Note For Cloud-Native 5G SMF, the host-length is hard-coded as '64'. Only network-length can be configured via the CLI.

Table 92: Examples of IPv6 Address-Range Split

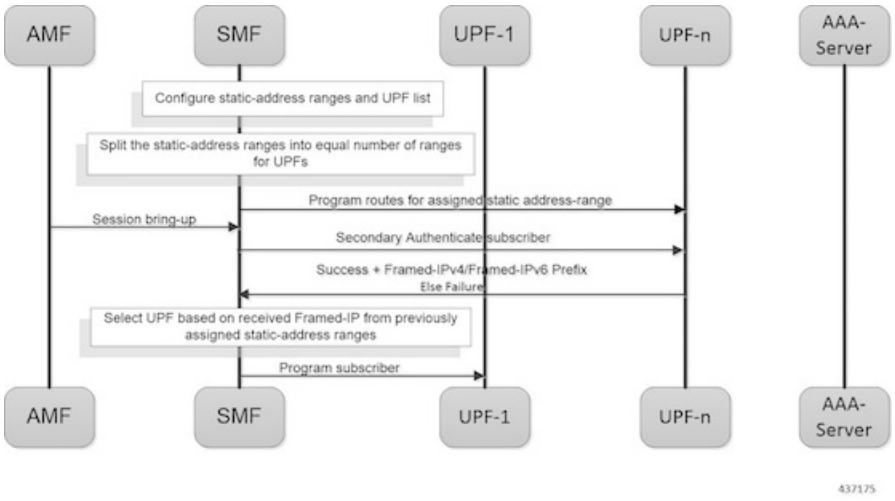
Prefix-Range	Split-Size (number of addresses per range)	Split-ranges (* Odd sized ranges)	Route Notation
1:2:3:: Nw-len = 48 Host-len = 64	8192	[1]1:2:3:: ... 1:2:3:1fff [2]1:2:3:2000:: ... 1:2:3:2fff:: [3]1:2:3:3000:: ... 1:2:3:3fff:: ...	[1]1:2:3::/51 [2]1:2:3:2000/51 [3]1:2:3:3000/51 ...

Call Flows

This section includes the following call flow.

Figure 77: SMF Static IP Call Flow

Figure 78:



Step	Description
1	Configures the static-address ranges and UPF list.
2	Splits the static-address ranges into equal number of ranges for UPFs.

Step	Description
3	Enables program routes for the assigned static address-range.
4	Brings up the session.
5	Enables secondary authentication under the DNN profile.
6	The SMF sends the Authentication Request to the RADIUS server. The RADIUS server sends an Authentication Response with the 'static-ip' of the subscriber. The SMF selects the UPF based on the 'static-ip' and continues with the programming.
7	Completes the subscriber programming.

Limitations

The Static IP Support feature has the following limitations:

- Change of a pool from dynamic to static and vice-versa is not supported when in system-running mode.
- Addition or removal of UPF is not supported when in system-running mode.
- The address-range split must be optimal based on the number of UPFs and number of addresses in the ranges.

  For example:

  - If there are 2 UPFs and 1024 addresses specified in the range, then specify the per-dp-split-size as 512.
  - If there are 3 UPFs and 1024 addresses, then specify the per-dp-split-size as 256.

Configuring Static IP Support

Use the following commands to configure the Static IP Support feature.

```
configure
  ipam
    address-pool pool_name
      static
      end
```

NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool_name*: Specifies the name of the address pool to enter the pool configuration. *pool_name* must be the name of the address pool.
- **static**: Enables the static IP mode.

Dual-Stack Static IP Support Through IPAM

Feature Description

The SMF supports dual-stack static IP using IPAM. For dual-stack sessions, the AAA server sends both the IPv4 and IPv6 address prefixes as part of the Access-Accept message. In the SMF-IPAM configuration, both the IPv4 and IPv6 address prefixes are added in the same pool. The IPAM assigns both the IPv4 and IPv6 routes to a single UPF.

During the UPF selection, the Node Manager application uses the UPF for both the IPv4 and IPv6 addresses from the IPAM to handle them accordingly.

How it Works

The SMF supports dual-stack static IP through IPAM in the following ways:

- Pool to UPF mapping—Based on the number of UPFs available, the IPv4 address-ranges and IPv6 prefix-ranges are split into smaller chunks. Then, the pair (chunk) is configured into the same IPAM pool.

  IPAM assigns all the addresses and prefixes that are configured in one dual-stack pool to a UPF in the manner they are received. The AAA server returns the dual-stack addresses from the same pair. From these addresses, SMF selects one UPF for dual-stack programming.

  The load-balancing of number of addresses and prefixes are managed. IPAM performs only the dual-stack static-pool to UPF mapping.

- Address-range no-split configuration—IPAM uses the "no-split" configuration to prevent splitting the address-ranges into smaller chunks. This configuration helps to prevent having multiple routes programming for a specific range.

  The following table lists the errors or exceptions and how to handle them:

Table 93: Error and Exception Handling

Error or Exception	Exception Handling
IPv4 UPF and IPv6 UPF are configured incorrectly	**1.** Select an active UPF. In case both the UPFs are active, select the UPF with the IPv4 address. **2.** Reset the IP information of the other stack and update the PDU session type accordingly.
IPv4 address is invalid or null	Select the UPF with IPv4 address and update the PDU session type accordingly.
IPv6 prefix is invalid or null	Select the UPF with IPv6 address and update the PDU session-type accordingly.
IPv4 address and IPv6 prefix are invalid	Both the IPv4 address and IPv6 prefix are rejected.

Limitations

The dual-stack static IP support using IPAM feature has the following limitation:

When the system is in running mode, the change in ‘no-split' configuration is not supported.

Configuring Dual-Stack Static IP Support Using IPAM Feature

This section describes how to configure the dual-stack static IP support using IPAM.

Configuring IPAM No-Split

This section describes how to configure the IPAM no-split.

```
configure
   ipam
      address-pool pool_name
      ipv4
         split-size no-split
         exit
      ipv6 prefix_ranges
         split-size no-split
         exit
      exit
```

NOTES:

- **split-size no-split**—Prevents the IPv4 address-ranges or IPv6 prefix-ranges from splitting into smaller chunks.

IPAM Offline Mode Support

Feature Description

The SMF supports the addition of a dynamic pool, IPv4, or IPv6 address-range to a dynamic pool by default. The new chunks are added to the respective tags, such as DNN, and are assigned from the same pool.

To delete a dynamic pool or an IPv4 or IPv6 address-range from a dynamic pool:

1. Configure the pool or address-range as offline. The IPAM then stops assigning addresses from the respective pool or address-range.
2. Use the following **clear-subscriber** CLI commands to delete the subscribers based on respective pool or address range that are configured to offline mode:
   - **clear subscriber ipv4-pool** *pool_name*
   - **clear subscriber ipv4-range** *pool_name/start_of_range*
   - **clear subscriber ipv6-pool** *pool_name*
   - **clear subscriber ipv6-range** *pool_name/start_of_range*

3. Use the following **cdl show-sub** CLI commands and wait until all the subscribers are deleted:
   - **cdl show sessions count summary filter { key ipv4-pool:** *pool_name* **condition match }**
   - **cdl show sessions count summary filter { key ipv4-range:** *pool_name/start_of_range* **condition match }**
   - **cdl show sessions count summary filter { key ipv6-pool:** *pool_name* **condition match }**
   - **cdl show sessions count summary filter { key ipv6-range:** *pool_name/start_of_range* **condition match }**
4. After all the subscribers are deleted, delete the pool or address-range from the IPAM configuration.

Configuring the IPAM Offline Mode

This section describes how to configure the IPAM offline feature for pool, IPv4 address-range, and IPv6 prefix-ranges.

Configuring Pool to Offline Mode

Use the following command to configure the entire pool to offline mode.

```
configure
   ipam
      address-pool pool_name
         offline
         ...
         exit
      exit
```

NOTES:

- **address-pool** *pool_name*—Specifies the name of the pool to enter the pool configuration. *pool_name* must be the name of the address pool.
- **offline**—Configures the pool to offline mode.

Configuring IPv4 Address-Range to Offline Mode

Use the following command to configure the IPv4 address-range to offline mode.

```
configure
   ipam
      address-pool pool_name
      vrf-name vrf_name_value
         ip4
            address-range start_ipv4_address end_ipv4_address offline
            address-range start_ipv4_address end_ipv4_address
         !
       !
     !
```

NOTES:

- **address-pool** *pool_name*—Specifies the name of the pool to enter the pool configuration. *pool_name* must be the name of the address pool.
- **ipv4**—Enters the IPv4 mode.
- **address-range** *start_ipv4_address end_ipv4_address*—Specifies the IP addresses for the start and end IPv4 address-range.
- **offline**—Configures the selected address-range to offline mode.

Configuring IPv6 Prefix-Ranges to Offline Mode

Use the following commands to configure IPv6 prefix-range to offline mode.

```
configure
   ipam
      address-pool pool_name
      vrf-name vrf_name_value
        ipv6
               prefix-ranges
                prefix-rangeprefix_value length length_valueoffline
                   prefix-rangeprefix_value length length_value
              !
           !
        !
   !
```

NOTES:

- **address-pool** *pool_name*—Specifies the name of the pool to enter the pool configuration. *pool_name* must be the name of the address pool.
- **ipv6**—Enters the IPv6 mode.
- **prefix-ranges**—Enters the prefix-ranges mode.
- **prefix-range** *prefix_value* **length** *length_value*—Specifies the prefix-range and prefix-length of the IPv6 prefix-range.
- **offline**—Configures the selected address-range to offline mode.

IPAM Redundancy Support Per UPF

Feature Description

The SMF supports IPAM redundancy and load-balancing for each UPF. The IPAM running in the Node Manager microservice has two IPAM instances that are associated to each UPF. When one IPAM instance is inactive, the other IPAM instance manages the address allocation requests for the UPF.

The IPAM redundancy support per UPF feature supports the following functionality:

How it Works

This section provides a brief of how the IPAM redundancy support per UPF feature works.

- Peer Selection—The Node Manager peer is selected during the UPF association.
- UPF Registration with Peer IPAM—IPAM is notified with the instance ID of the peer for the UPF during the registration of the UPF call. IPAM allocates routers from the local data for the specific DNN and checks if the peer IPAM instance is in active or inactive state.

  If the peer IPAM instance is active, a REST call is sent to it to register to the same UPF in the local instance and to receive the routes as response.

  If the peer IPAM instance is inactive, the local instance takes over the IPAM context of the remote instance. Then, the local instance registers to the UPF, receives the routes, and keeps the data back in the cache-pod. After the peer instance is active, it restores the same data from the cache-pod.

  Routes from both the instances are sent to UPF for load-balanced address allocations from both the instances.
- Address Allocation in Load-Balanced Model—As one UPF is registered to two IPAM servers, SMF sends the address allocation requests to any peer that is load-balanced. Respective IPAM instances assign new addresses from their local address bitmap. If one peer instance is inactive, the other peer instance handles all the requests.
- Address-Release Request Handling—In IPAM, the Address Release request is sent to the instance that had allocated the IP the first time. If that peer is inactive, the Address Release request is sent to the peer IPAM.

  The IPAM instance that receives the address releases for remote instances, keeps buffering these instances locally and updates the cache-pod periodically. After the remote peers are active, they handle the buffered address-release requests.
- Release of the UPF—When a peer IPAM is active during the release of a UPF, a REST call is sent to clear the data. If the peer IPAM is inactive, the existing IPAM instance takes over the operational data of the remote IPAM, clears the UPF information, and updates the cache-pod.

IPAM Quarantine Timer Support

Feature Description

The IPAM Quarantine Timer Support feature supports the IPAM quarantine timer for the IP pool address. This feature keeps the released IP address busy until the quarantine timer expires to prevent the reuse of that IP address. Each IP pool must be configured with a timer value. This value determines the duration of a recently released address to be in the quarantine state before it is available for allocation. After the timer expires, the IP address is available in the list of free addresses for allocation by the subscriber. A released IP address with no address quarantine timer is considered to be in use for allocation. If a subscriber attempts to reconnect when the address quarantine timer is armed even if it is the same subscriber ID, the subscriber does not receive the same IP address.

Configuring the IPAM Quarantine Timer Support Feature

This section describes how to configure the IPAM quarantine timer support feature.

Configuring IPAM Quarantine Timer

This section describes how to configure the IPAM quarantine timer.

```
configure
   ipam
      address-pool pool_name
         address-quarantine-timer quarantine_timer_value
         vrf-name vrf_name_value
         ip4
            address-range start_ipv4_address end_ipv4_address
            address-range start_ipv4_address end_ipv4_address
         !
       !
     !
```

NOTES:

- **ipam**—Enter the IPAM configuration.
- **address-pool** *pool_name*—Specifies the name of the pool to enter the pool configuration. *pool_name* must be the name of the address pool.
- **address-quarantine-timer** *quarantine_timer_value*—Specifies the value of the quarantine timer in seconds. The default value is 4.
- **vrf-name** *vrf_name_value*—Specifies the name of the VPN routing and forwarding (VRF) for the pool.
- **ipv4**—Enters the IPv4 mode.
- **address-range** *start_ipv4_address end_ipv4_address*—Specifies the IP addresses for start and end IPv4 address-range.

show ipam pool

Field	Description
PoolName	Name of the Address Pool.
Ipv4Utilization	Utilization percentage for IPv4 address for this pool.
Ipv6AddrUtilization	Utilization percentage for IPv6 address for this pool.
Ipv6PrefixUtilization	Utilization percentage for IPv6 prefix address for this pool.

show ipam pool <pool-name>

Field	Description
Ipv4Addr [Total/Used/Utilization]	Total IPv4 address available(configured for this pool) / Number of used address / Utilization percentage for IPv4 address.
Ipv6Addr [Total/Used/Utilization]	Total IPv6 address available(configured for this pool) / Number of used address / Utilization percentage for IPv6 address.
Ipv6Prefix [Total/Used/Utilization]	Total IPv6 prefix address available(configured for this pool) / Number of used address / Utilization percentage for IPv6 prefix

show ipam pool <pool-name> ipv4-addr

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane to which this address range is allocated.
Flag	Flag Indicate weather pool is Static or if it is offline.

show ipam pool <pool-name> ipv6-addr

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane to which this address range is allocated.
Flag	Flag Indicate weather pool is Static or if it is offline.

show ipam pool <pool-name> ipv6-prefix

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.

Field	Description
AllocContext	Name of data plane this address range is allocated.
Flag	Flag Indicates whether pool is Static or if it is offline, S(Static) and O(Offline).

show ipam dp

Field	Description
DpName	Name of the data plane which is registered.
Ipv4Utilization	Utilization percentage for IPv4 by this data plane.
Ipv6AddrUtilization	Utilization percentage for Ipv6 address by this data plane.
Ipv6PrefixUtilization	Utilization percentage for Ipv6 prefix by this data plane.

show ipam dp <dataplane-name>

Field	Description
Ipv4Addr [Total/Used/Utilization]	Total IPv4 address available(configured for this data plane) / Number of used address / Utilization percentage for IPv4.
Ipv6Addr [Total/Used/Utilization]	Total IPv6 address available(configured for this data plane) / Number of used address / Utilization percentage for IPv6.
Ipv6Prefix [Total/Used/Utilization]	Total IPv6 prefix address available(configured for this data plane) / Number of used address / Utilization percentage for IPv6 prefix.

show ipam dp <dataplane-name> ipv4-address

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
Route	Route allocated for this data plane.

Field	Description
N/P	Display the NodeMgr instance IDs from which it received routes Flag Indication S(Static) and O(Offline).

show ipam dp <dataplane-name> ipv6-addr

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of pool to which this address range belongs.
Route	Route allocated for this data plane.
N/P	Display the NodeMgr instance IDs from which it received routes.
Flag	Flag Indicate whether pool is Static or if it is offline, Flag Indication S(Static) and O(Offline).

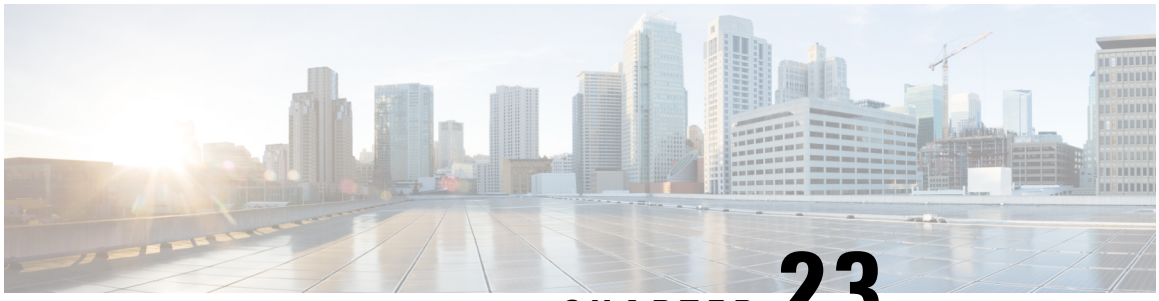
show ipam dp <dataplane-name> ipv6-prefix

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of pool to which this address range belongs.
Route	Route that is allocated for this data plane.
N/P	Displays the NodeMgr instance IDs from which it received routes Indication, N(Native InstId) and P(Peer InstId).
Flag	Flag Indicate weather pool is Static or if it offline Flag Indication, S(Static) and O(Offline).

show ipam

Field	Description
PoolName	Displays Ipv4Utilization, Ipv6AddrUtilization, and Ipv6PrefixUtilization.

Field	Description
DpName	Displays Ipv4Utilization, Ipv6AddrUtlization, and Ipv6PrefixUtlization.



CHAPTER 23

Load-based Selection of UPF

Feature Summary and Revision History

Summary Data

Table 94: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 95: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

Load based User Plane Function (UPF) selection in SMF distributes calls among active UPFs associated with SMF.

SMF Support for Load Control Feature

3GPP specifies Load Control feature as optional feature over N4 reference points. This enables UPF to send its load information to CP functions. To support Load Control feature, SMF can receive UPF provided Load Control information in the following PFCP messages:

- Session Establishment Response
- Session Modification Response
- Session Deletion Response
- Session Report Request

Load Control procedure details are mentioned in 3GPP TS 29.244 v14.0.0 Release 14 Section 6.2.3 and SMF adheres to the CP functionality.

Load Based UPF Selection

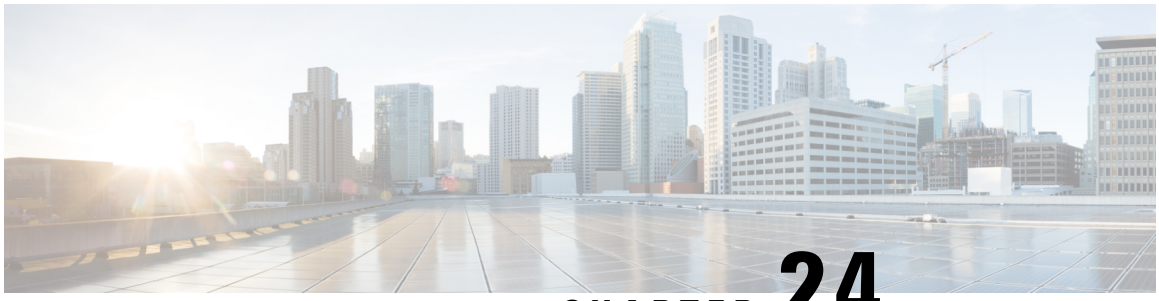
SMF stores the load information provided by UPF and uses it in selecting the UPF for new sessions being established. SMF selects the less loaded UPF among the candidate (DNN based) active UPFs.

This feature considers priority and capacity configured statically against each UPF. In cases where UPF does not send the load information statically, configured capacity is considered while selecting the UPFs.

Standards Compliance

The feature complies with the following standards:

- 3GPP TS 29.244 v14.0.0 Release 14



CHAPTER 24

Monitor Subscriber and Monitor Protocol

Feature Summary and Revision History

Summary Data

Table 96: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 97: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the Monitor Subscriber and Monitor Protocol on the Kubernetes environment. This feature allows to capture messages of subscribers and protocols.

Configuring the Monitor Subscriber and Monitor Protocol Feature

Monitoring the Subscriber

Use the following CLI command to monitor the subscriber in the SMF.

monitor subscriber supi *supi_id* **[capture-duration** *duration_sec* **| internal-messages { yes } | transaction-logs { yes }]**

NOTES:

- **supi** *supi_id*: Specifies the subscriber identifier. For example, imsi-123456789, imsi-123*
- **capture-duration** *duration_sec*: Specifies the duration in seconds during which the monitor subscriber is enabled. The default is 300 seconds (5 minutes).
- **internal-messages { yes }**: Enables internal messages. By default, internal messages are disabled.
- **transaction-logs { yes }**: Enables transaction logs. By default, transaction logs are disabled.

The **monitor subscriber** CLI command can be run simultaneously on multiple terminals. For example, run the CLI simultaneously in two SMF Ops Center terminals for two subscribers (for example, imsi-123456789012345 and imsi-456780123456789) to implement the following:

- Monitor the duration when the monitor subscriber is enabled.
- View internal messages for the specified subscriber.
- View transaction logs for the specified subscriber

Terminal 1: The following command monitors and displays subscriber messages for the specified subscriber.

```
monitor subscriber supi imsi-123456789012345 capture-duration 1000 internal-messages yes
```

Terminal 2: The following command monitors and displays transaction logs for the specified subscriber.

```
monitor subscriber supi imsi-456780123456789 capture-duration 500 internal-messages yes
transaction-logs yes
```

After the capture-duration is over or to stop the CLI, use the **Ctrl+C** keys. The captured messages are reordered and stored in a file. To retrieve the list of stored files, use the **monitor subscriber list** CLI command.

For example:

```
monitor subscriber list
RELEASE_NAMESPACE: 'smf'
'monsublogs/subscriberID_imsi-*_AT_2019-10-22T09:19:05.586237087.txt.sorted'
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

Viewing the Sorted File on SMF Ops Center

Use the following CLI command to view the sorted file on the SMF Ops Center screen.

monitor subscriber dump filename *filename*

For example:

```
monitor subscriber dump filename
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

Monitoring the Interface Protocol

Use the following CLI command to monitor the interface protocol on the SMF.

monitor protocol interface *endpoint_name* **capture-duration** *duration_sec*

NOTES:

- **interface** *endpoint_name*: Specifies the endpoint name on which PCAP is captured. This CLI allows the configuration of multiple endpoint names in a single CLI command.
- **capture-duration** *duration_sec*: Specifies the duration in seconds during which the monitor subscriber is enabled. The default is 300 seconds (5 minutes).
- The configured endpoint names can be retrieved using the **show endpoint** CLI command.

The **monitor protocol** CLI can be run simultaneously on multiple terminals. Also, the **interface** *endpoint_name* CLI allows the configuration of multiple endpoint names in a single CLI command. For example:

monitor protocol interface sbi,N4:10.86.73.161:8805,gtpc capture-duration 1000

Viewing Transaction History Logs

Use the following CLI command to view the transaction history on an OAM pod shell. On another terminal, use the **kubectl** command to tail the logs of the OAM pod and then run the following CLI from the Ops Center.

dump transactionhistory

NOTES:

In this release, the most recent transaction logs are stored in a circular queue of size 1024 transaction logs.

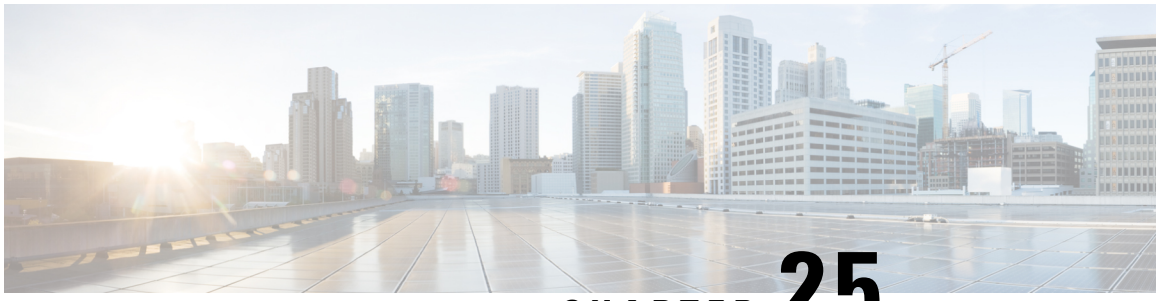
Sample Transaction Log

The following is a sample transaction log.

```
InstanceInfo: SMF.smf-service.DC.Local.0
TimeStamp: 2019-11-13 03:01:33.614095848 +0000 UTC
************* TRANSACTION: 00091 *************
TRANSACTION SUCCESS:
    Txn Type             : 24
    Priority             : 1
    Session State        : Update_Session
    Subscriber Id        : imsi-123456789012345
    Session Keys         : imsi-123456789012345:5 (primary)
LOG MESSAGES:
    2019/11/13 03:01:33.565 [INFO] [infra.application.core] Queue data 91
    2019/11/13 03:01:33.565 [DEBUG] [infra.transaction.core] Processing transaction Id: 91
 Type: 24 SubscriberID:  Keys: []
    2019/11/13 03:01:33.565 [TRACE] [infra.message_log.core] >>>>>>>
IPC message
Name: N11SmContextReleaseReq
```

```
MessageType: N11SmContextReleaseReq
Key:
--body--
{"smcontextreleasedata":{"cause":7}}
    2019/11/13 03:01:33.566 [DEBUG] [infra.transaction.core] Trying to load session
    2019/11/13 03:01:33.566 [DEBUG] [infra.session_cache.core] Get session by pk
imsi-123456789012345:5
    2019/11/13 03:01:33.566 [DEBUG] [infra.session_cache.core] Record found in local cache
 by key imsi-123456789012345:5
    2019/11/13 03:01:33.566 [DEBUG] [infra.transaction.core] Queuing new transaction for
processing
    2019/11/13 03:01:33.566 [DEBUG] [smf-service0.smf-app.messageprocessor] GetLockPriority
 for txn id: 91, Type: 24
    2019/11/13 03:01:33.566 [DEBUG] [infra.transaction.core] Session lock priority 0 txn
lock priority 10
    2019/11/13 03:01:33.567 [DEBUG] [infra.transaction.core] Session locked with priority
10
    2019/11/13 03:01:33.567 [DEBUG] [smf-service0.smf-app.gen] Handle Idle Events
    2019/11/13 03:01:33.567 [DEBUG] [smf-service0.smf-app.amf] Handling SM Context Release
 Event
    2019/11/13 03:01:33.567 [DEBUG] [smf-service0.smf-app.upf] Send N4 Release Request
    2019/11/13 03:01:33.567 [DEBUG] [infra.transaction.core] Requested host Setname:
smf-protocol Name:  Version:  ApiRoot:
    2019/11/13 03:01:33.567 [DEBUG] [infra.transaction.core] Selected remote host by set
name is Id 5 Name: smf-protocol4 Setname: smf-protocol Host: smf-protocol Port: 9003 Url:
 of available 10 hosts
    2019/11/13 03:01:33.567 [INFO] [infra.transaction.core] Calling RPC smf-protocol on
host smf-protocol4 proc-name smf-protocol proc-method: Sync
    2019/11/13 03:01:33.567 [DEBUG] [infra.ipc_action.core] Calling IPC RPC with Retry,
Retry Counter is 3
    2019/11/13 03:01:33.597 [DEBUG] [infra.ipc_action.core] Time taken to execute IPC is
0.03
    2019/11/13 03:01:33.597 [DEBUG] [infra.ipc_action.core] Destination Host 192.168.1.163
 serviced the IPC Message N4SessionReleaseReq
    2019/11/13 03:01:33.597 [DEBUG] [smf-service0.smf-app.upf] UPF N4 Session Release done
    2019/11/13 03:01:33.597 [DEBUG] [smf-service0.smf-app.messageprocessor] Returning
newStage (RELEASE: Idle)
    2019/11/13 03:01:33.597 [DEBUG] [infra.transaction.core] Last stage ( init_done ) ->
Next stage ( RELEASE: Idle )
    2019/11/13 03:01:33.598 [DEBUG] [smf-service0.smf-app.upf] Processing N4 Response
awtUpfRelProcUpfReleaseResp
    2019/11/13 03:01:33.599 [DEBUG] [infra.transaction.core] Requested host Setname:  Name:
 192.168.2.150 Version:  ApiRoot:
    2019/11/13 03:01:33.599 [DEBUG] [infra.transaction.core] Exact match found. Selected
remote host is Id 11 Name: 192.168.2.150 Setname:  Host: 192.168.2.150 Port: 9003 Url:
    2019/11/13 03:01:33.599 [INFO] [infra.transaction.core] Calling RPC smf-nodemgr on host
 192.168.2.150 proc-name smf-nodemgr proc-method: Sync
    2019/11/13 03:01:33.600 [DEBUG] [infra.ipc_action.core] Calling IPC RPC with Retry,
Retry Counter is 3
    2019/11/13 03:01:33.609 [DEBUG] [infra.ipc_action.core] Time taken to execute IPC is
0.01
    2019/11/13 03:01:33.609 [DEBUG] [infra.ipc_action.core] Destination Host 192.168.2.150
 serviced the IPC Message NmgrRersourceMgmtRequest
    2019/11/13 03:01:33.609 [DEBUG] [smf-service0.smf-app.resource] NodeMgr Resource(IP and
 commonID) Release Sent
    2019/11/13 03:01:33.609 [DEBUG] [smf-service0.smf-app.messageprocessor] Returning
newStage (RELEASE: Await UPF Release)
    2019/11/13 03:01:33.609 [DEBUG] [infra.transaction.core] Last stage ( RELEASE: Idle )
-> Next stage ( RELEASE: Await UPF Release )
    2019/11/13 03:01:33.609 [DEBUG] [smf-service0.smf-app.resource] Processing Rmgr Response
 awtRmgrRelProcNmgrResourceMgmtRsp
    2019/11/13 03:01:33.609 [DEBUG] [smf-service0.smf-app.resource] NodeMgr Resource(IP and
 commonID) Release done
    2019/11/13 03:01:33.610 [DEBUG] [smf-service0.smf-app.amf] Sending Sm context Release
```

```
Response
    2019/11/13 03:01:33.610 [DEBUG] [smf-service0.smf-app.messageprocessor] Returning
newStage (RELEASE: Await Resource Release)
    2019/11/13 03:01:33.610 [DEBUG] [infra.transaction.core] Last stage ( RELEASE: Await
UPF Release ) -> Next stage ( RELEASE: Await Resource Release )
    2019/11/13 03:01:33.610 [DEBUG] [smf-service0.smf-app.messageprocessor] Returning
newStage (finished)
    2019/11/13 03:01:33.610 [DEBUG] [infra.transaction.core] Last stage ( RELEASE: Await
Resource Release ) -> Next stage ( finished )
    2019/11/13 03:01:33.610 [DEBUG] [infra.transaction.core] Updating session
    2019/11/13 03:01:33.610 [DEBUG] [infra.session_cache.core] Save session with key
imsi-123456789012345:5 in cache
    2019/11/13 03:01:33.612 [DEBUG] [infra.session_cache.core] Queued datastore write for
key imsi-123456789012345:5
    2019/11/13 03:01:33.613 [TRACE] [infra.message_log.core] <<<<<<<<
    2019/11/13 03:01:33.613 [DEBUG] [infra.transaction.core] sent response message for 91
```



CHAPTER 25

Multiple and Virtual DNN Support

Feature Summary and Revision History

Summary Data

Table 98: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 99: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

Multi DNN support enables the SMF to have multiple PDN connections for end users to provide different services including Internet and VONR services.

The SMF fetches locally configured DNN profile-based DNN in PDU Session Establishment Request from the AMF and maintains the PDN connections based on using SUPI and pdu-session-id. SMF includes the received DNN in all SBI interfaces to authorize the end user to fetch subscription information, policy and charging related information and provisions forward path information to the UPF. The SMF integrates Multi-DNN Support with IPAM (IP Address Management) Module to allocate address to end-user based on received DNN, which maps the DNN-Profile that is derived from subscriber policies. The SMF also fetches DNN and IPv4 and IPv6 path information based on IPAM pool configuration and updates the UPF as a part of node association interactions.

Note Multiple DNN is supported only for 5GS procedures and is not qualified for EPS Session using SBI interfaces.

The SMF supports Virtual DNN mapping based on a subscriber profile. It supports mapping of a UE requested DNN to a configured DNN and sends the selected DNN profile towards the configured network interfaces.

How it Works

The DNN profile lookup is based on subscriber policy or DNN policy. They are associated in the SMF profile configuration. The subscriber policy has a higher precedence over the DNN policy when both the configurations are present.

The subscriber policy consists of a list of precedence values, and the selection of the precedence is based on the subscriber's SUPI, GPSI, Serving PLMN, and NSSAI value. Each precedence has an associated operator policy and the DNN policy is picked from the selected operator-policy.

The DNN policy can have a DNN profile configuration for each UE-requested DNN. The DNN profile has a Virtual or Mapped DNN with its list of interfaces.

The order of selection for a Virtual DNN is as follows:

- Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE requested DNN) > Virtual DNN mapping.
- Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE requested DNN) > Virtual DNN mapping.

PCF, CHF, UDM, UPF, and RMGR are the supported interfaces for Virtual DNN mapping.

If the Virtual DNN mapping is not configured, the UE-requested DNN is used across all the interfaces.

Limitations

The SMF includes first-configured DNN profile in "dnnSmfInfoList" of NFProfile during registration with NRF.

Configuring the Virtual DNN Feature

This section describes how to configure the Virtual DNN feature.

Configuring the Virtual DNN feature involves the following steps:

1. Configuring subscriber policy
2. Configuring operator policy and associating a DNN policy
3. Configuring DNN policy
4. Configuring virtual DNN under DNN profile
5. Associating subscriber policy and DNN policy under SMF profile

Configuring Subscriber Policy

To configure the subscriber policy use the following configuration:

```
configure
   policy subscriber policy_name
      precedence precedence_value operator-policy policy_name
      end
```

NOTES:

- **operator-policy** *policy_name*: Specifies the operator policy to be associated with the subscriber policy.

show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy_name*

Configuring Operator Policy and Associating a DNN Policy

To configure the operator policy, use the following configuration:

```
configure
   policy operator policy_name
      policy dnn policy_name
      end
```

NOTES:

- **policy dnn** *policy_name*: Specifies the DNN policy to be associated with the operator policy.

Verifying the Configuration

This section describes how to verify the above configuration.

show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy_name*

Configuring a DNN Policy

To configure the DNN policy, use the following configuration:

```
configure
   policy dnn policy_name
      dnn profile_name profile profile_name
      profile profile_name
      end
```

NOTES:

- **dnn** *profile_name*: Maps the specified Virtual DNN profile with the specified network DNN profile. *profile_name* must be an alphanumeric string.
- **profile** *profile_name*: Specifies the network DNN profile. *profile_name* must be an alphanumeric string.

Verifying the Configuration

This section describes how to verify the above configuration.

show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy_name*

Configuring a Virtual DNN under a DNN Profile

To configure a virtual DNN under a DNN profile, use the following configuration:

```
configure
   profile dnn profile_name
      dnn profile_name network-function-list [ chf | pcf | upf ]
 profile profile_name
      end
```

NOTES:

- **dnn** *profile_name*: Specifies the DNN profile name. *profile_name* must be an alphanumeric string.
- **network-function-list**: Specifies the network functions that the selected DNN profile will be sent. Supported values are **chf**, **pcf**, and **upf**.

Verifying the Configuration

This section describes how to verify the above configuration.

show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy_name*

Associating Subscriber Policy under the SMF Service

To associate a subscriber policy under SMF service, use the following configuration:

```
configure
  profile smf smf_profile_name
     service name nsmf-pdu
        subscriber-policy subscriber_policy_name
        end
```

NOTES:

- **subscriber-policy** *subscriber_policy_name*: Specifies the subscriber policy name. *policy_name* must be an alphanumeric string.

Verifying the Configuration

This section describes how to verify the above configuration.

show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy_name*

Dynamic Configuration Change Support

Feature Description

The Dynamic Configuration Change Support feature allows new sessions, or subsequent messages of existing sessions, to use the updated configuration values.

This feature supports the following SMF configurations:

- DNN Policy
- DNN Profile
- Subscriber Policy

How it Works

This section describes how dynamic change in configuration works for the supported SMF configurations.

DNN Policy

DNN Policy configuration defines the DNN Profile mapping with the DNN. After the DNN to profile mapping is changed, new subscriber for the same DNN uses the updated DNN Profile. So, there is no impact on existing subscribers.

DNN Profile

DNN Profile defines the various parameters for a DNN.

The following table describes if the configuration change can be dynamically allowed or if you must set the DNN to an offline mode.

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
DnsServers	Allowed	No impact
DnnInfo	Allowed	New values are used after database reload of the session
NetworkElementProfile	Not recommended (See NOTES)	
Timeout	Allowed	No impact
ChargingProfile	Not recommended (See NOTES)	
RemoteVmac	Allowed	No impact
PcscfProfile	Allowed	No impact
PpdProfile	Allowed	Immediate (new values are used)
DefaultSscMode	Allowed	No impact
DefaultPduSession	Allowed	No impact
AllowedPduSession	Allowed	No impact
QosProfile	Allowed	Immediate (new values are used)
UpfApn	Allowed	No impact
SecondaryAuthen	Allowed	No impact
LocalAuthorization	Allowed	No impact

NOTES:

- In this release, we do not recommend changing (modify or delete) the NetworkElementProfile and ChargingProfile configuration parameters. If they are changed, the behavior for:
  - NetworkElementProfile: Messages for the existing sessions may be sent on new servers.
  - ChargingProfile: There may be some inconsistency between SMF and UPF related to URRs.
- For modifying the DNN Profile mapping, the DNN Profile must be in the offline mode.
- The SMF may report a warning when the configurations are modified. These modifications may have an impact on the ongoing calls. We recommend that you review the warning messages and take the appropriate action.

- You can switch the DNN profile to an offline mode when dynamically configuring the parameters. This step avoids the network impact, which is caused by the configuration changes.

Subscriber Policy

Subscriber Policy is used for selecting operator policy based on SUPI range, slice information, and so on. Change in Subscriber Policy configuration can be applied dynamically as it has no impact on existing sessions. Operator policy for the new sessions are selected based on the updated configurations.

Limitations

The following limitations apply when the DNN is in the offline mode:

- The subsequent 5G calls for the offline DNN are rejected with the HTTP Cause - HTTP_STATUS_CODE_503_SERVICE_UNAVILABLE, and 5GSMCause as “Service option temporarily out of order”.
- The subsequent 4G calls for the offline DNN are rejected with the GTP cause “No resources available".

Configuring Dynamic Configuration Change Support

This section describes how to enable dynamic configuration for the DNN Profile.

Configuring the DNN Profile to Offline Mode

Use the following command to configure the DNN Profile to offline mode.

```
config
  profile dnn profile_name
    mode offline
    end
```

NOTES:

- **config**: Enters the configuration mode.
- **profile dnn** *profile_name*: Specifies the DNN profile.
- **mode**: Specifies the mode of operation.
- **offline**: Specifies the mode as offline.

Verifying the DNN Profile Offline Mode Configuration

This section describes how to verify if the DNN profile is configured in the offline mode.

The following configuration is a sample output of the **show running-config profile dnn** *profile_name* command:

```
show running-config profile dnn intershat
profile dnn intershat
 mode offline/online [default: online]
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
```

```
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat
 dcnr             true
exit
```

Dynamic Configuration Change OAM Support

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

Statistics

The following label is introduced as part of this feature:

- LABEL_DISC_PDUSETUP_DNN_OFFLINE: This label is defined to indicate that the call is rejected because the DNN is in the offline mode.

IP Pool Allocation per DNN

Feature Description

The IP Pool Allocation per DNN feature supports mapping of a UE-requested DNN to a configured DNN for IP Pool selection. This feature is supported for the SMF and PGW-C in 5GC and 4G.

The IP Pool Allocation per DNN feature supports the following functionalities:

- Enables SMF to support the new configuration under the DNN profile to enable mapping of the UE-requested DNN to IP pool DNN.
- Sends the mapped DNN over GRPC to the Resource Manager functionality under Node Manager service for IP allocation.
- Supports the new configuration for IP Pool DNN over the virtual DNN with Redundancy Manager, if present
- Sends the UE-requested DNN when both the new configuration for IP pool and the virtual DNN are not present.

How it Works

This section provides a brief of how the IP Pool Allocation per DNN feature works.

- The DNN profile lookup is based on the subscriber policy or DNN policy. The DNN profiles are associated in the SMF profile configuration. The subscriber policy takes precedence over the DNN policy when both the configurations are present.
- The subscriber policy contains a list of precedence values. The selection of the precedence is based on the SUPI, GPSI, serving PLMN, and NSSAI value of the subscriber.
- Each precedence has an associated operator policy. The DNN policy is picked from the selected operator policy.

- The DNN policy can have a DNN profile configuration for each of the UE-requested DNN.
- The DNN profile contains the virtual or mapped DNN with its list of interfaces. This is an existing configuration and Redundancy Manager is also in the list of interfaces. For more information, see the "Configuring a Virtual DNN under a DNN Profile" section.
- The new configuration under the DNN profile contains the mapping of the UE-requested DNN to IP Pool DNN.
- The DNN profile selection occurs in the following order:
  - Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE requested DNN) > Virtual DNN mapping.
  - Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE requested Dnn) > Virtual DNN mapping.

Note

- New IP pool DNN mapping takes precedence over the existing virtual DNN configuration if the Redundancy Manager configuration exists.
- If the both the configurations for the Redundancy Manager are not present, the UE-requested DNN is used to select the IP pool.
- If the mapped DNN does not have the IP pool configured, then IP allocation fails, and the call is. deleted.
- Both the EPS and 5G calls follow the same principles for IP allocation for a DNN.

Configuring IP Pool Allocation

This section describes how to configure the IP Pool Allocation per DNN feature.

Configuring the IP Pool Allocation per DNN involves either one of the following steps:

1. Configuring virtual DNN under DNN profile. For more information, see the "Configuring a Virtual DNN under a DNN Profile" section.

Note This is a generic configuration along with other interfaces as an option.

2. Allocating the IP pool per DNN.

Note This configuration is specifically only for IP allocation.

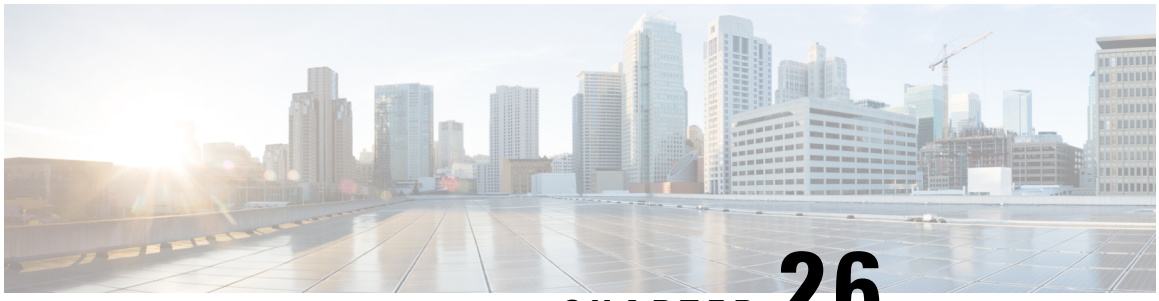
Allocating the IP Pool per DNN

To allocate the IP pool per DNN, use the following commands:

```
configure
  profile dnn pool_name
    dnn rmgr rmgr_name
    end
```

NOTES:

- **profile dnn** *pool_name*: Maps the specified Virtual DNN profile with the specified network DNN profile *pool_name* must be the name of the address pool.
- **dnn rmgr** *rmgr_name*: Specifies the Redundancy Manager to which the DNN profile will be sent. *rmgr_name* must be an alphanumeric string.



CHAPTER 26

Network-initiated Messages Support

Feature Summary and Revision History

Summary Data

Table 100: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 101: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

Connection Management (CM) includes the functions to establish and release a NAS signaling connection between a UE and the Access and Mobility Management Function (AMF) over the N1 interface. This signaling connection enables the NAS signaling exchange between the UE and the core network.

The 5GS CM states determine the NAS signaling connection of the UE with the AMF. The following are the CM states:

- **CM-Idle**—When a UE is in the CM-Idle state, the UE has no NAS signaling connection established with the AMF over the N1 interface. The AN signaling connection, N2 connection, and N3 connection do not exist in this state.
- **CM-Connected**—When a UE is in the CM-Connected state, the UE has a NAS signaling connection with the AMF over the N1 interface. A NAS signaling connection uses an RRC Connection between the UE and the NG-RAN and an NGAP UE association between the AN and the AMF for the 3GPP access.

The CM states for the 3GPP access and the non-3GPP access are independent of each other. It implies that both the access can be in the CM-Idle state and the CM-Connected state simultaneously.

SMF supports network-initiated messages when a UE is either in the CM-Idle state or in the CM-Connected state.

How it Works

When connected to the 5G core, a UE can be in CM-Connected with RRC Inactive state too. This state is between the CM-Idle and CM-Connected states.

The SMF cannot identify the UE CM state when the state is between UE and AMF. The SMF only identifies the user plane connection state. This state and the N1 and N2 transfer message response status control the behavior of SMF for network-initiated messages. These messages are for signaling modification or downlink data-related user plane activation procedures. The details for these procedures are described in the following call flows.

Call Flows

This section describes the following call flows:

- Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State
- Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State
- Network-Initiated Modification Call Flow for Active User Plane and UE in CM-Connected State
- Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State
- Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State

Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State

This section describes the downlink data notification User Plane activation call flow when UE is in the CM-Connected state.

Figure 79: Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State

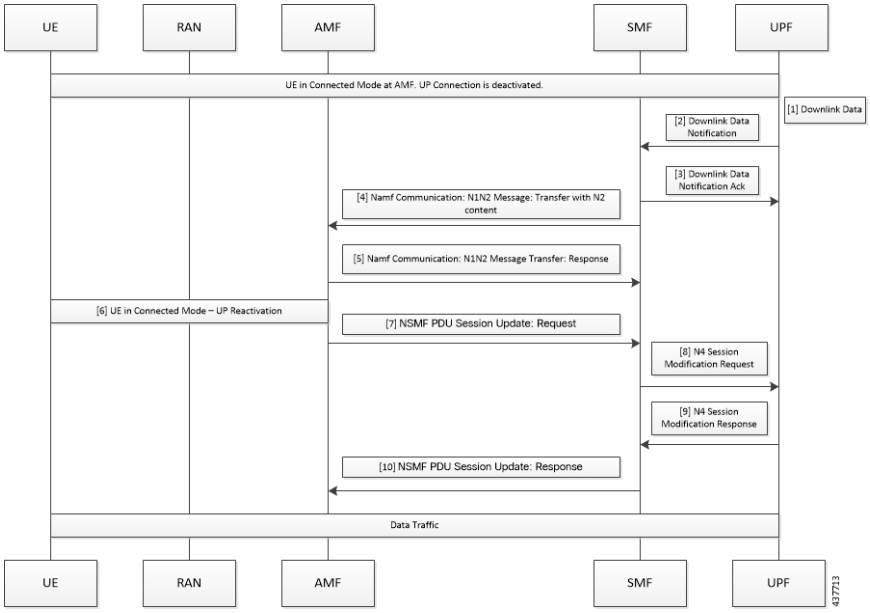


Table 102: Downlink Data Notification User Plane Activation Call Flow Description for UE in CM-Connected State

Step	Description
1	When the UPF receives the downlink data for a PDU session and if no AN tunnel information is saved in the UPF for the PDU session, the UPF buffers the downlink data. The buffering is done based on the instruction from the SMF.
2	The UPF sends data notification towards SMF. This notification includes the N4 session ID, the information to identify the QoS flow for the DL data packet, and the DSCP details.
3	The SMF sends the acknowledgement data notification to the UPF.
4	The SMF initiates the NAMF communication N1 and N2 message transfer towards the AMF. This message transfer includes details, such as PDU session ID, N2 SM information (QFIs, QoS profiles), CN N3 tunnel information, S-NSSAI, ARP, Paging Policy Indicator, 5QI, N1 and N2 transfer failure notification target address, and the PDU session resource setup request IE.
5	As the UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “200 OK” status code and the “N1_N2_TRANSFER_INITIATED” cause.
6	The User Plane Reactivation procedures begin. The reactivation procedures set up the radio resources and activate the user plane to establish the N3 tunnel.
7	The AMF sends the NSMF PDU Session Update SM Context Request toward SMF. This request contains the SM information of the N2 interface. The connection state of user plane is activated.
8	The SMF sends the N4 modification procedure toward the UPF to activate the session and to update the AN tunnel information, which is the IP and TEID. The session is activated by performing the remove buffer action and the set forward action.

Step	Description
9	The UPF modifies the session and sends the acknowledgement of the modification to the SMF.
10	The SMF responds back to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request with the connection state of user plane as activated.

Note The following N1 and N2 response error cases are handled:

- For 404 Context Not Found status, a PDU session is released.
- For 504 or 403 status with the "UE_IN_NON_ALLOWED_AREA" and "NOT_REACHABLE" cause, an N4 modification request is sent to drop the buffered packets and to not send the CP notification for the downlink data.
- For the N1and N2 transfer notification failure, the N4 modification request is sent to drop the buffered packets and to not send the CP notification for downlink data.
- For 409 status code with the Retry After timer value, the N1 and N2 transfer is re-initiated after the timeout value.
- For the 409 status code with "HIGHER_PRIORITY_REQUEST_ONGOING" cause, the lower priority N1 and N2 transfers are not allowed. Only the higher priority transfers are communicated to the AMF.

Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State

This section describes the downlink data notification User Plane activation call flow when UE is in CM-Idle state.

Figure 80: Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State

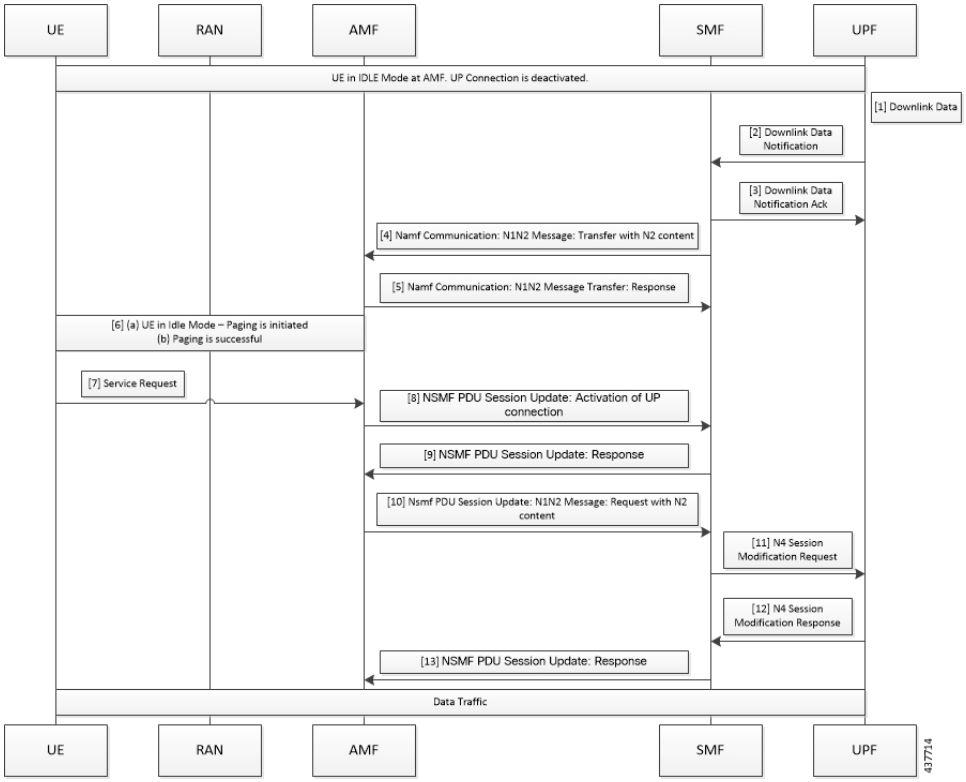


Table 103: Downlink Data Notification User Plane Activation Call Flow Description for UE in CM-Idle State

Step	Description
1	When the UPF receives the downlink data for a PDU session and if no AN tunnel information is saved in the UPF for the PDU session, then based on the instruction from the SMF, the UPF buffers the downlink data.
2	The UPF sends data notification towards the SMF. This notification includes the N4 Session ID, the information to identify the QoS flow for the DL data packet, and the DSCP details.
3	The SMF sends the acknowledgement data notification to the UPF.
4	The SMF initiates the NAMF communication N1 and N2 message transfer toward AMF. This message transfer includes details, such as PDU session ID, N2 SM information (QFIs, QoS profiles), CN N3 tunnel information, S-NSSAI, ARP, Paging Policy Indicator, 5QI, and N1 and N2 transfer failure notification target address.
5	As the UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “202 Accepted” status code and “ATTEMPTING_TO_REACH_UE” cause.
6	The AMF triggers the paging procedure towards the UE.
7	The UE receives the paging request and initiates the requested service to activate the session.

Step	Description
8	The AMF initiates the NSMF PDU Session Update SM Context Request towards SMF with connection state of user plane configured as activating.
9	The SMF responds back to the AMF with “200 OK” status code for the NSMF PDU Session Update SM Context Request. This request includes details, such as N2 SM information (QFIs, QoS profiles), CN N3 tunnel information, S-NSSAI, ARP, Paging Policy Indicator, 5QI, N1 and N2 transfer failure notification target address, and the PDU session resource setup request IE.
10	The AMF sends the NSMF PDU Session Update SM Context Request towards the SMF. This request contains the SM information of the N2 interface. The connection state of user plane is Activating.
11	The SMF initiates the N4 modification procedure towards the UPF to activate the session and to update the AN tunnel information, which is the IP and TEID. The session is activated by performing the remove buffer action and set forward action.
12	The UPF modifies the session and sends the acknowledgement of the modification to the SMF.
13	The SMF responds back to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request with connection state of user plane as Activated.

Network-Initiated Modification Call Flow for Active User Plane and UE in CM-Connected State

This section describes the network-initiated modification call flow when the UE is in CM-Connected State and the User Plane is activated. The network can be PCF, UDM, or SMF.

Figure 81: Network-Initiated Modification Call Flow for UE in CM-Connected State and Activated User Plane

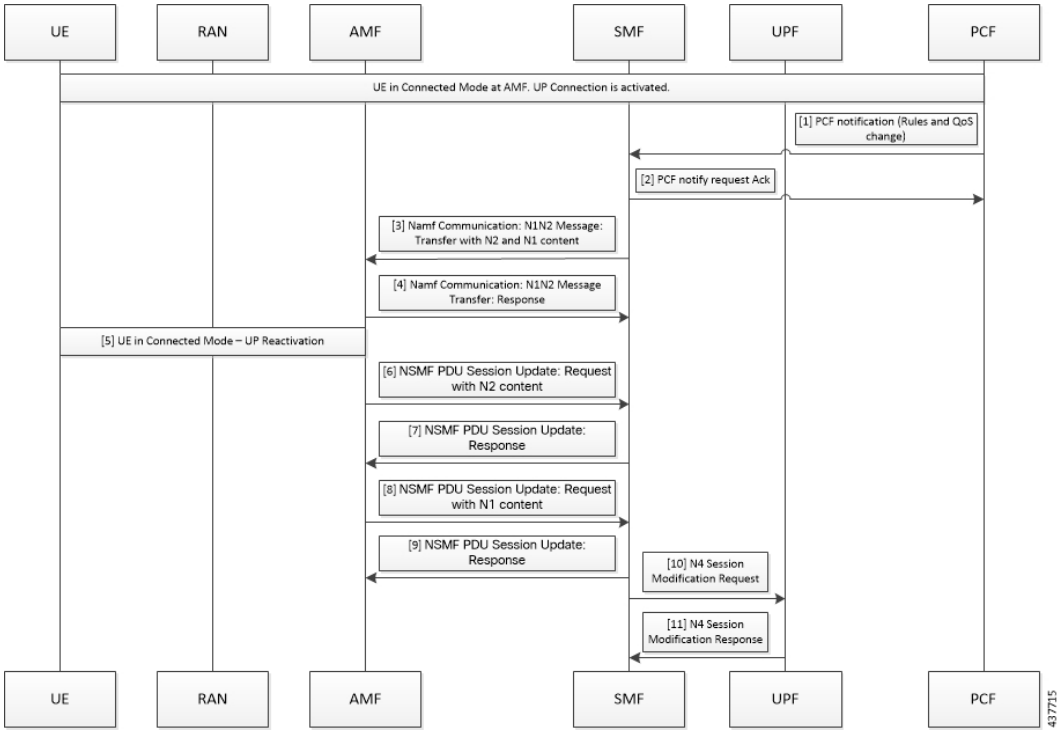


Table 104: Network-Initiated Modification Call Flow Description for UE in CM-Connected State and Activated User Plane

Step	Description
1	The PCF sends the notification towards SMF with policy decision to apply.
2	The SMF sends an acknowledgement for the policy notification to the PCF.
3	The SMF identifies the changes in QoS model that occur due to policy decision and triggers the NAMF Communication N1 and N2 message transfer toward AMF. This message transfer includes details, such as PDU Session ID, N2 SM information, N1 SM information, and N1 and N2 transfer failure notification target address. N2 includes the PDU session resource modify request transfer IE and N1 includes the PDU session modification request.
4	As UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “200 OK” status code and “N1_N2_TRANSFER_INITIATED” cause.
5	The user plane modification procedures begin both towards RAN and UE.
6	After receiving a response from RAN, the AMF sends the NSMF PDU Session Update SM Context Request towards the SMF. This request contains the SM information of the N2 interface.
7	The SMF responds back to the AMF with “200 OK” status code for the NSMF PDU Session Update SM Context Request.

Step	Description
8	After receiving a response from the UE, the AMF sends the NSMF PDU Session Update SM Context Request toward SMF. This request contains the SM information of the N1 interface.
9	The SMF responds back to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request.
10	Based on the new QoS information, the SMF initiates the N4 Modification procedure towards the UPF to modify the session.
11	The UPF modifies the session and sends the acknowledgement of modification to the SMF.

Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State

This section describes the network-initiated modification procedure when the UE is in CM-Connected state and the User Plane (UP) context is deactivated.

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “N1N2_TRANSFER_INITIATED” cause.
5. The SMF waits for the Nsmf_PDUSession_UpdateSMContext message from the AMF.
6. After receiving the response from UE, the SMF updates the subscriber’s session in the UPF with the modified parameter values and the UP context state remains as deactivated.
7. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details.
8. The UPF sends the N4 Session Modification response for the PDU session.
9. The SMF activates the UP connection as a result of the trigger to send downlink or uplink data.

Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State

This section describes the network-initiated modification procedure when the UE is in CM-Idle state and the User Plane (UP) context is deactivated.

The SMF supports the following use cases during the network-initiated PDU session modification procedure:

- When the UE turns active with the service request for PDN activation
- When the UE turns active with the control service request

Use case 1: When the UE turns active with the service request for PDN activation

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “ATTEMPTING_TO_REACH_UE” cause.
5. The SMF stops the retransmission of the N1 - PDU Session Modification response message to the UE. Further, it stops the N1 PDU Modification Command retransmission timer and waits for a response from the UE.
6. The UE receives the paging request from the AMF and initiates the requested service to activate the PDU session. The UE includes the PDU Session ID in PDU Session-to-Activate list only if the UP context needs to be activated.

   The SMF initiates the Idle-to-Active PDU Session transition procedure and suspends the current modification procedure.
7. After the Idle-to-Active procedure is complete, the SMF restarts the modification procedure and sends both the N1 and N2 content in N1 N2 transfer message and waits for both N1 and N2 response from the UE and gNB respectively.
8. The SMF receives the N2 response from gNB, and the N1 response from the UE respectively.
9. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details.
10. The UPF sends the N4 Session Modification response for the PDU session.

Use case 2: When the UE turns active with the control service request

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “ATTEMPTING_TO_REACH_UE” cause.
5. The SMF stops the retransmission of the N1 - PDU Session Modification response message to the UE. Further, it stops the N1 PDU Modification Command retransmission timer and waits for a response from the UE.
6. The AMF initiates the paging procedure towards the UE and the UE turns active with the Service Request for control message.
7. The SMF receives the N1 response from the UE.

8. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details. Then, the SMF sets the Forwarding Action Rule (FAR) action for the new rules as ‘drop’.
9. The UPF sends the N4 Session Modification response for the PDU session.

Limitations

In this release, this feature has the following limitation:

- Temporary rejections due to ongoing handover and registration procedures are not handled.

Standards Compliance

The network-initiated messages support for UE in CM-Idle or CM-Connected state feature complies with the 3GPP TS 23.502, V15.6.0 (2019-10).

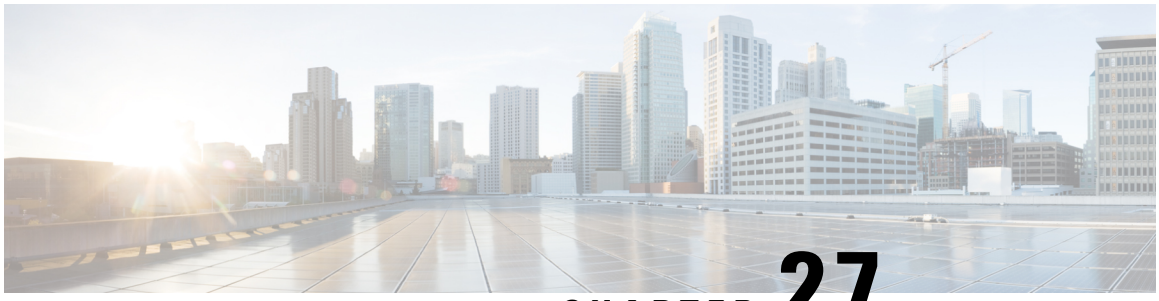
OAM Support

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

Statistics Support

The SMF maintains the following statistics triggered during the network-initiated modification procedure.

- Total number of attempted network-initiated modifications triggered when the UP context is deactivated.
- Total number of succeeded network-initiated modifications triggered when the UP context is deactivated.
- Total number of failed network-initiated modifications triggered when the UP context is deactivated.
- Total number of "ATTEMPTING_TO_REACH_UE" status received when the network-initiated modification procedure is triggered and the UP context is deactivated.
- Total number of "N1N2_TRANSFER_INITIATED" status received when the network-initiated modification procedure is triggered and the UP context is deactivated.



CHAPTER 27

Network-Initiated Service Request

Feature Summary and Revision History

Summary Data

Table 105: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 106: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The N3 tunnel profile helps in defining the forwarding action rules while moving from active to idle transition.

The N3 tunnel profile configuration includes:

- Enabling control plane notification (notify)
- Enabling buffering on UPF (buffer UPF)

How it Works

Call Flows

UE-initiated Idle to Active Transition

The following call flow depicts the UE initiated idle to active transition.

Figure 82: Idle to Active Transition (UE-Initiated) Call Flow

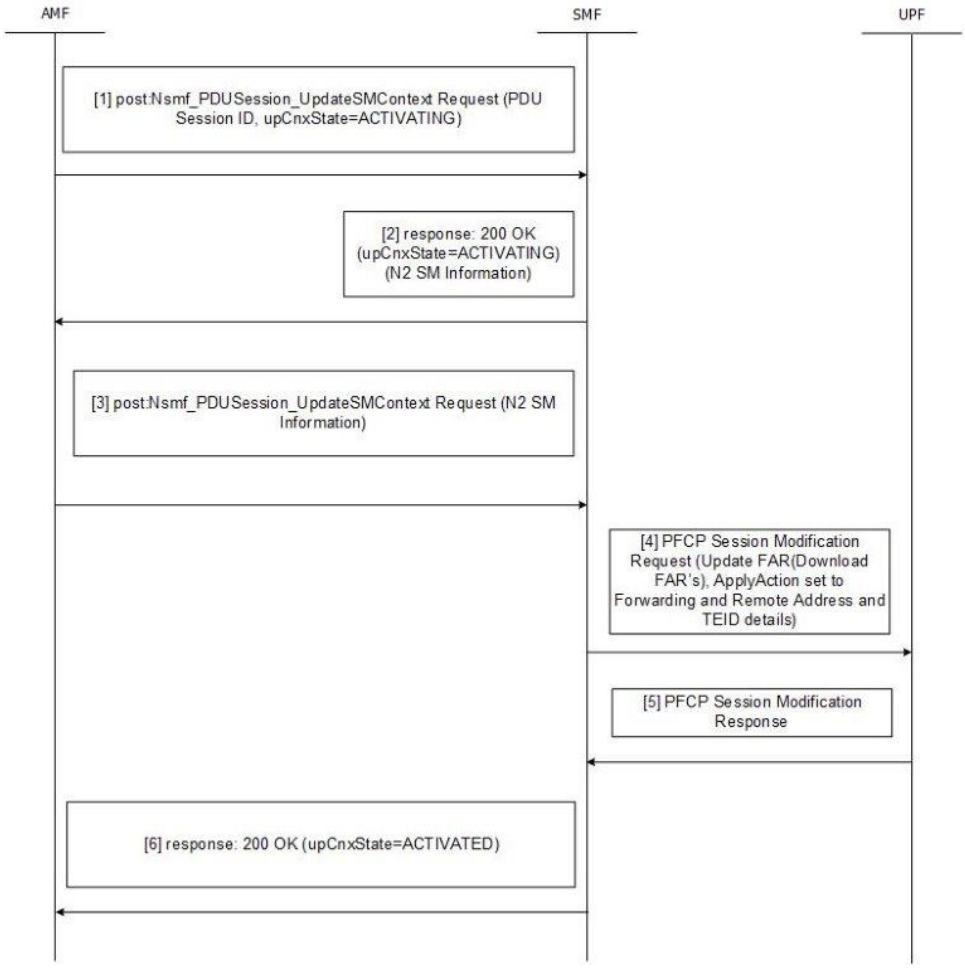


Table 107: Idle to Active Transition (UE-Initiated) Call Flow Description

Step	Description
1	The AMF requests SMF to activate the user plane connection of the PDU session by sending a POST request with the following information: • upCnxState attribute set to ACTIVATING. • User location, user location timestamp and access type associated to the PDU session (if modified). • Other information (if necessary).
2	Upon receipt of the request, the SMF starts activating the N3 tunnel of the PDU session. The SMF returns a 200 OK response with the following information: • upCnxState attribute set to ACTIVATING; • N2 SM information to request the 5G-AN to assign resources to the PDU session including the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for the current PDU session (i.e. UPF's GTP-U F-TEID for uplink traffic).
3	Subsequently, the AMF requests the SMF by sending POST request with the following information: • N2 SM information received from the 5G-AN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for the current PDU session (i.e. 5G-AN's GTP-U F-TEID for downlink traffic), if the 5G-AN succeeded in establishing resources for the PDU sessions.
4	The SMF initiates PFCP Session Modification Procedure towards UPF with down link FAR updated with the following options: • Forwarding Action enabled along with remote node “forwarding parameters” details like the IP address and GTP-U F-TEID.
5	Upon receipt of successful response from UPF node, the SMF sets the upCnxState attribute to ACTIVATED for the PDU session.
6	SMF then initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF.

Network-initiated Idle to Active Transition

The following call flow depicts network initiated idle to active transition.

Figure 83: Idle to Active Transition (NW Initiated) Call Flow

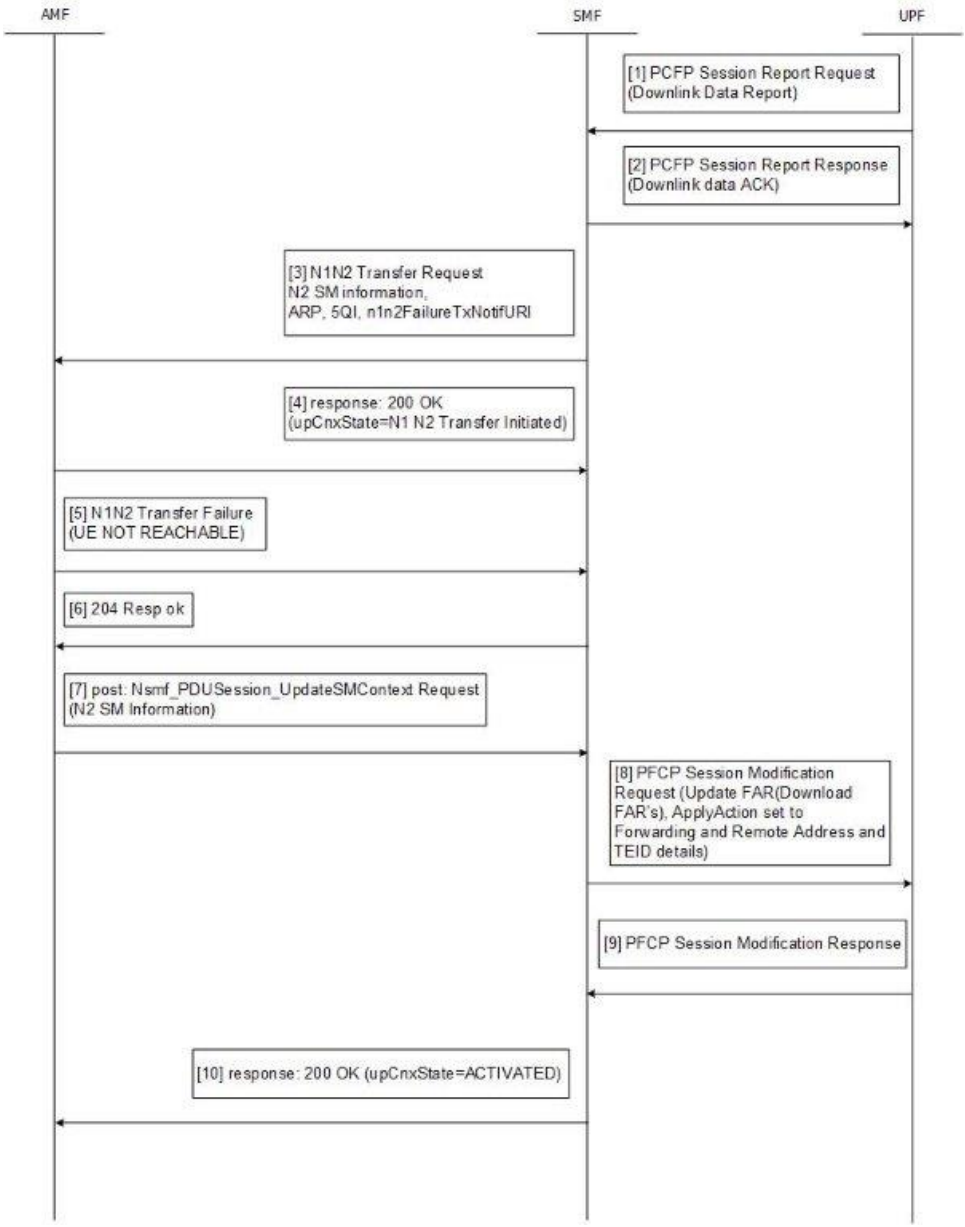


Table 108: Idle to Active Transition (NW Initiated) Call Flow

Step	Description
1	The UPF sends "PFCP session report request" to the SMF. • Report Type as DLDR (Downlink Data Report). • The "Downlink Data Report" IE contains corresponding "PDR ID".
2	The SMF sends the PFCP session report response.

Step	Description
3	The SMF sends "N1N2MessageTransfer" to AMF with the following attributes: • SUPI, PDU Session ID, • N2SMInformation as "ngapIeType":77 (id-PDUSessionResourceSetupListSUReq), "ngapMessageType":27 (id-PDUSessionResourceSetup). • PDUSessionResourceSetupListSUReq has the PDU session id, QFI, QoS profile, UPF's GTP-U F-TEID for uplink traffic, QFI, QoS profile, S-NSSAI, User Plane Security Enforcement, UE Integrity Protection Maximum Data Rate, and Cause. • Area of validity for N2 SM information, ARP, Paging Policy Indication, 5QI, N1N2TransferFailure Notification Target Address (n1n2FailureTxfNotifURI).
4	The SMF receives the “N1N2TransferResponse” with the following status codes: • 200/202 OK and cause as "N1_N2_TRANSFER_INITIATED" (proceed to Step 6). • 409/504 and Cause “UE_IN_NON_ALLOWED_AREA” (proceed to Step 7).
5	The AMF sends the N1N2 Transfer failure response. If the UE is not reachable, move to Step 7.
6	Subsequently, the AMF requests the SMF by sending POST request with the following information: • N2 SM information received from the 5G-AN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for the current PDU session (i.e. 5G-AN's GTP-U F-TEID for downlink traffic), if the 5G-AN succeeded in establishing resources for the PDU sessions.

7	The SMF initiates PFCP Session Modification Procedure towards UPF with down link FAR updated with following options:
	• If N2 Transfer is successful, Forwarding Action is enabled along with remote node “forwarding parameters” details like IP address and GTP-U F-TEID.
	• If the cause of transfer failure is ATTEMPTING_TO_REACH_UE or UE_IN_NON_ALLOWED_AREA:
	  • Update FAR > Apply Action > NOCP: 1
	  • Update FAR > Apply Action > DROP:1
	  • PFCPSMReq-Flags > DROBU:1
	• If the cause of transfer failure is UE_NOT_REACHABLE:
	  • Update FAR > Apply Action > NOCP: 0
	  • Update FAR > Apply Action > DROP:1
	  • PFCPSMReq-Flags > DROBU:1

Step	Description
8	Upon receipt of successful response from UPF node, the SMF sets the upCnxState attribute to ACTIVATED for the PDU session.
9	The SMF then initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF (Only if Step 6 is completed and response is received from Step 8).

Network Initiated Service Request

During network initiated service request, SMF handles the temporary reject for N1N2 response message from AMF as mentioned in 3GPP document TS 23.502 section 4.2.3.3.

Figure 84: Temporary Reject during Network Triggered Service Request - 1

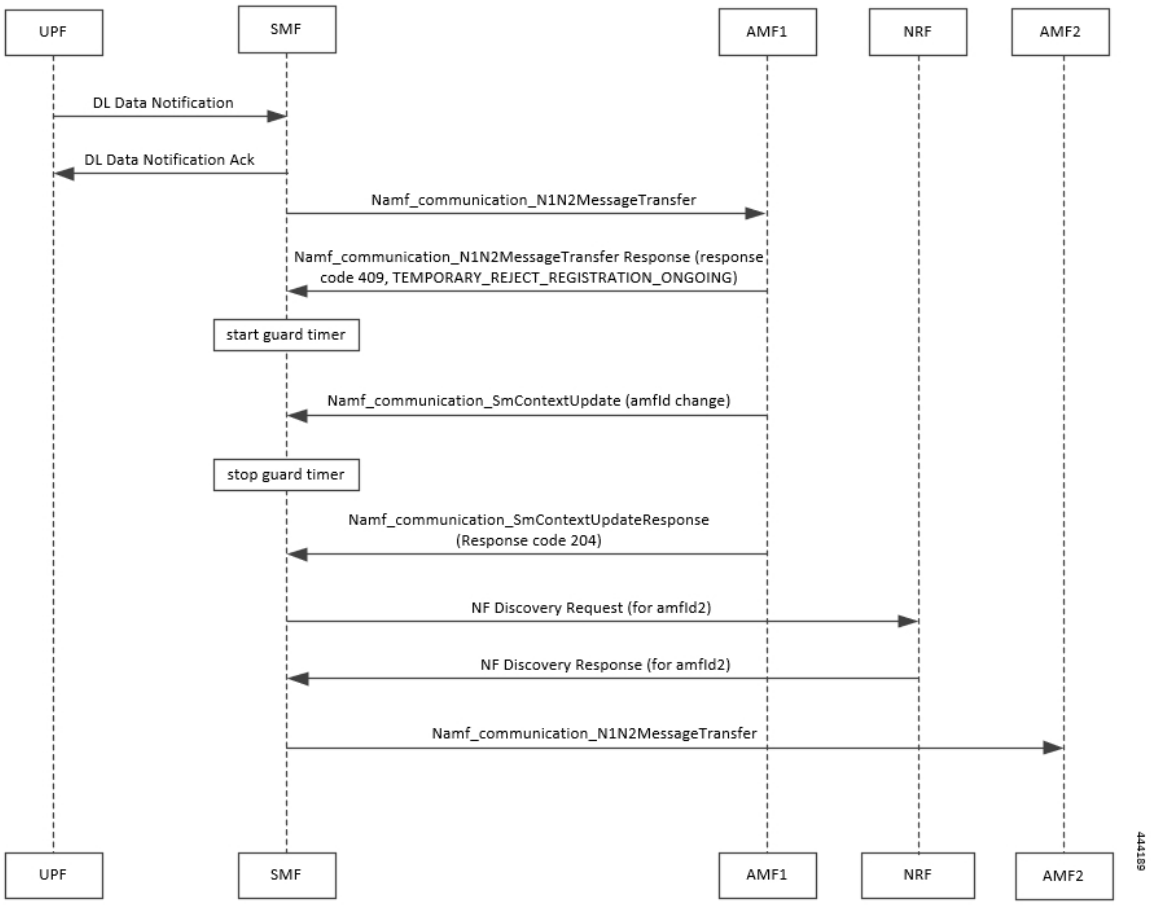


Table 109: Temporary Reject during Network Triggered Service Request - 1

Step	Description
1	On getting a trigger for service request in UP IDLE session state, SMF initiates a N1N2 message towards the AMF as part of Idle mode exit procedure.

Step	Description

2	If UE registration procedure with new AMF is in progress then AMF responds with temporary reject for N1N2 message with response code 409 and cause as:
	`TEMPORARY_REJECT_REGISTRATION_ONGOING`
	OR
	`TEMPORARY_REJECT_HANDOVER_ONGOING SMF`

3	On receiving the response, SMF starts a guard timer of 2 seconds that is configured locally.
4	While guard timer is running, SMF expects either a SM Context Update with AMF ID change or SM Context Update for handover.
5	On receiving SM Context Update with AMF ID change, SMF: **1.** Stops the guard timer. **2.** Removes the reference to the discovery information for old AMF. **3.** Stores the new UE location information, PLMN information and AMF information. **4.** Send SM Context Update response success without content. **5.** Reinitiates N1N2 message transfer to the new AMF. This involves NF discovery and subsequent transmission to the new AMF.
6	On receiving SM Context Update for N2 handover, SMF: **1.** Starts the Handover procedure. **2.** Suspends the Idle mode exit procedure and stops the guard timer. **3.** As part of the Handover procedure completion, old AMF details are removed and new AMF information is stored. **4.** Idle mode exit procedure resumes after Handover procedure is complete. **5.** Reinitiates N1N2 message transfer, if required, to the new AMF. This involves NF discovery and subsequent transmission to new AMF.

Figure 85: Temporary Reject during Network Triggered Service Request - 2

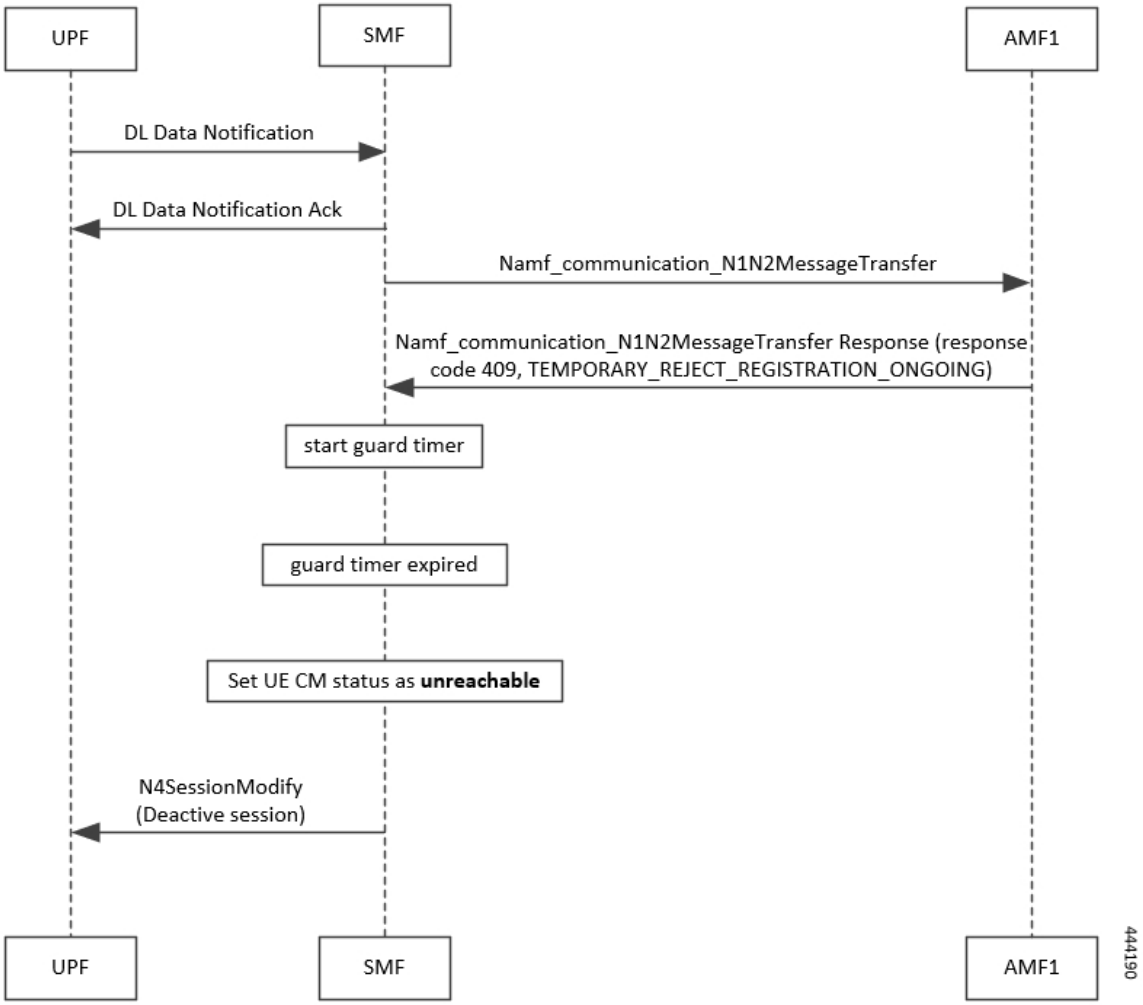


Table 110: Temporary Reject during Network Triggered Service Request - 2

Step	Description
1	On getting a trigger for service request in UP IDLE session state, SMF initiates a N1N2 message towards the AMF as part of Idle mode exit procedure.

2	If UE registration procedure with new AMF is in progress then AMF responds with temporary reject for N1N2 message with response code 409 and cause as:
	`TEMPORARY_REJECT_REGISTRATION_ONGOING`
	OR
	`TEMPORARY_REJECT_HANDOVER_ONGOING SMF`

3	On receiving the response, SMF starts a guard timer of 2 seconds that is configured locally.

Step	Description
4	Once guard timer expires, SMF: **1.** Sets the UE CM status as *NotReachable*. **2.** Deactivates the UP session state.

Limitations

The following are limitations in this release:

- It does not support location update and access-type changes.
- It does not support QoS flow modifications/errors.

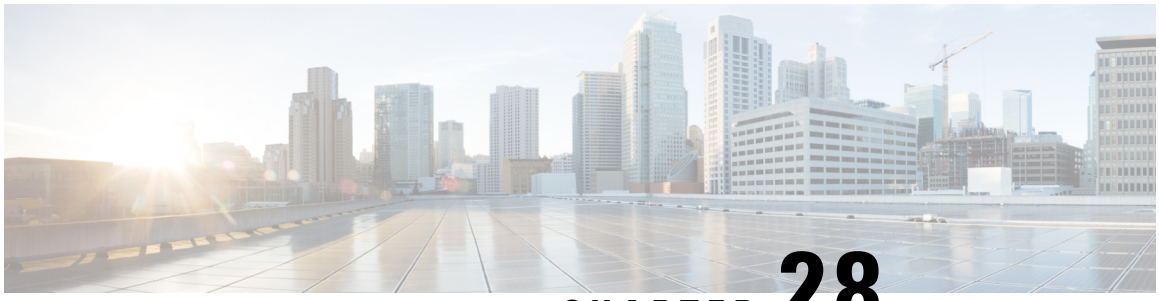
Configuring N3 Tunnel Profile

To configure the N3 tunnel profile, use the following configuration:

```
config
  n3-tunnel-profile profile_name
    buffer upf
      notify
      end
```

NOTES:

- **buffer** *upf*: Configures buffering for Downlink Data.
- **notify**: Enables data notification from UPF.



CHAPTER 28

NRF Discovery

Feature Summary and Revision History

Summary Data

Table 111: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 112: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The 3GPP-defined architecture model for 5G systems provides data connectivity based on techniques such as network function virtualization, software defined networking, and service-based interfaces. Some of the key principles are:

- Separate the User Plane (UP) functions from the Control Plane (CP) functions allowing independent scalability, evolution, and flexible deployments, such as centralized location or distributed (remote) location.
- Support "stateless" NFs where the "compute" resource is decoupled from the "storage" resource.

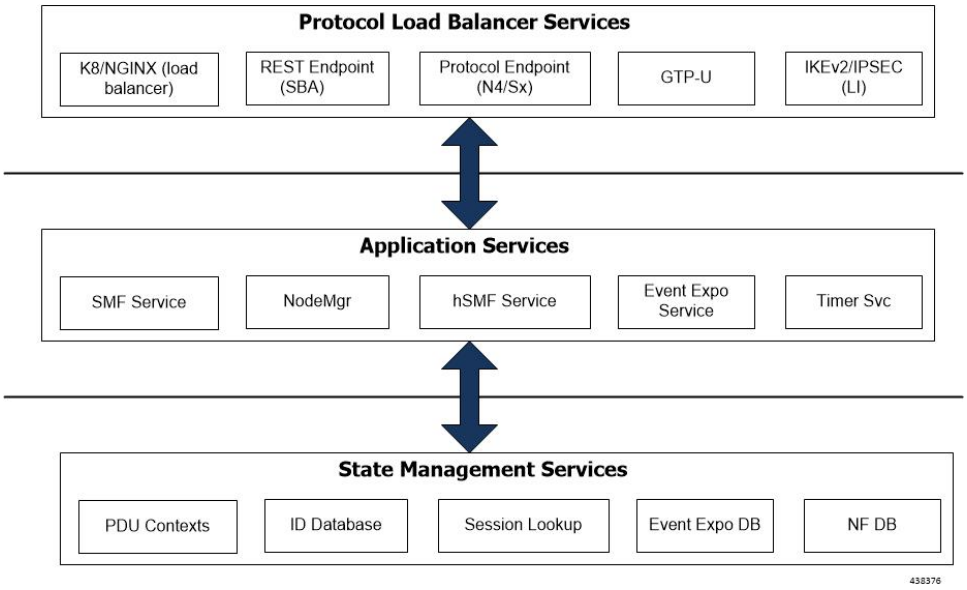
This feature discovers the set of NF instances (and their associated NF service instances), represented by their NF profile, that are currently registered in Network Repository Function (NRF) and satisfy several input query parameters.

Architecture

The SMF NF comprises of loosely coupled microservices. Microservice decomposition is based on three-layered architecture philosophies:

1. Layer 1: Protocol and Load Balancer Services (Stateless)
2. Layer 2: Application Services (Stateless)
3. Layer 3: Database Services (Stateful)

Figure 86: SMF 3-layered Micro Services Architecture



How it Works

The service operation is executed by querying the "nf-instances" resource. The request is sent to an NRF in the same PLMN of the NF service consumer.

Call Flows

The Service Discovery Request call flow described in 3GPP TS 29.510 v15.2.0 illustrates the NF-level messages for NF discovery.

Service Discovery Request Call Flow

This section describes the Session Discovery Request call flow.

Figure 87: Service Discovery Request Call Flow

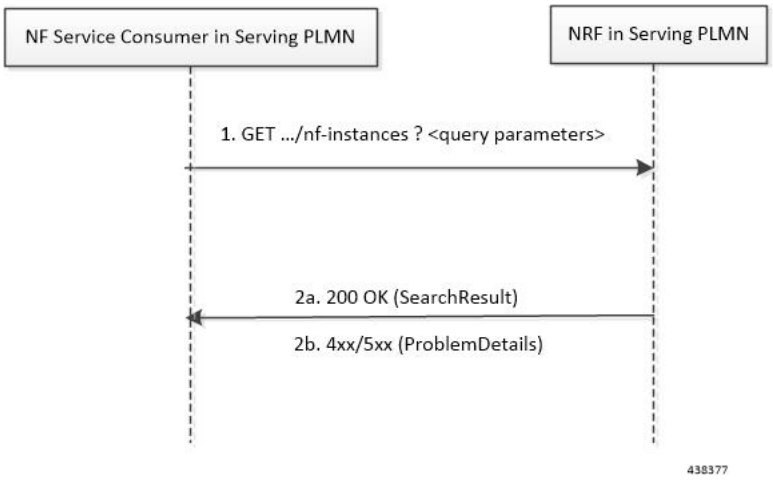


Table 113: Service Discovery Request Call Flow Description

Step	Description
1	The NF Service Consumer sends an HTTP GET request to the resource URI "nf-instances" collection resource. The input filter criteria for the discovery request is included in query parameters.
2a	On success, "200 OK" is returned. The response body contains a validity period, during which the search result can be cached by the NF Service Consumer, and an array of NF profile object that satisfy the search filter criteria (for example, all NF Instances offering a certain NF Service name).
2b	If the NF Service Consumer is not allowed to discover the NF services for the requested NF type provided in the query parameters, the NRF returns "403 Forbidden" response. If the discovery request fails at the NRF due to errors in the input data in the URI query parameters, the NRF returns "400 Bad Request" status code with the “ProblemDetails” IE providing details of the error. If the discovery request fails at the NRF due to NRF internal errors, the NRF returns "500 Internal Server Error" status code with the “ProblemDetails” IE providing details of the error.

The NF profile objects that are returned in a successful result contains generic data of each NF instance, applicable to any NF type, and it can also contain NF-specific data, for those NF instances belonging to a specific type (for example, the attribute "udrInfo" is typically present in the NF profile when the type of the NF instance takes the value "UDR"). In addition, the attribute "customInfo" can be present in the NF profile for NF instances with custom NF types. For NF instances, the "customInfo" attribute is returned by NRF, if available, as part of the NF profiles returned in the discovery response.

SMF service communicates with different NFs, such as UDM, AMF, PCF, CHF and so on, when the session is brought up. The NF discovery is based on set of filters that are associated with the session. The SMF service discovers the NFs, matching the filter criteria for the session, to send messages to NF.

NRF Library (NRF-LIB) provides APIs to discover and send a message to an NF matching a set of filter parameters. The NRF-LIB performs NF discovery for the filter and caches the discovered NFs in a local cache. The following filter parameters are supported:

- Dnn
- Tai
- TargetNfFqdn
- TargetPlmnList
- TargetNfInstanceId
- Snssais
- Preferred locality

The discovered NFs are cached with the filter as the key. The endpoint selection for sending the message is based on probabilistic load balancing algorithm (IETF RFC 2782) using the priority and capacity parameters. The NF discovery response carries a validity time, which decides the cache validity period.

NRF-LIB sends the messages to a new target based on the Location header URL in response to initial messages sent to NF.

NRF-LIB supports stickiness wherein the endpoint, service instance, and NF instance details of the selected endpoint for a message that is sent, will be provided to the App/Rest-Ep so that the same can be specified in subsequent message (instead of discovery filter). This helps maintaining stickiness for a session to a selected NF.

Standards Compliance

The NF Discovery feature complies with the following standards:

- 5G System; Network Function Repository Services; Stage 3 (Release 15):
  - 3GPP TS 29.510 version 15.0.0 (2018-06)
  - 3GPP TS 29.510 version 15.2.0 (2018-12)

Limitations

The following are known limitations of this feature:

- The cache maintained is local to the library. Therefore, in case of deployment with multiple replicas of Rest-Ep, if two Discovery/Send messages with the same discovery filter land on different pods, then the NF discovery will be triggered by both pods.
- Only UDM, PCF, CHF, and AMF discovery and load balancing are supported. UPF discovery is not supported.
- Dynamic configuration changes of NRF endpoints are not supported.

NF Heartbeat Support

Feature Description

The NF heartbeat implementation helps the NFs to notify the NRF that the NF is operational. Each NF registered with the NRF contacts the NRF periodically by invoking the NFUpdate service operation. The time interval at which the NRF is contacted is deployment-specific and is returned by the NRF to the NF Service Consumer as a result of a successful registration.

How it Works

Call Flows

NF Heartbeat Procedure

The following figure illustrates the NF Heartbeat call flow.

Figure 88: NF Heartbeat Call Flow

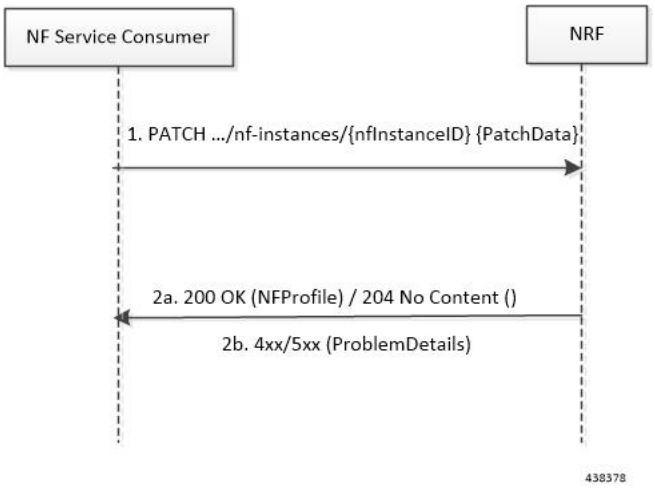


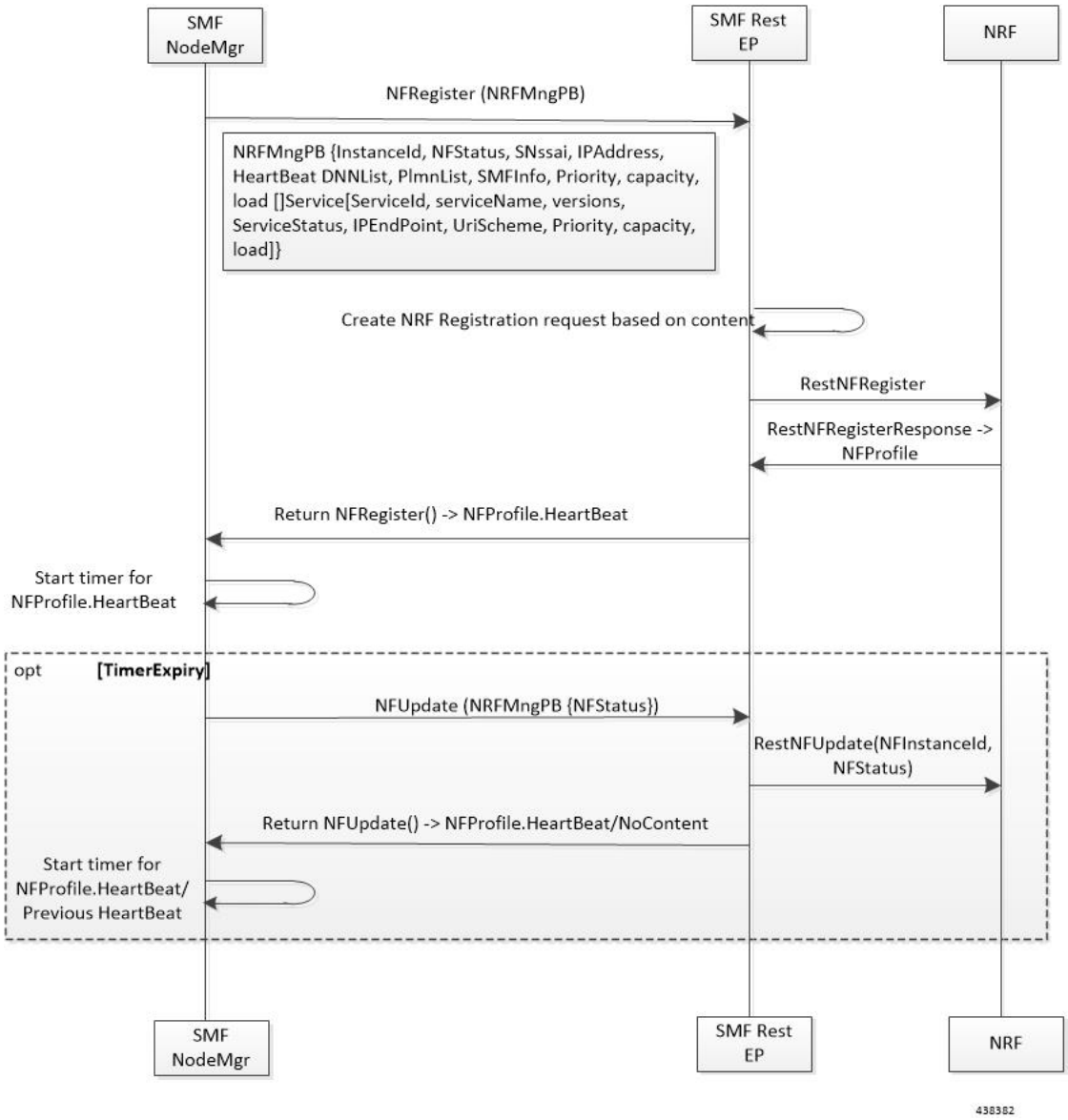
Table 114: NF Heartbeat Call Flow Description

Step	Description
1	The NF Service Consumer sends a PATCH request to the resource URI representing the NF instance. The payload body of the PATCH request contains a replace operation on the nfStatus attribute of the NF Profile of the NF instance, and set it to the value REGISTERED.
2	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body; otherwise, "204 No Content" is returned.
3	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF's database, the NRF returns "404 Not Found" status code with the ProblemDetails IE providing details of the error. Example: **PATCH .../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64** **Content-Type: application/json-patch+json** **[** **{"op": "replace", "path": "/nfStatus", "value": "REGISTERED"}** **]** **HTTP/2 204 No Content** **Content-Location: .../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64**

NRF Heartbeat Internal Call Flow

The following figure shows the internal call flow related to the NRF Heartbeat feature.

Figure 89: NRF Heartbeat Internal Call Flow



The SMF NF heartbeat implementation helps in notifying the NRF that the SMF is operational. The default heartbeat frequency is once in 10 seconds. If the NRF returns a different heartbeat frequency, the same is used for the periodic heartbeat. As part of the heartbeat, HTTP PATCH Request to the resource URI representing the NF instance is sent to the NRF. The payload body of the PATCH Request contains a "replace" operation on the "nfStatus" attribute of the NF profile of the NF instance, and sets it to the value "REGISTERED". Other parameters like load and capacity are not supported in this release.

Like NF registration, NF heartbeat is also triggered from the elected master node manager. Also, the heartbeat continues even on the elected node manager restart.

Standards Compliance

The NF Heartbeat feature complies with 3GPP TS 29.510, Version 15.2.0.

Caching Support for NF Discovery

Feature Description

The SMF provides caching support for discovered caching profiles. It uses the NF discovery (nnrf-disc) function to discover profiles such as AMF, UDM, PCF, and CHF. The received discovery response is associated with validity time. SMF caches the discovery response and uses the same response for future NF selections until the cache is valid. This caching support helps in reducing the number of NRF interactions during an ongoing session.

Relationships

Caching support for NF Discovery has functional relationship with the following features:

- NRF Support for SMF Subscription and Notification
- NRF Interface Per Endpoint

How it Works

The SMF maintains the cache data in a Cache pod. It uses the cache pod to share the NF discovery cache across multiple instances of SBI pods. The SBI pod periodically updates the cache pod on receiving an NF discovery response. All SBI pods refreshes its cache data periodically with the help of the cache pod.

Currently, the SMF does not invalidate the NF discovery cache entry even on the expiration of the validity time. If a message is sent to a NF that meets a specific criterion, the SMF looks up the cache data for further processing. During a cache look-up:

- On a cache hit without an expired entry, the selected cached NF response is used to send a message for an endpoint selection.
- On a cache hit with an expired entry, SMF sends NF discovery requests to NRF to fetch a new list of NF discovery responses.
- If there is a cache miss, the SMF sends the NF discovery request again to the NRF to retrieve a new list of discovery responses.

Call Flows

Cache Lookup Call Flow

This section describes the Cache Lookup call flow.

NRF-LIB (in smf-rest-ep/SBI) maintains a local cache and updates the external cache (cache-pod). The key for a cache is a combination of nfType and filter (a string that is prepared from multiple filter parameters in "key1=value, key2=value2" format).

Figure 90: Caching Support Call Flow

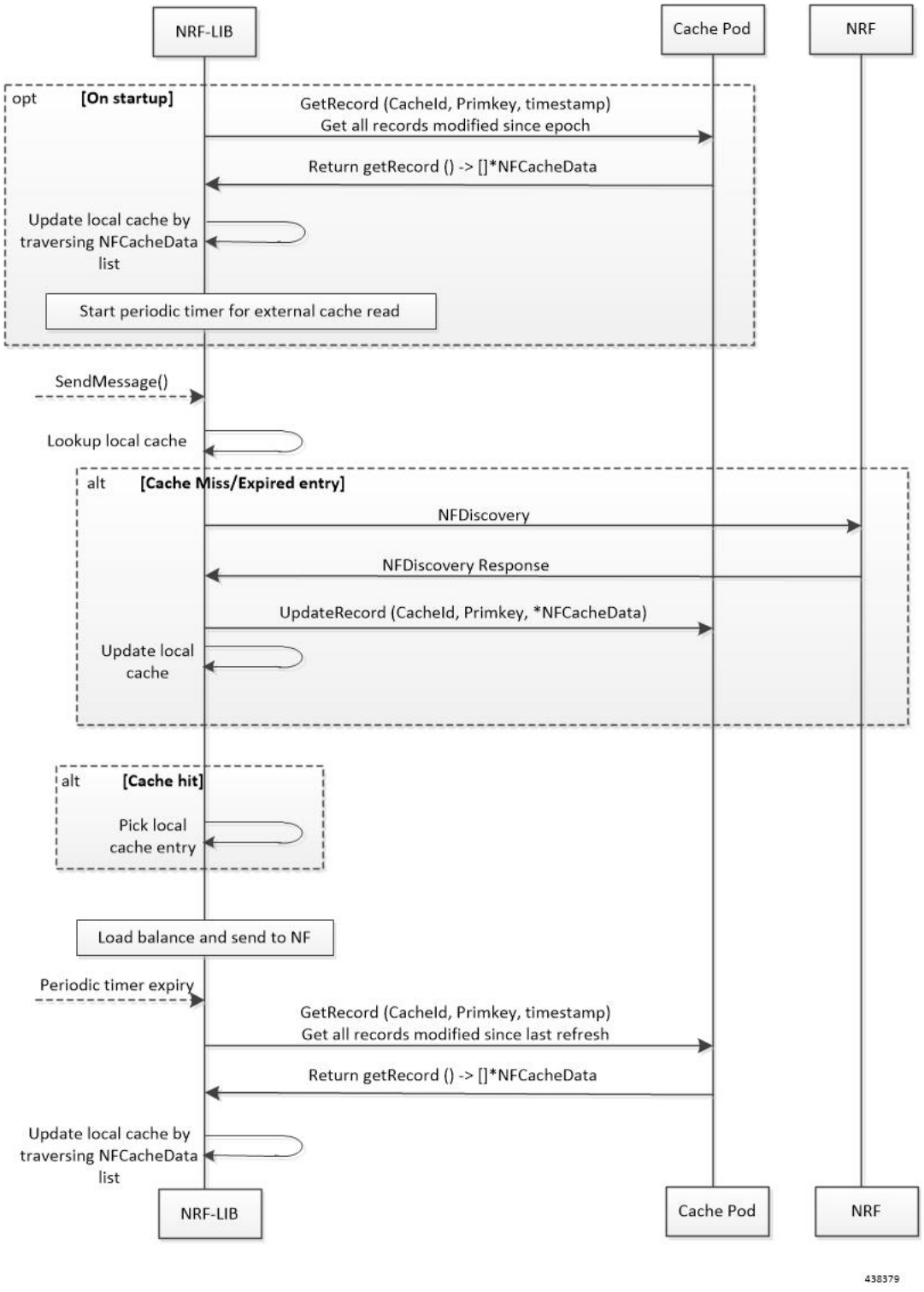


Table 115: Caching Support Call Flow Description

Step	Description
1	On Startup, NRF-LIB (in smf-rest-ep/SBI): **1.** Retrieves all the cache entries that were modified since epoch from cache-pod so that it can build the local cache. Once the local cache is built, the same cache is used in the sendmessage flow for lookup. **2.** A periodic refresh routine is initiated to refresh the local cache using the cache-pod.
2	Periodic Refresh, NRF-LIB (in smf-rest-ep/SBI): Local cache is periodically refreshed by getting all records from the cache-pod that were modified since last refresh. The resultant record list is traversed, and the local cache is updated.
3	Send Message NRF-LIB (in smf-rest-ep/SBI): **1.** When smf-rest-ep (SBI) triggers a send message (say to UDM), NRF-LIB looks up the local cache for the cache entry with the nfType and filter key: **a.** When a cache lookup miss occurs, a discovery query is sent to NRF to fetch NF profiles from NRF. If NRF responds with NF profiles, then these NF profiles are stored in a local cache and updated in cache-pod. **b.** On a successful lookup, the cached entry is used to send a message for endpoint selection. **2.** The NF profiles are load-balanced, and a message is sent to the selected endpoint.

Standards Compliance

The Caching Support for NF Discovery feature complies with the following standards:

- 3GPP TS 29.510, V15.2.0
- 3GPP TS 29.510, V15.0.0

Limitations

The Caching Support for NF Discovery feature has the following limitations:

- This feature only supports UDM, PCF, AMF discovery, and load-balancing.
- It does not support UPF discovery.
- It does not support Dynamic Configuration changes of NRF endpoints.
- It does not support Liveliness check of the NRF endpoints.
- NF Discovery is always attempted on primary host followed by the secondary and then tertiary host.

NRF Support for SMF Subscription and Notification

Feature Description

The SMF uses the NRF-provided Subscribe service to subscribe to NF status changes that the NF receives as a discovery response. This helps in updating the cached NF discovery responses.

The SMF honors only the notification changes in load, capacity, status at the NF level, and at the service level. It ignores all other parameter changes in the notification.

How it Works

The NRF Support for 5G-SMF Subscription and Notification feature uses the NF Subscribe service to subscribe to changes on the status of NF instances that the NF receives as discovery responses. The SMF sends a subscription for the response validity period for each of the NF profiles that it receives in the discovery response. The SMF checks if an existing NF instance subscription time needs an extension or not depending on the current response time validity. If a subscription needs an extension, a subscription PATCH is sent with the extended validity time.

During subscription, the NRF may respond with a modified validity time. This validity time might differ from the SMF validity time request. In such a scenario, the SMF tracks the required subscription time and the actual subscription time returned by the NRF.

The SMF periodically (every two minutes) checks in database if there is any subscription with the actual subscription time ending soon (as in next five minutes) but has required validity time more than the actual validity time. In this scenario, the SMF sends a PATCH subscription to extend the subscription validity time.

The SMF fills the Status Notification URI based on the interface NRF configuration that is specified in the configuration. The notification vip ip and vip port are used to frame the status notification URI.

```
http://{nrfinterface.vip-ip}:{ nrfinterface.vip-port}/{notifResourceURI}
```

On status notification, the SMF updates the local cache and the external cache (cache pod) with the changed attributes.

Call Flows

This section provides the call flows for this feature.

Subscription(PATCH) Call Flow

The NRF updates the subscription to notifications on NF Instances to refresh the validity time, when the specified time is due to expire. The SMF can request a new validity time to the NRF. The NRF can assign and provide a new validity time to the NF, if the operation is successful.

Updating the "subscriptionID" resource, initiates the Subscription(PATCH) operation. Issuing an HTTP PATCH request on the URI representing the individual resource, starts the operation.

Figure 91: Subscription to NF Instances in the Same PLMN

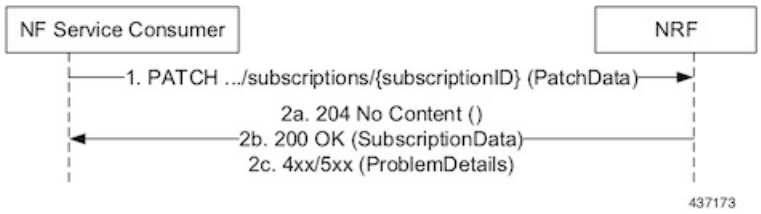


Table 116: Call Flow Description for Subscription to NF Instances in the Same PLMN

Step	Description
1	The SMF sends a PATCH request to the resource URI identifying the individual subscription resource. The payload body of the PATCH request contains a "replace" operation on the "validityTime" attribute of the SubscriptionData structure. The request also contains a new suggested value for the "validityTime" attribute. This replace operation does not replace any other attribute of the resource.
2a	When a subscription is successful, the NRF sends a "204 No Content" response. This indicates that the NRF accepts: • Extension of the lifetime of the subscription • Value of the "validityTime" attribute
2b	The NRF returns a "400 Bad Request" status code with the problem details if the subscription fails due to errors in the JSON Patch object in the request body.

2c	The NRF returns a "500 Internal Server Error" with the problem details if the subscription fails due to internal errors in the NRF.
	Example:
	`PATCH .../subscriptions/2a58bf47`
	`Content-Type: application/json-patch+json`
	`[`
	`{ "op": "replace", "path": "/validityTime", "value": "2018-12-30T23:20:50Z"`
	`},`
	`]`

Subscription(POST) Call Flow

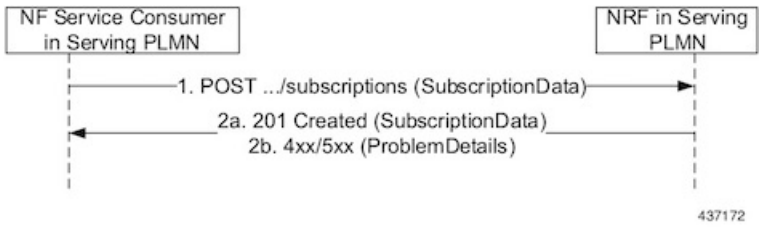
The Subscription service operation allows to:

- Create a subscription such that the SMF can request notification (depending on certain filters) in the following scenarios:
  - When there is a registration or deregistration in the NRF.
  - When there is a modification to a profile.
- Create a subscription to a specific NF instance such that the SMF can request notification in the following scenarios:

- When there is a modification to an NF instance.
- When there is a deregistration of an NF instance.

Important Currently, SMF only supports subscription of NF instances that the NF receives as its discovery response.

Figure 92: Subscription to NF Instances in the Same PLMN



Implementing the subscription to notifications on NF instances creates a new individual resource under the collection resource "subscriptions." Issuing a POST request starts the operation on the Uniform Resource Identifier (URI) representing the "subscriptions" resource.

Table 117: Call Flow Description for Subscription to NF Instances in the Same PLMN

Step	Description
1	The NF Service Consumer sends a POST request to the resource URI representing the "subscriptions" collection resource. The request body includes data that indicates the type of notifications that the SMF has subscribed to receive. It also contains a callback URI, where the SMF prepares to receive the actual notification from the NRF. The notification contains the SMF suggested validity time, which represents the time span during which the subscription remains active. The subscription request may also include more parameters indicating the list of attributes in the NF Profile to monitor (or to exclude from monitoring). This request determines if the NRF must send a notification, when there is a change in any of the attributes of the profile.
2a	When a subscription is successful, the NRF sends a "201 Created" response. This response contains newly created subscription data that includes the NRF-determined validity time beyond which, the subscription is invalid. When the subscription expires, the SMF creates a new subscription in the NRF to continue receiving status notifications.
2b	The NRF returns a "400 Bad Request" status code with the problem details if the subscription fails due to errors in the subscription data. The NRF returns a "500 Internal Server Error" with the problem details if the subscription fails due to internal errors in the NRF.

NFStatus Notify Call Flow

Issuing a POST request to each callback URI of the various subscribed NF Instances, initiates the NFStatus Notify operator.

Figure 93: Notification from NRF in the Same PLMN

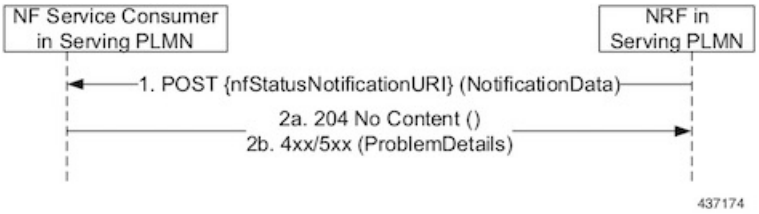


Table 118: Call Flow Description for Notification from NRF in the Same PLMN

Step	Description

1	The NRF sends a POST request to the callback URI.
	The request body for a profile change notification request includes the following:
	• **event**: This attribute indicates the notification type. It can be one of the following:
	  • NF_REGISTERED
	  • NF_DEREGISTERED
	  • NF_PROFILE_CHANGED
	• **nfInstanceUri**: Uniform Resource Identifier (URI) of the NF Instance associated to the notification event.
	• **nfProfile**: Indicates the new or updated NF profile.

2a	When the notification is successful, the NRF sends a "204 No content" response.
2b	The SMF returns a "404 Not Found" status code with the problem details if the SMF disregards the "nfStatusNotificationURI" as a valid notification URI. For example, if the URI does not belong to any of the existing subscriptions that the SMF has created in the NRF.

Limitations

In this release, the NRF Support for SMF Subscription and Notification feature has the following limitations:

- NF status notification supports only NF profile load, NF profile capacity, NF profile status, service load, service capacity, and service status parameter changes.
- SMF supports only the NFPofiile field in the "NotificationData." It does not support the "Change item" field.

Configuring NRF Support for SMF Subscription and Notification

This section describes how to configure the NRF Support for SMF Subscription and Notification feature.

Use the following commands to configure the NRF interface, vip-ip, vip-port, and loopback Port to open the server endpoints for the NF status notification.

```
configure
  endpoint sbi
    replicas integer
      vip-ip ip_address
        interface nrf
          vip-ip ip_address
          vip-port port_number
          loopbackPort port_number
          end
```

NOTES:

- **endpoint sbi**: Specifies the service-based interface (sbi) as the endpoint.
- **replicas**: Specifies the number of instances of the service-based interface.
- **vip-ip** *ip_address*: Specifies the virtual IP address of the virtual host.
- **interface nrf**: Specifies the interface as NRF.
- **vip-ip** *ip_address*: Specifies the virtual IP address of the virtual host. The SMF uses this as the listening IP address for the status notification.
- **vip-port** *port_number*: Specifies the port number of the virtual host. The SMF uses this as the listening port for the status notification.
- **loopbackPort** *port_number:*: Specifies the internal port number of the loopback host. The SMF uses this port for the NF status notification.

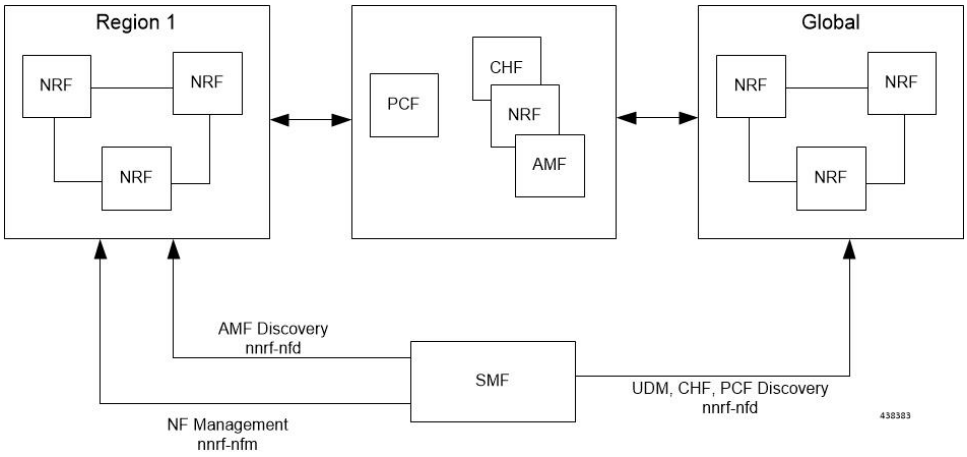
NRF Interface per Endpoint

Feature Description

The Network Repository Function (NRF) deployment can be logically segmented as global, regional, and so on, for a reliable network management. You can accomplish this segmentation by specifying different NRF endpoint groups for the discovery of different network functions. With associating a single NRF interface for each endpoint, the self-management of an NF improves the productivity.

For example, the SMF interacts with Region 1 NRF endpoints for management and AMF discovery. For UDM, CHF, and PCF discovery, the SMF communicates with the Global NRF endpoints.

Figure 94: NRF Deployment



Standards Compliance

The NRF Interface Per Endpoint feature complies with the following standards:

- 3GPP TS 29.510 V15.2.0 (2018-12)
- 3GPP TS 29.510 V15.0.0 (2019-06)

Limitations

The NRF Interface Per Endpoint feature has the following limitations:

- The NF discovery and load-balancing capabilities are available only for UDM, PCF, CHF, and AMF.
- The dynamic configuration changes of NRF endpoints is not available.
- Support for the liveliness check of the NRF endpoints is not available.
- The SMF attempts the NF discovery first on the primary host. In the absence of the primary host, SMF attempts the discovery on the secondary host and switches to the tertiary if both primary and secondary are unavailable.

Configuring the NRF Interface Per Endpoint

This section describes how to configure the NRF Interface Per Endpoint feature.

Configuring the NRF Interface Per Endpoint feature involves the following steps:

1. Associating a Discovery Group with NF Type
2. Configuring Locality for NF Types
3. Associating NRF Management and SMF Locality to NRF Endpoint
4. Configuring the NRF Group
5. Configuring Locality for SMF

6. Configuring NF Profiles for a DNN
7. Configuring Network Element Profile Parameters for the NF

Associating a Discovery Group with NF Type

Use the following CLI commands for pairing a discovery group with NF types.

```
configure
   profile nf-pair nf-type nf_type
     profile nf-pair nf-type nf_type nrf-discovery-group nrf_discovery_group_name

      end
```

NOTES:

- **nf-type** *nf_type*: Specifies the NF type. The *nf_type* can be: 5G_EIR, AF, AMF, AUSF, BSF, CHF, GMLC, LMF, N3IWF, NEF, NRF, NSSF, NWDAF, PCF, SEPP, SMF, SMSF, UDM, UDR, UDSF, UPF, or range.
- **nrf-discovery-group** *nrf_discovery_group_name*: Specifies the discovery group name.
- Discovery group is the logical link to the NRF endpoint groups (nrf-group). For each NF type, you can associate a discovery group and the locality information.

Configuring Locality for NF Types

The SMF provides locality aware NF discovery.

Use the following configuration to configure locality for NF types.

```
configure
   profile nf-pair nf-type nf_type locality { client client_name | geo-server
 geo_server_name | preferred-server preferred_server_name }
   end
```

NOTES:

- **client** *client_name*: Specifies the client locality information. Client locality is the SMF's locality and is a mandatory parameter.
- **geo-server** *geo_server_name*: Specifies the geo-server locality information. Geo-server locality is geo redundant site for the preferred locality and is generally used as the next best server locality after preferred locality, during NF discovery.
- **preferred-server** *preferred_server_name*: Specifies the preferred server locality information. Preferred server locality is the locality that should be considered as the locality of preference during the corresponding NF discovery.

Verifying the Association of the Discovery Group and Locality Configuration

This section describes how to verify the discovery group association and locality configuration for NF.

```
show running-config profile nf-pair
profile nf-pair nf-type UDM
```

```
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server PREF_LOC
 locality geo-server GEO
exit
```

Associating NRF Management and SMF Locality to NRF Endpoint

Use the following CLI commands for configuring NRF Management (nrf-group) and SMF Locality and associating them to NRF Endpoint.

```
configure
   group nf-mgmt mgmt_name
      nrf-mgmt-group nrf_group_name
      locality locality_name
      end
```

Verifying the Association of the NRF Management and SMF Locality to NRF Endpoint

This section describes how to verify the configuration that associates the NRF Management and SMF Locality to NRF Endpoint.

```
show running-config group nf-mgmt
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
```

Configuring the NRF Endpoints Profile Parameters

The SMF provides CLI for configuring NRF endpoints for different services that are supported by NRF, such as **nnrf-nfm** (NF management) and **nnrf-nfd** (NF Discovery).

Note For a discovery group, only the **nnrf-disc** service can be configured. For management service, only **nnrf-nfm** can be configured.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The SMF uses the priority and capacity parameters to load balance between these endpoints. Primary, secondary, and tertiary host [ip:port] can be configured within each endpoint. Both IPv4 and IPv6 address can be specified. If both are specified, then IPv4 address is preferred.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, its structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

" apiRoot " is a concatenation of the following parts: scheme ("http" or "https")

Note In this release of the specification, both HTTP and HTTPS scheme URIs are allowed. See 3GPP TS 33.501, Subclause 13.1 for further details on security of service-based Interfaces.

- the fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character. [api-root in CLI]

```
configure
   group nrf { mgmt mgmt_name | discovery discovery_name }
      service type nrf { nnrf-nfm | nnrf-disc }
         endpoint-profile epprofile_name
            priority priority_value
            capacity capacity
            api-root api_string
            api-uri-prefix uri_prefix_string
            uri-scheme { http | https }
            endpoint-name ep_name { capacity capacity | primary ip-address {
 ipv4 ipv4_address | ipv6 ipv6_address | port port_num } | secondary ip-address
{ ipv4 ipv4_address | ipv6 ipv6_address | port port_num } | tertiary ip-address
{ ipv4 ipv4_address | ipv6 ipv6_address | port port_num } }
            version [ uri-version version_num full version version_num ]
            end
```

NOTES:

- **api-root** *api_string* **:** Specifies the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string:* Specifies the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity:* Specifies the profile capacity.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }:** Specifies the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.
- **capacity** *capacity*: Specifies the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.
- The endpoint selection for sending the message is based on probabilistic load-balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
- **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specifies the primary endpoint IPv4 address, IPv6 address or port.
- **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specifies the secondary endpoint IPv4 address, IPv6 address or port.
- **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specifies the tertiary endpoint IPv4 address, IPv6 address, or port.
- **priority** *priority_value*: Specifies the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range of 0-65535.

- **uri-scheme { http | https }**: Specifies the URI scheme, as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specifies the api/Version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

Verifying the NRF Endpoints Profile Parameters

This section describes how to verify the configuration of the NRF Endpoints Profile Parameters.

```
show running-config group nrf
group nrf discovery udmdiscovery
 service type nrf nnrf-disc
  endpoint-profile epprof
   capacity       10
   priority       1
   api-uri-prefix nudm-sdm
   api-root       root
   uri-scheme     http
   version
    uri-version v1
     full-version 1.1.1.[1]
    exit
   exit
   endpoint-name endpointName
    priority 1
    capacity 100
    primary ip-address ipv4 231.1.1.1
    primary ip-address port 3021
   exit
  exit
 exit
exit
```

Configuring Locality for SMF

This section describes how to configure the locality for SMF.

This is a mandatory configuration if the SMF performs NF discovery using the NRF.

```
configure
   profile smf smf_profile_name
      locality value
      end
```

NOTES:

- **locality** *value*: Specifies the SMF locality. *value* must be an alphanumeric string representing the deployed SMF locality. By default, this CLI command is disabled.
- To disable this configuration, use the **no locality** *value* command.

Configuring NF Profiles for a DNN

This section describes how to configure the NF profile that the configured Data Network Name (DNN) uses.

```
configure
   profile dnn dnn_profile_name
```

```
network-element-profiles { amf | chf | pcf | udm } nf_profile_name
end
```

NOTES:

- **network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name*: Specifies one or more NF types such as AMF, CHF, PCF, and UDM as the network element profile. *nf_profile_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable this configuration, use the **no network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name* command.

Configuring Network Element Profile Parameters for the NF

This section describes how to configure the network element profile parameters for the configured NF.

```
configure
   profile network-element { { amf | chf | pcf | udm } nf_profile_name }
      failure-handling-profile profile_name
      nf-client-profile profile_name
     query-params { dnn | supi | tai | target-nf-instance-id | target-plmn
 }
      end
```

NOTES:

- **failure-handling-profile** *profile_name*: Specifies the NRF failure handling network profile for the configured NF type. *profile_name* must be an alphanumeric string representing the corresponding NRF failure handling network profile name.
- **nf-client-profile** *profile_name*: Specifies the local NF client profile. *profile_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | supi | tai | target-nf-instance-id | target-plmn }**: Specifies one of the following query parameters to include in the NF discovery request towards the NRF.
  - **dnn**: Specifies a DNN as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specifies a SUPI as the query parameter in the NF discovery request towards the NRF.
  - **tai**: Specifies a TAI as the query parameter in the NF discovery request towards the NRF.
  - **target-nf-instance-id**: Specifies a target NF instance Identifier as the query parameter in the NF discovery request towards the NRF.
  - **target-plmn**: Specifies a target PLMN as the query parameter in the NF discovery request towards the NRF.
  - **limit**: Specifies a limit for the maximum number of profiles that the NRF sends in the NF discovery response.
  - **max-payload-size**: Specifies the maximum payload size as the query parameter in the NF discovery request towards the NRF.

- **requester-snssais**: Specifies the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.

- This is an optional configuration. By default, these CLI commands are disabled.
- To disable this configuration, use the **no** variant of these commands. For example, **no nf-client-profile** CLI command.

Verifying the Local Configuration for the NRF Interface Per Endpoint

This section describes how to verify the configuration for the NRF Interface Per Endpoint feature.

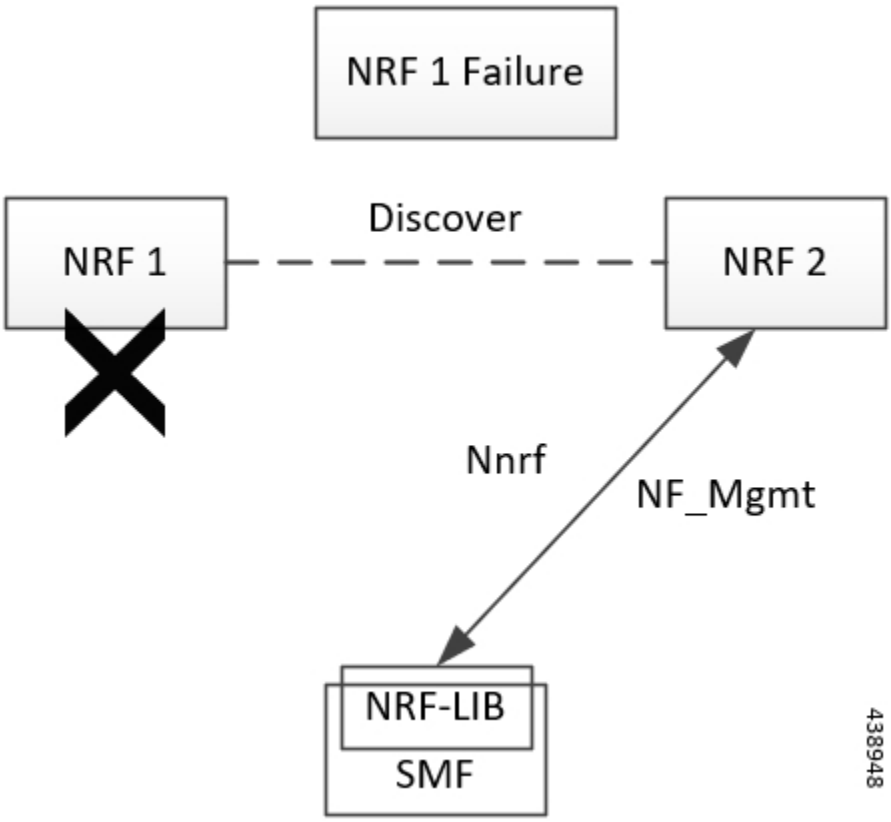
```
config
profile dnn cisco
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit

profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 127.0.0.1
 bind-port        8008
 fqdn             cisco.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end
```

NRF Failure Handling Support

Feature Description

The Network Repository Function (NRF) communication failure handling logic is implemented within the NRF client library. The NRF client library uses the NF registration messages for tracking the management NRF group operational status.

How it Works



In the preceding diagram, NRF 1 is Primary and NRF 2 is secondary for SMF. On bringing up, the SMF registers (NF registration) with NRF 1 and starts NF heartbeat with NRF 1. The SMF uses the heartbeat response to track the operational status.

In case, the SMF detects NRF 1 failure by missing NF heartbeat response, the SMF registers to NRF 2 (secondary NRF) and starts sending NF heartbeat. The SMF continues to send NF Register message1 to NRF 1 to keep track of its status.

If the SMF receives register response from NRF 1, it detects that the NRF 1 is up again. The SMF marks NRF 1 as active once it recovers and stops sending NF heartbeats to NRF 2.

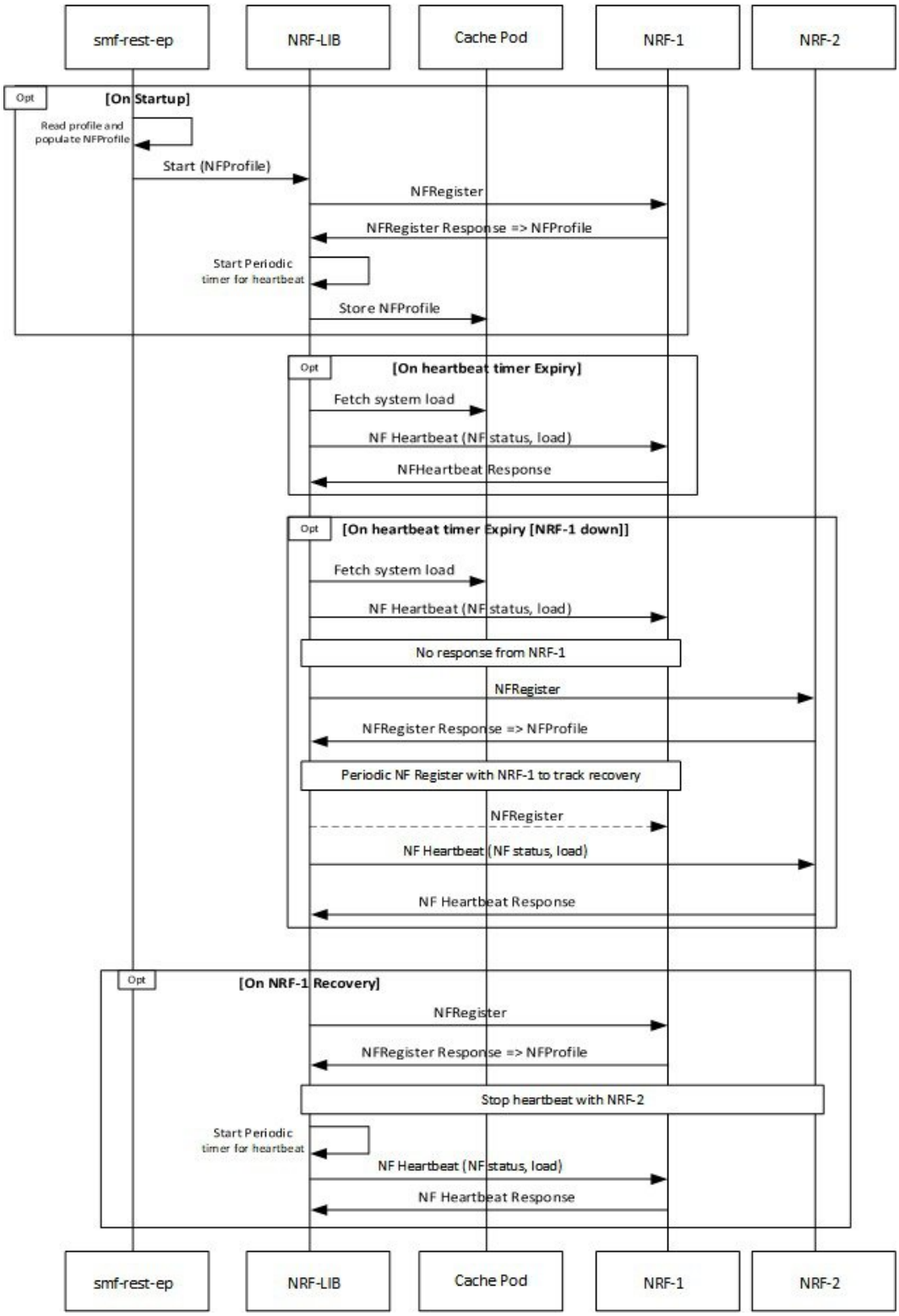
Note NF Reregistration (default behavior) on failover and fallback should be configuration driven. When NRF 2 detects that the SMF has stopped sending heartbeats, it checks from NRF 1 if it has received SMF registration by using discovery with SMF instance ID.

As the management and discovery endpoint groups are separate, the Registration based operation status check is not used for NRF failure handling during NF discovery. During NF discovery, the configured NRF endpoints within the group are attempted in the priority order. If the first choice NRF endpoint is not responding the next best NRF endpoint is chosen and so on.

Call Flow

The following diagram shows the basic NF management call flows covering the NF registration, NF management and the NRF failure handling.

Figure 95: NF Management Call Flow



Verifying the NRF Failure Handling

NF Management Failure Handling

Management NRF endpoint configuration sample is shown below.

```
product smf# show running-config group nf-mgmt
group nf-mgmt MGM
 nrf-mgmt-group mgmt_group
 locality       LOC1
exit
product smf# show running-config group nrf mgmt
group nrf mgmt mgmt_group
 service type nrf nnrf-nfm
  endpoint-profile epprof
   uri-scheme http
   endpoint-name EP1
    priority 2
    primary ip-address ipv4 10.105.227.219
    primary ip-address port 8082
    secondary ip-address ipv4 10.105.227.220
    secondary ip-address port 8082
   exit
   endpoint-name EP2
    priority 10
    primary ip-address ipv4 10.1.227.21
    primary ip-address port 8082
    secondary ip-address ipv4 10.1.227.22
    secondary ip-address port 8082
   exit
  exit
 exit
exit
product smf#
```

In the sample configuration, EP1 is the higher priority endpoint name as its priority is lesser than EP2 (2 against 10). So on bringing up, SMF sends NF registration to primary ip:port of EP1 [10.105.227.219:8082]. SMF uses secondary ip:port of EP1 if primary is down. SMF failovers to EP2 only if all ip:port of EP1 is down.

On successful registration with EP1 primary, SMF starts heartbeat with EP1 primary. If EP1 primary goes down, SMF detects the same by missing heartbeat response. On detecting EP1 primary down, SMF sends heartbeat to EP1 secondary [no reregistration]. Also, it periodically sends NF Heartbeat to EP1 primary to detect if it has recovered.

If SMF detects that EP1 primary and secondary is down, SMF failovers to EP2. When SMF failovers to EP2 primary, it sends reregistration (default behavior). It is assumed that all the endpoints with an endpoint name shares the database and so reregistration is only supported when failover is across endpoint names. In this case, EP1 primary and secondary shares the database. EP2 has a separate database and EP2 primary and secondary shares the database. On failover to EP2 primary, periodic NF registration is sent to primary of the EP1 only (to detect recovery).

Whenever a higher priority endpoint name is detected to be recovered, SMF falls back to the recovered IP:Port. For example, here the current active NRF endpoint is EP2 primary and SMF detects that EP1 primary has recovered, then SMF does reregistration with EP1 primary (default behavior) and stops heartbeat on EP2 primary.

Within endpoint NF heartbeat is used to track operational status. Across endpoints, registration is used to track the operational status. Message send timeout/RPC error and HTTP response codes 408, 429, 500, 501, 502, 503 are considered as failure to move to next NRF.

NF Discovery Failure Handling

Discovery NRF endpoint configuration sample is shown below.

```
product smf# show running-config profile nf-pair nf-type UDM
profile nf-pair nf-type UDM
 nrf-discovery-group others_group
 locality client LOC1
exit
product smf# show running-config group nrf discovery others_group
group nrf discovery others_group
 service type nrf nnrf-disc
  endpoint-profile ep1
   capacity 30
   priority 50
   uri-scheme http
   endpoint-name ED1
    priority 56
    primary ip-address ipv4 110.105.227.219
    primary ip-address port 8082
    secondary ip-address ipv4 110.105.227.220
    secondary ip-address port 8082
    exit
   endpoint-name ED2
    priority 10
    primary ip-address ipv4 110.1.227.21
    primary ip-address port 8082
    secondary ip-address ipv4 110.1.227.22
    secondary ip-address port 8082
   exit
  exit
 exit
exit
product smf#
```

In the sample configuration, ED1 has the higher priority endpoint name as its priority is lesser than ED2 (2 against 10). So, whenever there is a NRF discovery required primary ip:port of ED1 [110.105.227.219:8082] is attempted. SMF uses secondary ip:port of ED1 if primary is down. SMF failovers to ED2 only if all ip:port of ED1 is down. There is no state maintained regarding NRF discovery failure with any NRF endpoint. Every time SMF needs to send NRF discovery, SMF starts with ED1 primary and failovers to ED1 secondary in case of failure, followed by ED2 primary and so on.

Local Configuration for NF Management

Feature Description

The SMF learns about the other NF endpoints such as Unified Data Management (UDM), Access and Mobility Management Function (AMF), Policy Control Function (PCF), Charging Function (CHF) and so on, through NF discovery service exposed by Network Repository Function (NRF) or through the CLI configuration. The SMF prioritizes the NF discovery through the NRF. If the NRF is not available, then the SMF uses the local configuration of NF endpoints to discover the NFs.

Relationships

The Local Configuration for NF Discovery feature depends on the configuration of NRF endpoints, and the response from NRF. That is, the SMF uses the locally configured endpoints of the NFs only if the NRF endpoints remain unconfigured or if the NRF did not return any NFs matching the preferred server locality or geo locality.

For more information, see the NRF Interface per Endpoint, on page 391 section in this chapter.

Standards Compliance

The Local Configuration for NF Discovery feature complies with 3GPP TS 29.510, Versions 15.0.0 and 15.2.0.

Limitations

The Local Configuration for NF Discovery feature has the following limitations:

- Discovery and load balancing are available only for the UDM, PCF, CHF, and AMF but not for the UPF.
- Support for the liveliness check of the NF endpoints is currently not available.
- The SMF attempts the NF discovery first on the primary host. In the absence of the primary host, the SMF attempts the discovery on the secondary host and switches to the tertiary if both the primary and secondary are unavailable.

Configuring the NFs for NF Discovery

This section describes the Local Configuration for NF Discovery feature.

Configuring the NF for NF Discovery feature involves the following steps:

1. Configuring Locality for SMF
2. Configuring NF Profiles for a DNN
3. Configuring Network Element Profile Parameters for the NF
4. Configuring NF Client Profile
5. Defining Locality within NF Profile
6. Configuring NF Endpoint Profile Parameters

Configuring Locality for SMF

This section describes how to configure the locality for SMF. This is a mandatory configuration if the SMF performs the NF discovery using the NRF.

```
configure
   profile smf smf_profile_name
      locality value
      end
```

NOTES:

- **locality** *value*: Specifies the SMF locality. *value* must be an alphanumeric string representing the deployed SMF locality. By default, this CLI command is disabled.
- To disable this configuration, use the **no locality** *value* command.

Configuring NF Profiles for a DNN

This section describes how to configure the NF profile that the configured Data Network Name (DNN) uses.

```
configure
   profile dnn dnn_profile_name
      network-element-profiles { amf | chf | pcf | udm } nf_profile_name
      end
```

NOTES:

- **network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name* : Specifies one or more NF types such as AMF, CHF, PCF, and UDM as the network element profile. *nf_profile_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable this configuration, use the **no network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name*command.

Configuring Network Element Profile Parameters for the NF

This section describes how to configure the network element profile parameters for the configured NF.

```
configure
   network-element-profiles { { amf | chf | pcf | udm } nf_profile_name }
      failure-handling-profile profile_name
 nf-client-profile profile_name
     query-params { dnn | supi | tai | target-nf-instance-id | target-plmn
 }
      end
```

NOTES:

- **failure-handling-profile** *profile_name*: Specifies the NRF failure handling network profile for the configured NF type. *profile_name* must be an alphanumeric string representing the corresponding NRF failure handling network profile name.
- **nf-client-profile** *profile_name*: Specifies the local NF client profile. *profile_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | supi | tai | target-nf-instance-id | target-plmn }:** Specifies to include one of the following query parameters in the NF Discovery Request towards the NRF.
  - **dnn**: Specifies a DNN as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specifies a SUPI as the query parameter in the NF discovery request towards the NRF.

- **tai**: Specifies a TAI as the query parameter in the NF discovery request towards the NRF.
- **target-nf-instance-id**: Specifies a target NF instance Identifier as the query parameter in the NF discovery request toward the NRF.
- **target-plmn**: Specifies a target PLMN as the query parameter in the NF discovery request toward the NRF.
- **limit**: Specifies a limit for the maximum number of profiles that the NRF sends in the NF discovery response.
- **max-payload-size**: Specifies the maximum payload size as the query parameter in the NF discovery request towards the NRF.
- **requester-snssais**: Specifies the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.

- This is an optional configuration. By default, these CLI commands are disabled.
- To disable this configuration, use the **no** variants of these commands. For example, **no nf-client-profile** CLI command.

Configuring NF Client Profile

This section describes how to configure the NF endpoints for AMF, CHF, PCF, and UDM.

```
configure
   profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf
 pcf-profile | udm udm-profile } nf_profile_name }
   end
```

NOTES:

- **profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}**: Specifies the required NF client profiles and provides the local configuration for any of the following configured NFs:
  - **amf**: Enables the AMF local configuration
  - **chf**: Enables the CHF local configuration
  - **pcf**: Enables the AMF local configuration
  - **udm**: Enables the AMF local configuration

  For example, if you are configuring the **amf amf-profile** keyword, then this command enables the AMF local configuration. The same approach applies for the other configured NFs too.

  nf_profile_name must be an alphanumeric string representing the corresponding NF client profile name.

- You can configure multiple NF profiles within a given service.
- To disable this configuration, use the **no profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}** command.

Defining Locality within NF Profile

This section describes how to define the locality of the NF endpoints. For the NF endpoint selection, the SMF first considers the preferred locality that is configured with the **profile nf-pair** CLI command. The admin determines the preferred locality based on the proximity of the locality and the network function. The SMF then uses the geo-server locality configurations as the next preferred locality for the NF discovery. For information on the **profile nf-pair** command, see Configuring Locality for NF Types, on page 393 in the NRF Interface per Endpoint, on page 391 section.

The SMF selects the other locality endpoints if the **profile nf-pair** CLI command does not include the preferred server locality configuration, or if the **profile nf-client** CLI command does not include the endpoint configured with the preferred server or geo server locality. For the other locality endpoint selection, the SMF uses the **priority** configuration within the **locality** CLI command.

```
configure
   profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf
 pcf-profile | udm udm-profile } nf_profile_name }
     locality locality_name [ priority priority | service name type service_types
 { endpoint-profile epprofile_name } ]
      end
```

NOTES:

- **locality** *locality_name*: Specifies the locality of the NF endpoint. The SMF uses the locality configurations (that is, the preferred server locality and geo server locality) to select the appropriate NF endpoints.
- **priority** *priority*: Specifies the priority for the locality configuration.
- **service name type** *service_types*: Specifies the configured NF service types. The service types vary depending the configured service.

  The AMF service supports the following service types:

  - namf-comm
  - namf-evts
  - namf-loc
  - namf-mt

  The CHF service supports the following service types:

  - nchf-convergedcharging
  - nchf-spendinglimitcontrol

  The PCF service supports the following service types:

  - npcf-am-policy-control
  - npcf-bdtpolicycontrol
  - npcf-eventexposure
  - npcf-policyauthorization
  - npcf-smpolicycontrol

- npcf-ue-policy-control

The UDM service supports the following service types:

- nudm-ee
- nudm-pp
- nudm-sdm
- nudm-ueau
- nudm-uecm

- **endpoint-profile** *epprofile_name:* Specifies the endpoints at a per NF service level. The NF-specific services are available within the locality configuration.
- You can configure multiple endpoints per profile name for the configured NF.

Configuring NF Endpoint Profile Parameters

This section describes how to configure the NF endpoint profiles within the service, and its associated parameters.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The SMF uses the priority and capacity parameters to load balance between these endpoints. All endpoints under an endpoint profile share the session context. That is, when selecting an endpoint profile for initial message of a session, then the SMF sends the subsequent messages (for example, update, delete, and so on) of the session to any of the endpoints in the endpoint profile.

NRF Library (NRF-LIB) provides APIs to discover and send a message to an NF matching a set of filter parameters.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, its structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

" apiRoot " is a concatenation of the following parts:

- scheme ("http" or "https")
- the fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character. [api-root in CLI]

```
configure
   profile nf-client { nf-type { amf amf-profile | chf chf-profile |
pcf pcf-profile | udm udm-profile } nf_profile_name }
      locality locality_name [ priority priority | service name type
service_types ]
         endpoint-profile epprofile_name
            api-root api_string
            api-uri-prefix uri_prefix_string
```

```
            capacity capacity
           endpoint-name ep_name { capacity capacity | primary ip-address
 { ipv4 ipv4_address | ipv6 ipv6_address | port port_num } | secondary
ip-address { ipv4 ipv4_address | ipv6 ipv6_address | port port_num } | tertiary
 ip-address { ipv4 ipv4_address | ipv6 ipv6_address | port port_num } }
           priority priority_value
           uri-scheme { http | https }
           version [ uri-version version_num full version version_num ]
           end
```

Important In this release of the specification, both HTTP and HTTPS scheme URIs are allowed. See 3GPP TS 33.501 subclause 13.1 for further details on security of service-based interfaces.

NOTES:

- **api-root** *api_string* **:** Specifies the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string:* Specifies the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity:* Specifies the profile capacity.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**: Specifies the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.
  - **capacity** *capacity*: Specifies the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.

    The endpoint selection for sending the message is based on probabilistic load balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
  - **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specifies the primary endpoint IPv4 address, IPv6 address or port.
  - **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specifies the secondary endpoint IPv4 address, IPv6 address or port.
  - **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specifies the tertiary endpoint IPv4 address, IPv6 address or port.
- **priority** *priority_value*: Specifies the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range 0-65535.
- **uri-scheme { http | https }**: Specifies the URI scheme as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specifies the api/Version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

Verifying the Local Configuration for NF Discovery Feature

This section describes how to verify the Local Configuration for NF Discovery feature.

Use the following show command to verify the feature configuration details.

show running-config

The following is a sample output of this show command.

```
config
profile dnn cisco
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit


profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 127.0.0.1
 bind-port        8008
 fqdn             cisco.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end

profile nf-client nf-type udm
 udm-profile PROF1
  locality PREF_LOC
   priority 10
   service name type nudm-sdm
    endpoint-profile epprof
     api-uri-prefix nudm-sdm
     api-root       root
     uri-scheme     http
     version
      uri-version v1
       full-version 1.1.1.[1]
```

```
      exit
     exit
     endpoint-name endpointName
      priority 1
      capacity 100
      primary ip-address ipv4 231.1.1.1
      primary ip-address port 3021
     exit
    exit
   exit
  exit
 exit
exit
```

Fallback to Static IP Address Support

Feature Description

The SMF follows a priority order for the different NF selection options. It prioritizes the NF discovered from the network repository function (NRF) over the local configuration. The SMF uses the locally configured NFs in the following scenarios:

- When the NRF endpoints (for discovery) are not configured.
- When the NF discovery response has no valid NFs.

Depending on the deployment, the preferred server and geo locality server are configured for each of the NFs. The general rule is to select NFs in the preferred server locality followed by NFs in the geo locality server in case the preferred server NFs fail.

For each NF, the SMF provides an option to configure preferred and geo server locality [**profile nf-pair**]. For more details, see Configuring Locality for NF Types, on page 393 in the NRF Interface per Endpoint, on page 391 section.

In addition, each NF discovery response comes with associated validity time. The SMF caches this NF discovery response and uses it to fetch subsequent sessions. The SMF performs the NF discovery in the following conditions:

- The NF discovery response cache has no matching entries.
- The NF discovery response cache has matching entries, but the validity has expired.

Relationships

The Fallback to Static IP Address feature has functional relationship with the following features:

- NF Discovery, NF Selection, and Load Balancing
- NRF Interface Per Endpoint
- Caching Support for NF Discovery

How it Works

The SMF follows this sequence for NF selection:

1. It looks up the local cache (NF discovery response cache) for the NF
2. If the NF is a valid entry (not expired), it uses that entry. Else, SMF proceeds to Step 3.
3. The SMF reaches NRF for discovery [see, NRF Discovery (Priority 1)]. Else, SMF moves to Step 4.
4. If SMF cannot use the NRF for discovery, it uses the expired NF cache [see, Expired NF Cache (Priority 2)]. If expired NF cache is not available, SMF moves to Step 5.
5. If SMF does not find the NF in the local cache nor is it able to get it in the NRF discovery response, it uses the locally-configured NF [see, NF Local configuration (Priority 3)].

The priority order for NF selection is as follows:

1. **NRF Discovery (Priority 1)**

   The SMS uses the NRF-provided, NF discovery service to discover NFs like AMF, UDM, and PCF. The SMF sets the preferred locality as provided in the "**profile nf-pair**" configuration in the discovery query. (For more details about the "**profile nf-pair nf-type**" CLI configuration, see Configuring Locality for NF Types, on page 393 in the NRF Interface per Endpoint, on page 391 section.) For each NF, the query parameters are configurable. (For more details, see Configuring Network Element Profile Parameters for the NF, on page 397in the NRF Interface per Endpoint, on page 391 section) The NRF returns all the NFs matching the query criteria. When present, the NRF prefers NF profiles with a locality attribute that matches the preferred-locality. The NRF could return more NFs in the response, which are not matching the preferred target NF location. This occurs when there is no NF profile that is found matching the preferred target NF location. To avoid this, the NRF could set a lower priority for any additional NFs on the response not matching the preferred target NF location than those matching the preferred target NF location. The locality-aware NF selection logic of SMF is as follows:

   a. If the NF has both the preferred and geo locality server configurations, all the NFs in the response that are matching these are cached. SMF ignores the balance NFs. The load-balancing logic first selects the preferred locality NFs. If the preferred locality NFs fail, SMF picks the geo locality NFs for a retry. If N retry is allowed, N-1 retries are on the preferred locality and the last retry is on the geo locality NF. If the N-1 endpoints are unavailable in the preferred locality, SMF attempts all the endpoints of the preferred locality. Else, SMF picks up the geo locality endpoints for the remaining retries. Multiple retries on the same host (port) is not attempted.

   b. If the NF has only the preferred locality configuration, all the NFs in the response that match the preferred locality are cached. The load-balancing logic selects the endpoints from these NFs.

   c. If the NF does not have the preferred locality or geo locality configuration, then SMS caches all the discovery response NFs. The load-balancing logic selects from these NFs.

Note

- The load-balancing logic is based on priority, capacity, and load. The logic is similar to server selection as defined in IETF RFC 2782. But the weight is considered as "capacity * (100 - load)".
- If SMF selects the NRF-discovered NFs (in any of the three cases), even when all attempts to reach preferred and geo locality fail, the SMF does not fall back to the local configuration NFs for a retry.

2. **Expired NF Cache (Priority 2)**

   The SMF performs an NF discovery only in the following scenarios:

- If the matching entries are not present for the query filter in its NF discovery cache
- If matching entries are present in its NF discovery cache but the validities of these entries have expired

  The retention of an expired cache entry is configuration-based. If the expired cache entry is present and the NRF is not reachable or returns an error, then SMF uses the expired cache entry for NF selection. You can configure the SMF to control the cache entry usage with the following options:

  - Invalidate the cache entry on expiration of validity.
  - Use the invalidated cache entry for a configurable time period (timeout) and fallback to the static configuration after the timeout expires.

Note The SMF controls the cache entry usage - only when the NRF is down - through these options. The configurations are based on the **profile nf-pair**. Additionally, the SMF provides flexibility in configuring different cache usage rule for different NFs. For instance, the SMF always uses the expired cache to discover PCF when the NRF is down. But, for discovering the UDM, the SMF uses the expired cache for a timeout period of 10 milliseconds (ms) when the NRF is down.

3. **NF Local Configuration (Priority 3)**

   The locally configured NFs are the last option for NF endpoint selection. (For more details, see the Local Configuration for NF Management, on page 403 section.) The local configuration too considers the preferred and geo server locality for NF selection. The priority order is as follows:

   a. If the preferred server is configured for the NF [in **profile nf-pair**], SMF selects the NF endpoints under the preferred locality, first. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

   b. If the geo locality is configured for the NF [in **profile nf-pair**], SMF selects the NF endpoints under the geo locality as the fallback option. That is, if the preferred server locality NF endpoints fail or preferred server locality endpoints are not configured. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

   c. If the preferred server and geo locality server are not applicable, SMF picks up the locality based on the priority that is configured for each locality in the local NF configuration. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

Note The priority under locality is applicable only if the preferred and geo locality servers are not applicable.

The failure template is configurable for each of the NFs. Also, the message type in the template can set the retry count and action for the possible HTTP return codes. For a sample configuration, see the Configuring the Fallback to Static IP Address Support Feature, on page 414 section.

Standards Compliance

The Fallback to Static IP Address Support feature complies with the following standards:

- 3GPP TS 29.510 V15.2.0 (2018-12)
- 3GPP TS 29.510 V15.0.0 (2019-06)

Limitations

The Fallback to Static IP Address Support feature has the following limitation:

There is no support for dynamic configuration changes of NRF endpoints.

Configuring the Fallback to Static IP Address Support Feature

This section describes how to configure the Fallback to Static IP Address Support feature.

Configuring the Failure Template

This section describes how to configure the failure template.

```
configure
   profile nf-client-failure { nf-type { amf | chf | pcf | udm }
      profile failure-handling failure_handling_name
      end
```

NOTES:

- **profile nf-client-failure { nf-type { amf | chf | pcf | udm }**: Specifies the required NF client failure profile and provides the local configuration support for the following configured NF:
  - **amf**: Enables the AMF local configuration
  - **chf**: Enables the CHF local configuration
  - **pcf**: Enables the PCF local configuration
  - **udm**: Enables the UDM local configuration

    For example, if the NF type that is selected is **udm**, then this command enables the UDM local configuration. The same approach applies for the other configured NFs.

- **profile failure-handling** *profile_name*: Specifies the failure handling profile name. For example, "udmFail".

Sample Configurations

The following is a sample configuration of the failure template mapping to dnn:

```
profile dnn cisco
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
```

```
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit
```

The following is a sample configuration of the failure template mapping to smf:

```
profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 127.0.0.1
 bind-port        8008
 fqdn             cisco.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end
```

For more information, see Configuring NF Profiles for a DNN, on page 396 in the NRF Interface per Endpoint, on page 391 section.

Configuring NF Service and Message Type

This section describes how to configure the NF service and its different message types.

```
configure
  profile nf-client-failure { nf-type { amf | chf | pcf | udm }
     profile failure-handling failure_handling_name
        service name type service_type
          message type message_type
          end
```

NOTES:

- **service name type** *service_type*: Specifies the configured NF service types and provides the local configuration support for the following configured NF. The service types vary depending on the configured service.

  The AMF service supports the following service types:

  - **namf-comm**
  - **namf-evts**

- **namf-loc**
- **namf-mt**

The CHF service supports the following service types:

- **nchf-convergedcharging**
- **nchf-spendinglimitcontrol**

The PCF service supports the following service types:

- **npcf-am-policy-control**
- **npcf-bdtpolicycontrol**
- **npcf-eventexposure**
- **npcf-policyauthorization**
- **npcf-smpolicycontrol**
- **npcf-ue-policy-control**

The UDM service supports the following service types:

- **nudm-ee**
- **nudm-pp**
- **nudm-sdm**
- **nudm-ueau**
- **nudm-uecm**

For example, if the *service_type* that is selected is **nudm-sdm**, then this command enables the UDM local configuration. The same approach applies for the other configured NFs.

- **message type** *message_type*: Specifies the configured NF message type and provides the local configuration support for the following configured NF.

  The message types are varied depending on the configured profile and service type.

The following example provides a sample of the configured profile, service, and message type options.

Profile	Service Type	Message Type Options
amf	namf-comm	• AmfCommEBIAssignment • AmfCommN1N2MessageTransfer • AmfCommSMStatusChangeNotify • range

Profile	Service Type	Message Type Options
chf	nchf-convergedcharging	• ChfConvergedchargingCreate • ChfConvergedchargingDelete • ChfConvergedchargingUpdate • range
pcf	npcf-am-policy-control	• PcfSmpolicycontrolCreate • PcfSmpolicycontrolDelete • PcfSmpolicycontrolUpdate • Range
udm	nudm-sdm	• UdmRegistrationReq • UdmSdmGetUESMSubscriptionData • UdmSdmSubscribeToNotification • UdmSubscriptionReq • UdmUecmRegisterSMF • UdmUecmUnregisterSMF • UdmSdmUnsubscribeToNotification • range

Note The example does not cover all the message options that are provided for each profile and service type.

Configuring NF Failure Retry, Action, and Message Type

This section describes how to configure the failure retry and action for each service of the NF and its different message types.

```
configure
   profile nf-client-failure { nf-type { amf | chf | pcf | udm }
   profile failure-handling failure_handling_name
      service name type service_type
         message type message_type
            status-code httpv2 { integer }
            retry integer
            action { continue | retry-and-continue | retry-and-terminate
 | terminate }
            end
```

NOTES:

- **status code httpv2 {** *integer* **}**: Specifies the status code for the retry and action for the NF service. Currently only "http" status code is provided. *integer* specifies the status code. *integer* must be an integer in the range of 300-599.
- **retry** *integer*: Specifies the number of times the NF service must retry before proceeding with the action.
- **action**: Specifies the action. The different actions supported are:
  - **continue**: Specifies to continue the session without any retry. The retry count configuration is invalid with this action.
  - **retry-and-continue**: Specifies to retry as per the configured retry count and continue the session.
  - **retry-and-terminate**: Specifies to retry as per the configured retry count and terminate the session in case all retry fails.
  - **terminate**: Specifies to terminate the session without any retry. Retry count configuration is invalid with this action.

    The retry and action for a message send is picked based on the first send status code failure. A different status code in the retry does not lead to picking a new retry count and action.

Configuring Invalidate (Purge) NF Discovery Cache

This section describes how to configure the cache entry invalidation (purge) for the NF discovery cache.

```
configure
   profile nf-pair nf-type { amf | chf | pcf | udm }
      cache invalidation { false | true [ timeout integer ] }
        end
```

NOTES:

- **cache invalidation { false | true [timeout** *integer* **] }** : Configures the interval and cache invalidation rule. The default value is false.
  - **false** : Specifies that the cache entry will never be invalidated.
  - **true timeout** *integer* : Specifies that the cache entry will be invalidated. **timeout** *integer* specifies the time period in milliseconds (ms) for controlling the usage of the expired cache entry (when NRF is unreachable). The default value is 0 ms.

The following is a sample configuration that sets the cache invalidation to false for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation false
 end
```

The following is a sample configuration that sets the cache invalidation to true for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation true timeout 10
 end
```

NF Profile Update

Feature Description

The SMF invokes NF Update service operation when there are changes to the NF registration parameters due to the SMF profile configuration change.

NF Update service updates the profile of NF that was previously registered in the NRF by providing the updated profile of the requesting NF to the NRF. The update operation could be a whole NF profile update (complete replacement of the existing profile with a new profile), or an update to only a subset of the NF profile parameters (including adding, deleting, or replacing services to the NF profile).

Standards Compliance

The NF Profile Update feature complies with the 3GPP TS 29.510, V15.2.0 (2018-12).

Limitations

The SMF currently supports only the complete replacement of NF profile.

How it Works

The following figure illustrates a call flow representing the complete NF profile replacement.

Figure 96: NF Profile Complete Replacement

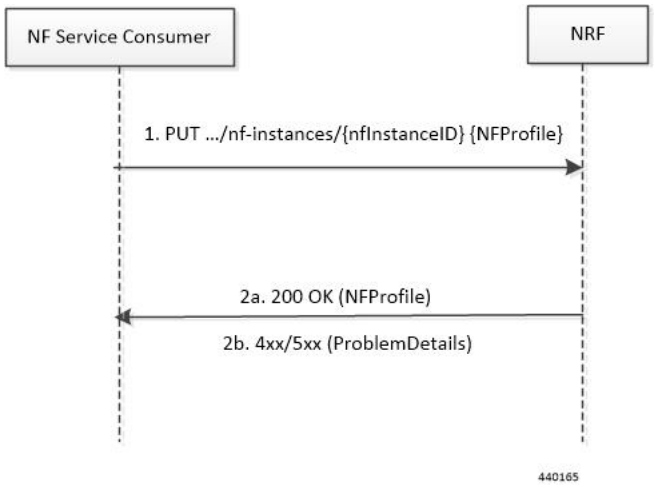


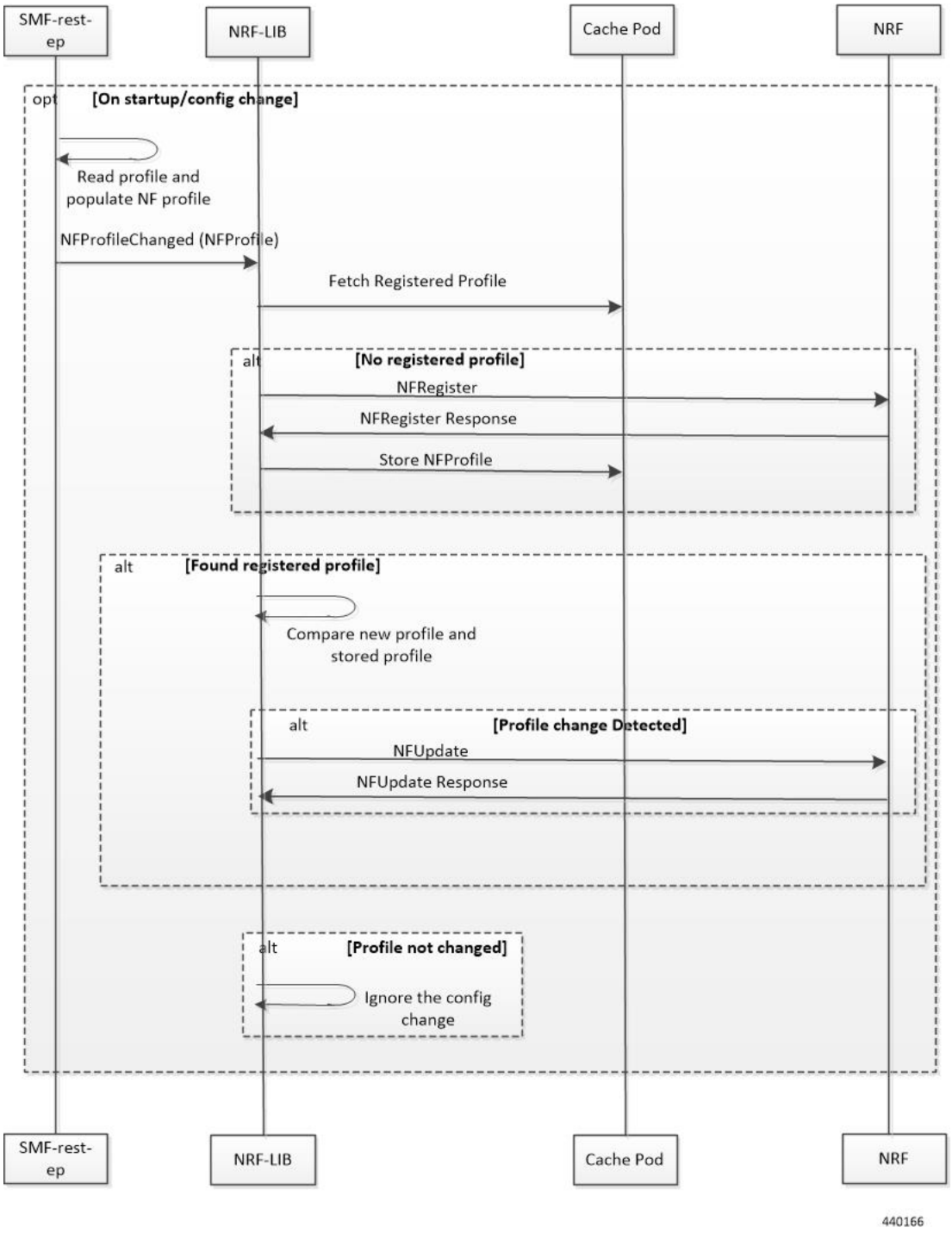
Table 119: NF Update Call Flow Description

Step	Description
1	The NF Service Consumer sends a PUT request to the resource URI representing the NF instance. The payload body of the PUT request contains an update operation on the NF Profile of the NF instance

Step	Description
2a	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body.
2b	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF database, the NRF returns 4xx or 5xx status code with the ProblemDetails IE providing details of the error.

The following figure illustrates the call flow representing the NF registration and NF update messaging from NRF client library on NF profile change trigger from SMF-rest-ep.

Figure 97: NF Registration and NF Update Call Flow



1. The SMF rest-ep, on start-up, reads the SMF profile configuration and accordingly populates the NF management Profile. The rest-ep then triggers NRF-LIB to indicate the NF Profile change.
2. NRF library (NRF-LIB) maintains the NF registration status and the registered profile in an external cache pod. The NRF client detects whether the NF registration with NRF is completed. If the NRF client detects

that the registration is not completed during NF profile change handling, perform Step 3. If the NF registration is complete, perform Step 4.

3. The NRF-LIB sends NF Register to NRF. It allows an NF Instance to register its NF profile in the NRF. It includes the registration of the general parameters of the NF Instance along with the list of services exposed by the NF Instance.
4. NRF-LIB fetches the registered NF profile and then compares it with the new profile.
5. The NRF-LIB NF sends NF update (PUT) request to the NRF when any of the parameters in the NF management profile changes due to SMF profile configuration change.
6. The NRF-LIB ignores the trigger if there is no change detected.

Important The NF update is sent only from the elected master.

Load parameter is not set as part of NF update PUT message. Heartbeat is set as the current active heartbeat interval.

Configuration Support for List of Tracking Areas and Tracking Area Ranges

Feature Description

The SMF provides an optional configuration to configure the supported list of Tracking Areas and Tracking Area Ranges for a Public Land Mobile Network (PLMN). When a new configuration is present, the SMF sends the configured Tracking Area Identity (TAI), that is, TAIList and TAIRangeList, to the Network Function (NF) Repository Function (NRF) during the SMF Service Registration.

Important Any change in the configuration results in SMF Service update towards the NRF with the new configured TAIList and TAIRangeList values.

The PLMN value sent in the NRF discovery message remains the same as the PLMN configured on the SMF.

For more details on the NF Registration and NF Registration Update, see the NF Profile Update, on page 419 section.

Configuring TAI Group

This section describes how to configure the TAI Group.

Configuring TAC List

Use the following configuration to configure the TAC list within TAI profile.

```
configure
   profile tai-group tai_group_name
      mcc mcc_value mnc mnc_value
      tac list [ tac_list_values ]
      end
```

NOTES:

- **tac list [** *tac_list_values* **]**: Configures the list of TAC values. For example, [1111 2222 3333]

Configuring TAC Range List

Use the following configuration to configure the TAC range list within TAI profile.

```
configure
   profile tai-group tai_group_name
      mcc mcc_value mnc mnc_value
      tac range start start_value end end_value
      end
```

NOTES:

- **tac range start** *start_value* **end** *end_value*: Configures a specific TAC range or multiple TAC range lists. For example, **tac range start DDDD end EEEE**

  You can configure a maximum of 16 values in a range.

- Use the **no tac range start** *start_value* **end** *end_value* command to remove a specific TAC range or TAC Ranges.

Verifying the TAI Group Configuration

Use the following show command to verify the TAI group configuration.

```
show running-config profile tai-group tai_group_name
```

The following is an example of the **show command** configuration.

```
show running-config profile tai-group t1
profile tai-group t1
mcc 111 mnc 222
  tac list [ 1111 2222 3333 ]
  tac range start 4444 end 5555
  exit
exit
mcc 333 mnc 44
  tac list [ AAAA BBBB CCCC ]
  tac range start DDDD end EEEE
  exit
exit
exit
```

Dynamic Configuration Change Support

Feature Description

Global configuration table was built for NRF configurations and rebuilt each time when there was a change in configuration. NRF transaction/procedure (such as discovery, management, and so on) picked the configuration for the respective transaction/procedure from the global configuration tables. Therefore, the ongoing transactions were impacted if the configurations were modified in the middle of the transaction/procedure.

With this feature:

- NRF transaction/procedure picks a configuration version (v1) and uses the same version till the NRF transaction/procedure complete.
- If a user changes the configuration during an ongoing NRF transaction, then a new configuration version (v2) is created. However, the new configuration is not applied to the ongoing transaction.

The dynamic configuration changes are for the following data structures:

- NrfFailureProfileSt
- NrfClntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

NRF Show Command Enhancements

show nrf registration-info

Field	Description
NF Status	Displays NRF Registration Information.
Registration Time	Displays Time of Registration with NRF.
Active MgmtEP Name	Active NRF Management End Point name.
Heartbeat Duration	Displays Heart Beat Duration.
Uri	Displays Uri Information.
Host Type	Displays NRF Host Type Information.

show nrf subscription-info

Field	Description
NF Instance Id	Displays NF instance Identity.
SubscriptionID	Displays the Subscription Identity information.
Actual Validity Time	Displays Actual Validity Time received from NRF server.
Requested Validity Time	Displays NF Requested Validity subscription Time.

show nrf discovery info

Field	Description
NF Type	Displays NF Type Information.

show nrf discovery-info AMF discovery-filter

Step	Description
Discovery Filter	Displays Discovery Filter Information.
Expiry Time	Displays Expiry Time for discovery Filter.

shownrfdiscovery-infoAMFdiscovery-filterdnn=intershatnf-discovery-profile

show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile

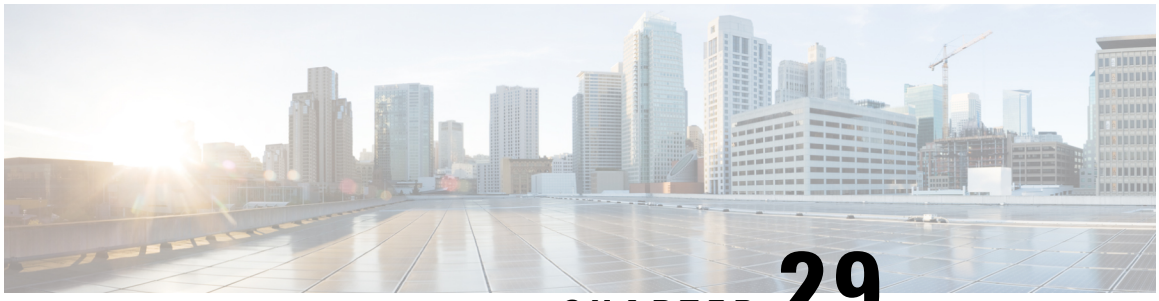
Field	Description
NF InstanceId	Displays the NF Instance Identity.
NF Type	Displays the NF Type Information.
Discovery Filter	Displays the Discovery Filter Information.
NF Status	Displays the NF Status Information.
Priority	Displays the Priority Information.
Capacity	Displays the NF Profile Capacity Information.
Load	Displays the Load Information.
Locality	Displays the Locality Information.
ipv4 address	Displays IPv4 Address received from the discovery response for this NF profile.

Field	Description
ipv6 address	Displays the IPv6 Address received from the discovery response for this NF profile.

shownrfdiscovery-infoAMFdiscovery-filterdnn=intershatnf-discovery-profile f9882966-a253-32d1-8b82-c785b34a7cc9 nf-service

show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile f9882966-a253-32d1-8b82-c785b34a7cc9 nf-service

Field	Description
ServiceInstanceId	Displays the NF Service Instance ID.
ServiceName	Displays the NF Service Name.
UriScheme	Displays the Uri Scheme Information.



CHAPTER 29

Peer NF Failure Handling Support

Feature Summary and Revision History

Summary Data

Table 120: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 121: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Offline Failover Support for Charging

Feature Description

The SMF supports offline failover for charging when a CHF server fails. When the SMF continues after the CHF server failure, the SMF relays the offline charging services to the offline CHF server.

How it Works

The offline failover support for the charging feature works as follows.

Selecting a CHF Server

The CHF server selection involves the following steps:

1. The smf-service sends packets to rest-ep. The NF library of rest-ep attempts to search a CHF server through NRF discovery. This library receives a CHF server IP address or the list along with the priority as a search result.
2. The NF library selects the CHF server based on the priority from the list that is received through NRF discovery. If no CHF server is selected, NF library falls back to the static configuration that exists in the CHF network profile.

After selecting a CHF server or a list, NF library relays the message to the first CHF server according to the priority.

Handling a CHF Server Failure

The CHF server failure occurs when the selected CHF sends failure response or sends no response. For a CHF server failure, the NF library sends status code that is based on the failure template. This template is associated with the CHF network profile. The smf-service sends the profile information to smf-rest-ep while sending the IPC message.

The failure template is configured with the list of HTTP error codes and the associated failure actions and retry count, as required. Following are the failure actions as available in the feature template for this feature:

- Retry and Continue—For this failure action, NF library attempts until the configured number of times before fallback. After the configured number of times completes, the NF library falls back to the lower priority CHF server IP address. If the failure or no response is received from CHF server, the "continue" action is returned to the smf-service.
- Terminate—For this failure action, NF library does not attempt to send message to other CHF servers. The library sends a reply to smf-service with the action as "terminate". For the "terminate" failure action, the smf-service deletes the session.
- Continue—For this failure action, the smf-service continues the session and sends the charging message to the offline CHF server. This server is configured as part of the local static CHF profile that is meant for the offline purpose. In addition, the failure handling profile for offline CHF is configured.

NOTE: For the "continue" failure action, you must configure the offline CHF server at SMF in a separate profile. SMF will use this profile after the CHF server failure. If the offline CHF server is not confgured, the session is continued without imposing any charging.

Relaying to an Offline CHF Server

After CHF server failure, when the SMF continues, it converts the ongoing charging services as follows:

- Converts the services with both online and offline charging method to the offline charging method.
- Converts the services with online charging method to the offline charging method.
- Makes no change for the services with the offline charging method.

HTTP Cause Code Mapping with Failure Actions

Following table lists the mapping of failure actions with the associated HTTP cause code. Based on the network requirements, you can change the mapping.

Table 122: HTTP Cause Code Mapping with Failure Actions

Http-2 Cause Codes and Description		Converged CHF Failure Action			Offline CHF Failure Actions		
Code	Description	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
400	Bad Request	Terminate	No config	No config	Terminate	No config	No config
403	Forbidden	Terminate	No config	No config	Terminate	No config	No config
404	Not found	Terminate	No config	No config	Terminate	No config	No config
405	Method Not allowed	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	No config	No config
408	Request Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
500	Internal Server Error	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
503	Service Unavailable	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
508	Gateway Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
0	No reply from server	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue

SMF Behaviour for Failure Actions

The following table describes the SMF behaviour on receiving different failures (Continue, Ignore, and Terminate) in CDR-(I/U/T).

CHF Failure Actions	Converged CHF			Offline CHF		
	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
Continue	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF if offline CHF is configured	Continue the session without charging	Continue the session without charging	Continue the session deletion
Terminate	Delete the session	Delete the session	Continue the session deletion	Delete the session	Delete the session	Continue the session deletion
Ignore	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion

Standards Compliance

The offline failover support for charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290
- 3GPP TS 32.291

Limitations

The offline failover support for charging feature has the following limitations:

- Session Level Limits are mandatory from CHF or you must configure them locally. As per the 3GPP specification, the last linked URR cannot be removed when online URR needs to be delinked from the offline URR.

Configuring the Offline Failover Support for Charging

This section describes how to configure the offline failover support for charging feature.

Configuring the offline failover support for charging feature involves the following steps:

1. Configure failure handling profile in an NF library
2. Configuring an offline server client and an offline failure handling profile

Configuring Failure Handling Profile in an NF Library

This section describes how to configure the failure handling profile in an NF library.

Use this CLI configuration to configure the failure handling profile. You can configure HTTP status code with the corresponding action for the CHF create, update, or release messages. Based on the configuration of the failure handling profile, NF library takes an action when the CHF server failure occurs.

```
configure
   profile nf-client-failure nf-type chf_name
     profile failure-handling profile_failure_handling_name
 service name type service_name_type
       message type message_type_value
       status-code status_code_value
       action failure_action_value
       exit
```

NOTES:

- **profile nf-client-failure nf-type** *chf_name*—Enter the name of the network function that is required after the NF client failure.
- **profile failure-handling** *profile_failure_handling_name*—Enter the name of the profile for failure handling.
- **service name type** *service_name_type*—Enter the name of the service type.

  service_name_type : nchf-convergedcharging
- **message type** *message_type_value*—Enter the value for type of message.*message_type_value* can be one of the following values:
  - ChfConvergedchargingCreate
  - ChfConvergedchargingUpdate
  - ChfConvergedchargingDelete
- **status-code** *status_code_value*—Enter the status code as per the configured failure template. *status_code_value* can be one of the following values:
  - 500
  - 400
  - 404
- **action** *failure_action_value*—Enter the value for the failure action as per the configured failure template. *failure_action_value* can be one of the following values:
  - continue
  - terminate
  - retry-and-continue
  - retry-and-terminate
  - retry-and-ignore

Configuring an Offline Server Client and an Offline Failure Handling Profile

This section describes how to configure the offline server client and offline failure handling profile.

Use this CLI to configure the offline client profile and offline failure handling profile for the selected CHF server.

```
configure
   profile network-element chf chf_name
      nf-client-profile nf_client_profile_name
      failure-handling-profile failure_handling_profile_name
      query-params [ dnn ]
      nf-client-profile-offline nf_client_profile_offline_IP_port_number
      failure-handling-profile-offline failure_handling_profile_offline_name
      exit
```

NOTES:

- profile network-element chf – Enter the name of the CHF server.
- nf-client-profile – Enter the name of the client profile.
- failure-handling-profile – Enter the name of the failure handling profile.
- query-params – Enter the query parameter value, which is the data network name.
- nf-client-profile-offline – Enter the name of the offline client profile.
- failure-handling-profile-offline – Enter the name of the offline failure handling profile.

SMF Failover to Secondary PCF

Feature Description

The NF failover support is available in the SMF using the NRF Client profile configuration and the NRF failure profile configuration. The following functionality is supported:

- Configure multiple endpoints for a service as primary and secondary endpoints.
- Specify the failure behavior based on:
  - Message Type
  - HTTP Status Codes in the response messages

SMF Functionality

The SMF utilizes the NF Failover to achieve the PCF failover support functionality. This section covers working of SMF for message-level failures handling and the corresponding HTTP Status Code-based failure.

The SMF PCF failover supports the following messages that are initiated from the SMF.

- PcfSmpolicycontrolCreate

- PcfSmpolicycontrolUpdate
- PcfSmpolicycontrolDelete

During the PDU session lifecycle, the SMF exchanges the preceding messages at various stages with the PCF. Depending on the HTTP Status code configured in the NRF failure profile, the SMF receives one of the following actions:

- Ignore
- Continue
- Terminate

Table 123: Relationship between SMF PCF Failover Messages and Actions

	PcfSmpolicy controlCreate	**PcfSmpolicy controlUpdate**	**PcfSmpolicy controlDelete**
Ignore	Continue with locally configured/UDM-provided policy parameters. **Note** Do not contact PCF for subsequent messages. **PCF-Interaction Status: OFF**	Continue with 'currently available snapshot' of policy parameters. Contact PCF for subsequent messages. **PCF-Interaction Status: ON**	Current failure ignored. Session is deleted. **PCF-Interaction Status: Session deleted**
Continue	Continue with locally configured/UDM-provided policy parameters. **Note** Do not contact PCF for subsequent messages. **PCF-Interaction Status: OFF**	Continue with 'currently available snapshot' of policy parameters. **Note** Do not contact PCF for subsequent messages. **PCF-Interaction Status: OFF**	Current failure ignored. Session is deleted. **PCF-Interaction Status: Session deleted**
Terminate	Terminate the session.	Terminate the session.	Terminate the session.

Note The messages in Table 123: Relationship between SMF PCF Failover Messages and Actions, on page 433 are SMF-initiated messages.

SMF PCF Failure Handling

- **PCF-Interaction Status: ON**

SMF-initiated messages: The SMF continues to initiate the messages towards the PCF whenever the criteria is met.

PCF-initiated messages: The SMF continues to accept all the messages initiated from the PCF towards the SMF.

- **PCF-Interaction Status: OFF**

  SMF-initiated messages: The SMF does not initiate or send the messages towards the PCF whenever the criteria is met. The SMF treats the PCF as if it is not available and continues further actions.

  PCF-initiated messages: There are two messages initiated by the PCF.

  - SmPolicyUpdateNotifyReq: On receiving this message, the SMF sends a 404 error code in response and cleans up the session and does not send the Delete Request to the PCF.

    Note The SMF also sends FIVEGSM_CAUSE value as **REACTIVATION REQUESTED** in the FIVEG_PDU_SESSION_RELEASE_COMMAND to UE for 5G. In case of 4G, the SMF sends cause **REACTIVATION REQUESTED** in DELETE BEARER REQUEST message to the S-GW.

  - SmPolicyAssociationTerminationReq: On receiving this message, the SMF sends a success response and cleans up the session. As part of this interaction, the SMF sends a Delete Request to the PCF.

    Note This is an exception when the PCF-Interaction Status is set to OFF.

Configuring SMF Failover to Secondary PCF Support

Use the following configuration to configure the PCF failure handling profile with action config:

```
profile nf-client-failure nf-type pcf
 profile failure-handling FH1
  service name type npcf-smpolicycontrol
   message type PcfSmpolicycontrolCreate
    status-code httpv2 0
     action continue
```

Use the following configuration to configure the association of FH profile in the respective network element:

```
profile network-element pcf pcf1
 nf-client-profile PP1
 failure-handling-profile FH1
 query-params [ dnn ]
 rulebase-prefix cbn#
 predefined-rule-prefix crn#
exit
```

Use the following configuration to configure secondary and tertiary IP addresses:

```
profile nf-client nf-type pcf
 pcf-profile PP1
  locality LOC1
   priority 30
   service name type npcf-smpolicycontrol
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 primaryipaddress
      primary ip-address port 8098
      secondary ip-address ipv4 secondaryipaddress
      secondary ip-address port 9098
      end
```

Statistics

The following statistics are added in support of SMF Failover to Secondary PCF feature.

- PcfSmpolicyControlCreate
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- PcfSmPolicyControlUpdate
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- PcfSmpolicyControlDelete
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- PolicyUpdateNotifyReq
  - Number of accepted requests
  - Number of rejected requests
  - Number of skipped requests
- PolicyDeleteReq
  - Number of accepted requests
  - Number of rejected requests

    - Number of skipped requests

- PolicyUpdateRequest
    - Number of accepted requests
    - Number of rejected requests
    - Number of skipped requests

- Gauge counter for number of subscribers with policy type local/pcf.

UPF Failure Handling

Feature Description

During a session, if the User Plane function (UPF) is in congested state, it rejects the Packet Forwarding Control Protocol (PFCP) establishment messages from SMF with a cause code in the response message. To reduce the call loss, SMF retries to send PFCP establishment messages to a different UPF. Then, SMF selects a UPF based on priority (configuration) and capacity (load information from UPF).

The UPF failure handling support on N4 interface feature in SMF introduces a new failure handling template (FHT) profile for PFCP. This profile is associated with the UPF profile in SMF (in network elements).

The FHT template provides flexibility for SMF to fine tune its interactions with UPFs for sessions. It supports SMF to handle the error cause codes in response from UPF for both new and existing sessions. Based on the error cause codes in response from UPF, this feature provides the following configurable actions:

- terminate
- retry-terminate

Configuring the UPF Failure Handling on N4 Interface

This section describes how to configure the UPF failure handling on N4 interface feature.

```
configure
  profile failure-handling pfcp_name
     interface pfcp message N4SessionEstablishmentReq
     cause-code pfcp-entity-in-congestion
     action retry-terminate max-retry value
     end
```

NOTES:

- **profile failure-handling**: Specifies the UPF profile that is associated with FHT.
- **interface pfcp message {N4SessionEstablishmentReq | N4SessionModificationReq}**: Specifies the failure handling for N4SessionEstablishmentReq (for new sessions) and N4SessionModificationReq messages (for existing sessions).

Note UPF reselection is not applicable for message type N4SessionModificationReq because the session is already active on a UPF.

- **cause-code {pfcp-entity-in-congestion | mandatory-ie-incorrect | mandatory-ie-missing | session-ctx-not-found | system-failure | service-not-supported | no-resource-available | no-response-received | reject}**: Specifies the error codes that SMF receives in the failure response message from UPF.

  Note
  - The **no-response-received** cause code is introduced in this feature to identify the scenarios where SMF does not receive any response from UPF.
  - FHT does not support the following cause codes, which are configured with their default behaviour:

    request-reject-unspecified, **cond-ie-missing**, **invalid-length**, **invalid-fw-policy**, **invalid-fteid-alloc-opt**, **no-established-pfcp-assoc**, **rule-creation-mod-failure**.

  - **pfcp-entity-in-congestion**: Specifies the cause code when UPF is congested.
  - **reject**: Specifies the option to handle the cause codes in the failure response message from UPF, which are not configured by using the CLI commands available for this feature.

- **action {retry-terminate | terminate}**: Specifies the action to perform based on the error cause code received in the failure response message from UPF.
  - **retry-terminate**: Specifies a retry attempt to an alternate UPF. If the retry attempt fails, the session is terminated.

    Note If all UPFs are in congested state, call fails even if the action is set to **continue**.

  - **max-retry**: Specifies the number of retry attempts to reselect an alternate UPF.
    - **Default value**: 2
    - **Maximum value**: 5

Configuring the Failure Profile Association

This section describes how to configure the failure profile association in this feature.

```
configure
  profile upf-group upf upf_group_name
    failure-profile pfcp_name
    end
```

NOTES:

- **profile upf-group upf**: Specifies the UPF group.
- **failure-profile**: Specifies the FHT profile for PFCP.

Configuration Matrix

This section describes the configuration options available for N4 Session Establishment Request and N4 Session Modification Request messages in this feature.

Message Type	Applicable Action	Applicable Cause Code	Default Behaviour
N4SessionEstablishmentReq	retry-terminate	• pfcp-entity-in-congestion • system-failure • service-not-supported • no-resource-available • no-response-received	terminate
N4SessionModificationReq	terminate	• mandatory-ie-incorrect • session-ctx-not-found • no-response-received	continue

Monitoring and Troubleshooting

This section describes the show command that is supported by the UPF failure handling on N4 interface feature.

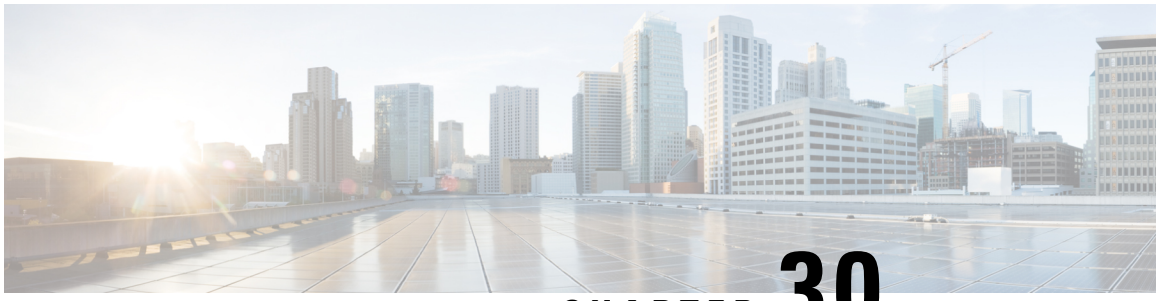
show running-config

Use the show **running-config** command to view the configuration.

The following configuration is a sample output of the show running-config command:

```
profile network-element upf upf1
       pfcp pfcp-failure-profile pfcp1
node-id      n4-peer-upf1
n4-peer-address ipv4 1.1.1.1
n4-peer-port 0000
keepalive    60
 dnn-list     [ uncarrier.5g ]
capacity     10
priority     1
exit
profile failure-handling pfcp1
 interface pfcp message N4SessionEstablishmentReq
  cause-code pfcp-entity-in-congestion
   action retry-terminate max-retry 2
  exit
 exit
interface pfcp message N4SessionModificationReq
  cause-code mandatory-ie-incorrect
   action terminate
  exit
```

```
 exit
exit
```



CHAPTER 30

Protocol Data Unit RAN Tunnel Endpoint Identifier Session

This chapter covers the following topics:

Feature Summary and Revision History

Summary Data

Table 124: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 125: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports activation and deactivation of the user plane connection of a PDU session.

How it Works

Labels are introduced at SMF-service to account active-to-idle and idle-to-active transitions. Existing idle and connected counters are used to track number of PDU sessions that are currently active or idle.

Label	Description
PROCEDURE TYPE	New label introduced. ue_req_active_to_idle ue_req_idle_to_active

Deactivation of the User Plane Connection of a PDU Session

This procedure is used to release the logical NG-AP signaling connection and the associated N3 user plane connections, and (R)AN RRC signaling and resources.

The following reasons may trigger the initiation of AN release:

- (R)AN-initiated with cause. For example, O&M Intervention, unspecified failure. (R)AN (For example, Radio) link failure, user inactivity, inter-system redirection, request for establishment of QoS flow for IMS voice, release due to UE generated signaling connection release, mobility restriction and so on.
- AMF-initiated with cause. For example, unspecified failure.

Limitations

- In this release, SMF supports only UE-initiated deactivation.
- Location update is not supported.

Call Flow

Figure 98: Deactivation of the User Plane Connection of a PDU Session Call Flow

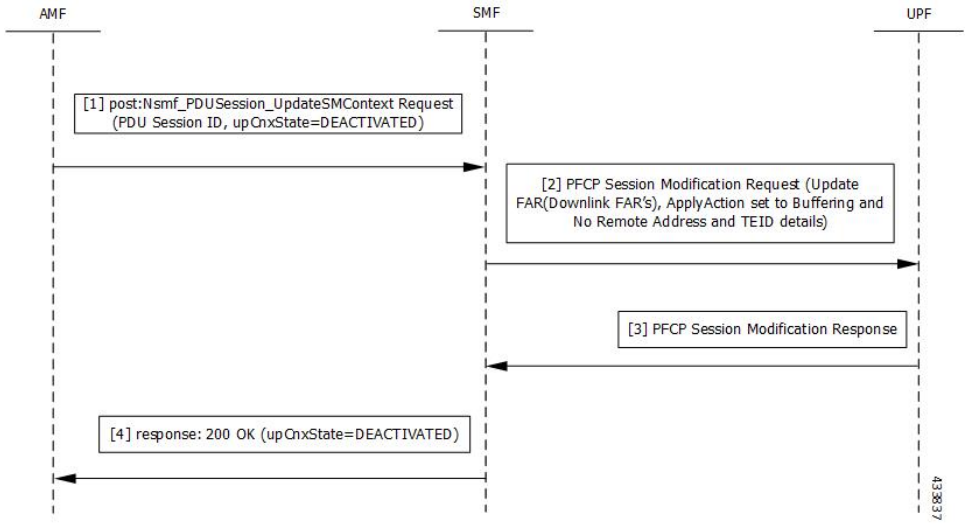


Table 126: Deactivation of the User Plane Connection of a PDU Session Call Flow Description

Step	Description
1	NF Service Consumer requests the SMF to deactivate the user plane connection of the PDU session by sending a POST request with the following information: • upCnxState attribute set to DEACTIVATED. • User location and user location timestamp. • Cause of the user plane deactivation. The cause may indicate a cause received from the 5G-AN or due to an AMF internal event. • Other information (if required).
2	SMF deactivates and releases the N3 tunnel of the PDU session after receiving such a request. SMF initiates PFCP session modification procedure towards UPF with downlink FAR updated with the following options: • Buffering Action is enabled without remote node "forwarding parameters" details like IP address and GTP-U F-TEID. **Note** NOCP (Notify the CP function) is not enabled. Support for notification is not available on SMF.
3	SMF sets the upCnxState attribute to DEACTIVATED for the PDU session after receiving successful response from UPF node.
4	SMF initiates 200 OK response including the upCnxState attribute set to DEACTIVATED towards AMF.

Activation of the User Plane Connection of a PDU Session

The service request procedure is used when the UE is in CM-IDLE and in CM CONNECTED to activate a user plane connection for an established PDU session. The UE in CM IDLE state initiates the service request procedure to send uplink signaling messages, user data or as a response to a network paging request.

Limitations

- In this release, SMF supports only UE-initiated service requests.
- Paging and network-initiated service requests are not supported.
- Location update and access-type changes are not supported.
- QoS flow modifications and errors are not supported.

Call Flow

Figure 99: Activation of the User Plane Connection of a PDU Session Call Flow

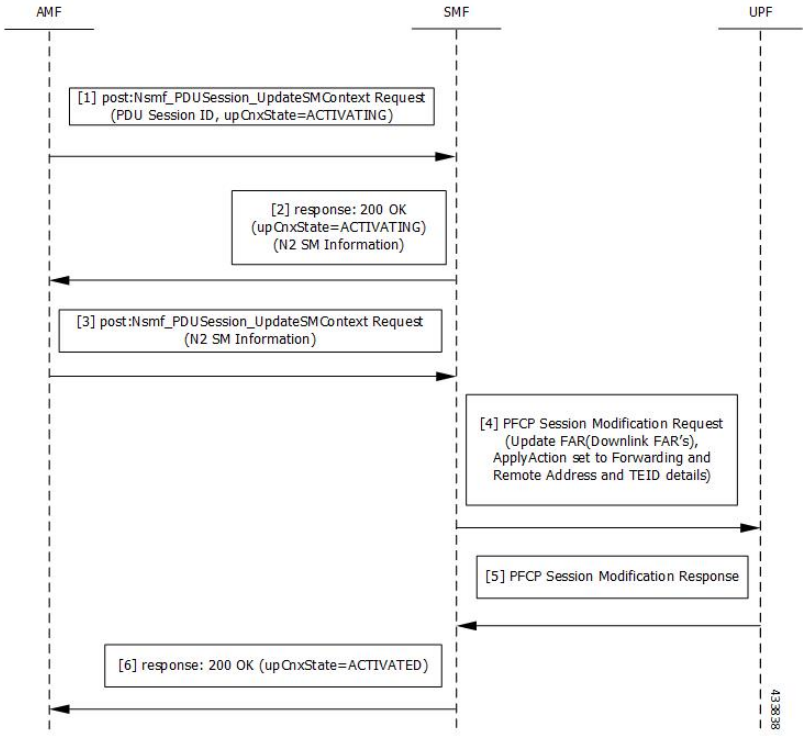


Table 127: Activation of the User Plane Connection of a PDU Session Call Flow Description

Step	Description
1	AMF requests the SMF to activate the user plane connection of the PDU session by sending a POST request with the following information: • upCnxState attribute set to ACTIVATING. • User location, user location timestamp, and access type associated to the PDU session (if modified) • Other information (if required).
2	SMF starts activating the N3 tunnel of the PDU session after receiving the request. SMF returns a 200 OK response including the following information: • upCnxState attribute set to ACTIVATING. • N2 SM information to request the 5G-AN to assign resources to the PDU session including the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session that is UPF's GTP-U F-TEID for uplink traffic.
3	AMF requests the SMF by sending POST request, with the following information: • SM information received from the 5G-AN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session, 5G-AN's GTP-U F-TEID for downlink traffic if the 5G-AN succeeded in establishing resources for the PDU sessions.
4	SMF initiates PFCP session modification procedure towards UPF with down link FAR updated with following options: • Forwarding Action is enabled with remote node “forwarding parameters” details like IP address and GTP-U F-TEID.
5	SMF sets the upCnxState attribute to ACTIVATED for the PDU session after receiving successful response from UPF node.
6	SMF initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF.

Always-On PDU Session Support

Feature Description

Some applications like the IP Multimedia Subsystem (IMS) require an always-on Protocol Data Unit (PDU) session that the User Plane resource establishes for every transition from the 5GMM-IDLE mode to the 5GMM-CONNECTED mode. The UE requests the establishment of a PDU session as an always-on PDU

session based on the request indication of the upper layers. It is the network that decides whether to establish a PDU session as an always-on PDU session.

How it Works

Call Flows

This section includes the following call flows.

PDU Session Establishment Call Flow

This section describes the call flow of the PDU session establishment.

Figure 100: PDU Session Establishment Call Flow

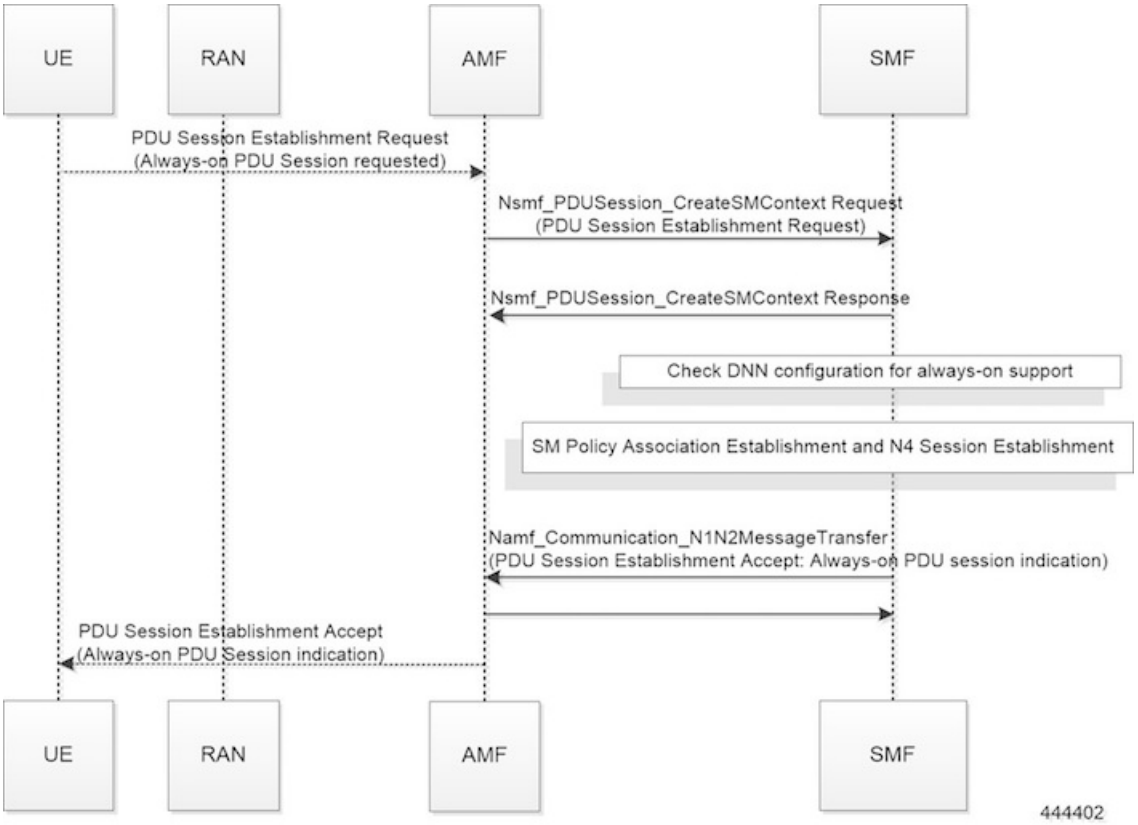


Table 128: PDU Session Establishment Call Flow Description

Step	Description
1	If the UE requests to establish an always-on PDU session, the UE includes an ‘Always-on PDU Session Requested’ IE in the PDU Session Establishment Request message.
2	The SMF checks the DNN profile to determine whether the “always-on” support is enabled.

Step	Description
3	The SMF includes an ‘Always-on PDU Session Indication’ in the PDU Session Establishment Accept message if any one of the following is true: • 'Always-on PDU Session Indication' is sent with value as "enabled" if the always-on configuration is enabled under the DNN profile. • 'Always-on PDU Session Indication' is sent with value as "disabled" when 'Always-on PDU Session Request' IE is received and configuration is disabled.
4	The SMF does not include an ‘Always-on PDU Session Indication’ only when both these conditions are true: • If the UE did not send an ‘Always-on PDU Session Requested’ IE • If always-on configuration is disabled in the DNN profile.

UE-Requested PDU Session Modification Call Flow

This section describes the call flow of the UE-requested PDU session modification.

Figure 101: UE-Requested PDU Session Modification Call Flow

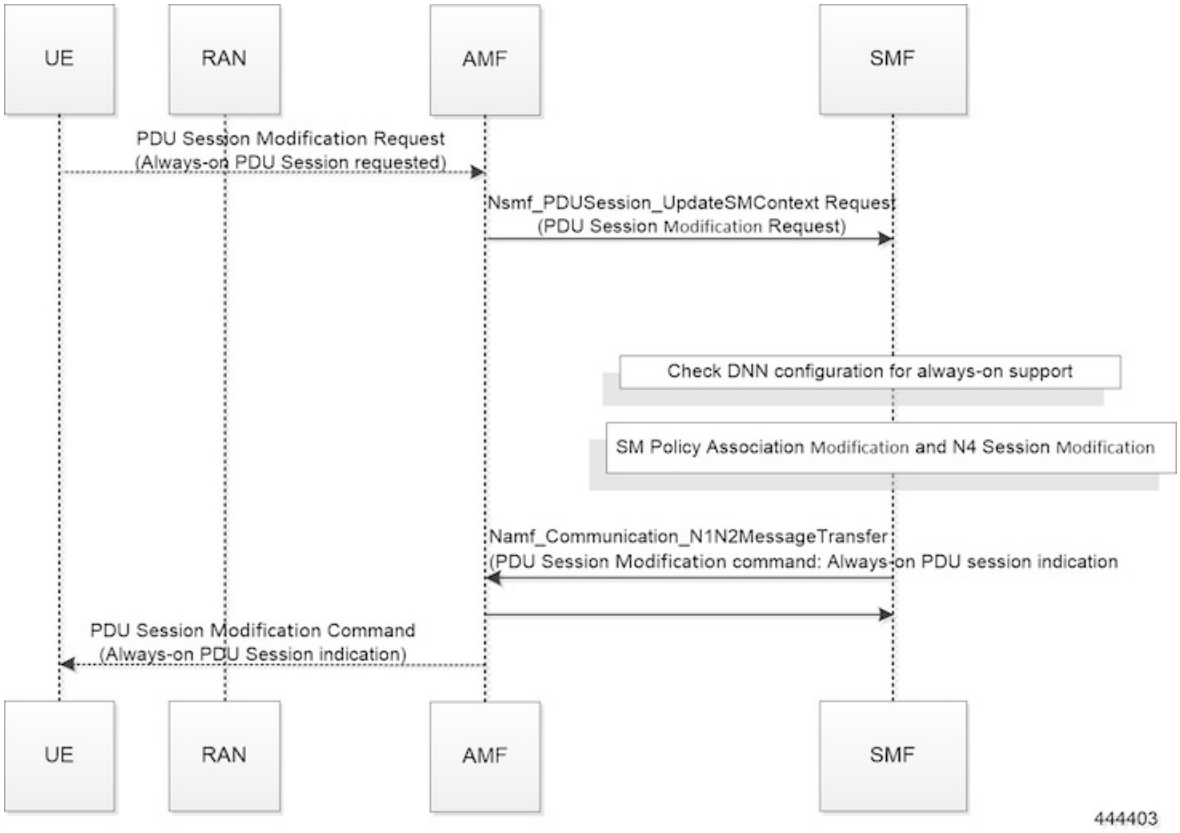


Table 129: UE-Requested PDU Session Modification Call Flow Description

Step	Description
1	The UE sends an ‘Always-on PDU Session Requested’ IE in the PDU Session Modification Request message.
2	The SMF checks the DNN profile to determine whether the “always-on” support is enabled.
3	The SMF includes an ‘Always-on PDU Session Indication’ in the PDU Session Modification Command when any one of the following is true: • 'Always-on PDU Session Indication' is sent with the value as "enabled" when the always-on configuration is enabled under the DNN profile. • 'Always-on PDU Session Indication' is sent with the value as "disabled" when an 'Always-on PDU Session Request' IE is received and configuration is disabled.
4	The SMF does not include an ‘Always-on PDU Session Indication’ only when both these conditions are true: • If the UE did not send an ‘Always-on PDU Session Requested’ IE. • If always-on configuration is disabled in the DNN profile. **Note** As per specification 23502, for a PDU session that was established in the EPS, when the UE moves from EPS to 5GS for the first time, the UE includes an 'Always-on PDU Session Requested' indication in the PDU Session Modification Request message if it wants to change the PDU session to an "always-on" PDU session.

Network-Requested PDU Session Modification Call Flow

This section describes the call flow of the network-requested PDU session modification.

Figure 102: Network-Requested PDU Session Modification Call Flow

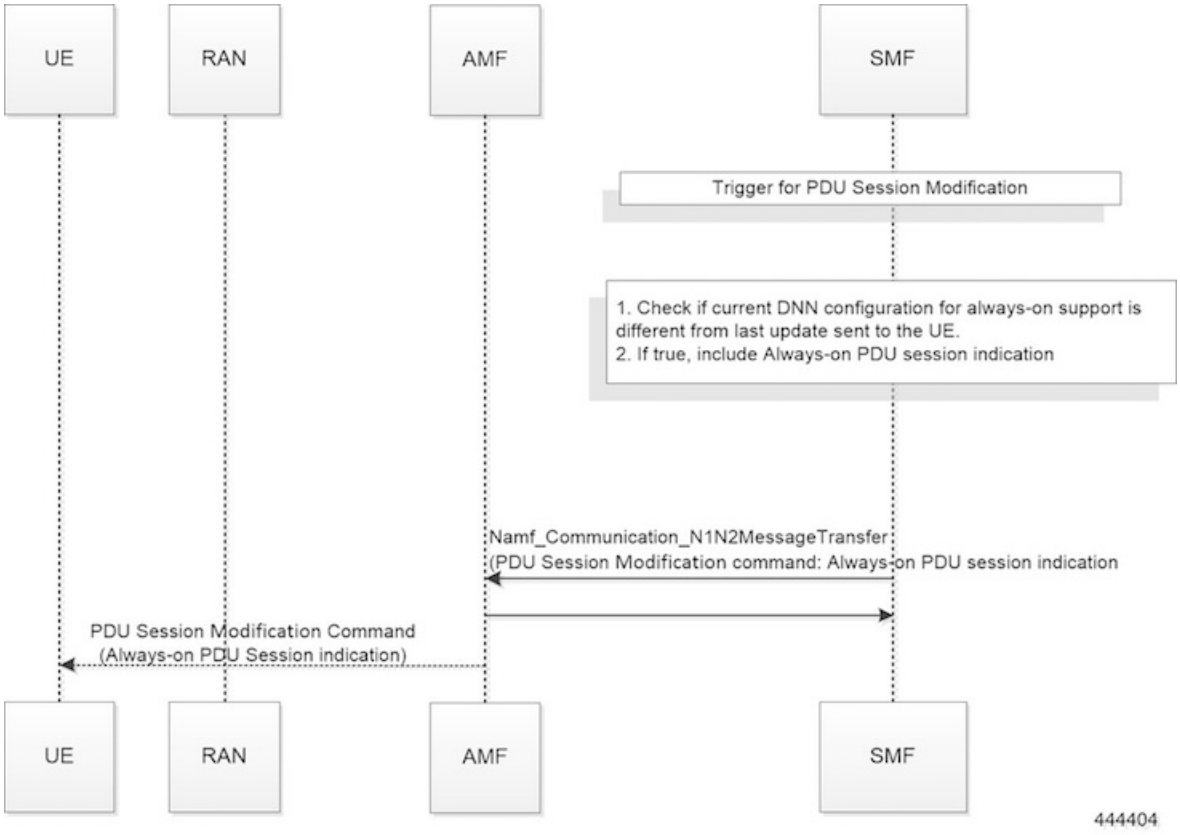


Table 130: Network-Requested PDU Session Modification Call Flow Description

Step	Description
1	The SMF decides to trigger a PDU Session Modification due to PCF, UDM, or RAN initiated procedures.
2	The SMF checks the DNN profile to determine whether the “always-on” support is enabled.
3	The SMF determines whether the current DNN configuration for “always-on” is different from the last indication sent to UE. If it differs, the SMF includes an ‘Always-on PDU Session Indication’ IE in the PDU Session Modification Command message.

Configuring Always-On PDU Session Support

To configure always-on PDU session support under the DNN profile, use the following commands:

```
configure
  profile dnn name
  always-on { true | false }
  end
```

- **always-on { true | false }**: Enables or disables the "always-on" PDU session support.
  - **true**: Enables always-on PDU session support.
  - **false**: Disables always-on PDU session support.

Verifying Always-On PDU Session Support

Use the **show subscriber supi** *supi_id* CLI command to verify the always-on PDU session support.

Note The show output for always-on PDU session support displays any one of the following options:

- “alwaysOn”: “UE Requested”
- “alwaysOn”: “Enabled”
- “alwaysOn”: “UE Requested & Enabled”

The following is a sample output of the command:

```
show subscriber supi imsi-123456789012345
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-123456789012345",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
   "accessType": "ACCESS_5G",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "123",
      "mnc": "456"
    },
    "sScMode": 1,
    "uetimeZone": "UTC+12:00",
    "allocatedIp": "12.0.4.4",
    "nrLocation": {
      "ncgi": {
        "mcc": "123",
        "mnc": "456",
        "nrCellId": "123456789"
      },
      "tai": {
        "mcc": "123",
        "mnc": "456",
        "tac": "1820"
      }
    }
    "alwaysOn":  "UE Requested"
  },
  "accessSubData": {
    "amfID": "AFbe08",
    "amfPlmnId": {
      "mcc": "123",
      "mnc": "456"
    },
    "ueCmStatus": "UeCMConnected",
```

```
    "amfNrfID": "76517361-338e-4d77-bc76-713a79779574"
  },
  "policySubData": {
    "TotalDynamicRules": 1,
    "TotalFlowCount": 1,
    "TotalNonGBRFlows": 1,
    "pccRuleList": [
      {
        "pccRuleId": "defaultrule",
        "qfi": 1,
        "mbrDl": 125000000,
        "mbrUl": 100000000,
        "flowInformation": [
          {
            "flowDirection": 3,
            "flowDescription": "permit out ip from any to any"
          }
        ]
      }
    ],
    "qosFlow": [
      {
        "qfi": 1,
        "GBRFlow": "False",
        "bindingParameters": {
          "x5Qi": 5,
          "arp": {
            "preemptCap": 1,
            "preemptVuln": 1,
            "priorityLevel": 15
          },
          "priorityLevel": 1
        },
        "AggregatedULMFbr": 100000000,
        "AggregatedDLMFbr": 125000000,
        "pccRuleList": "defaultrule"
      }
    ]
  },
  "chargingData": {},
  "upfServData": {
    "numberOfTunnels": 1,
    "smfSeid": 21790984727,
    "UPState": "Activated",
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel"
        }
      ]
    }
  }
}
```

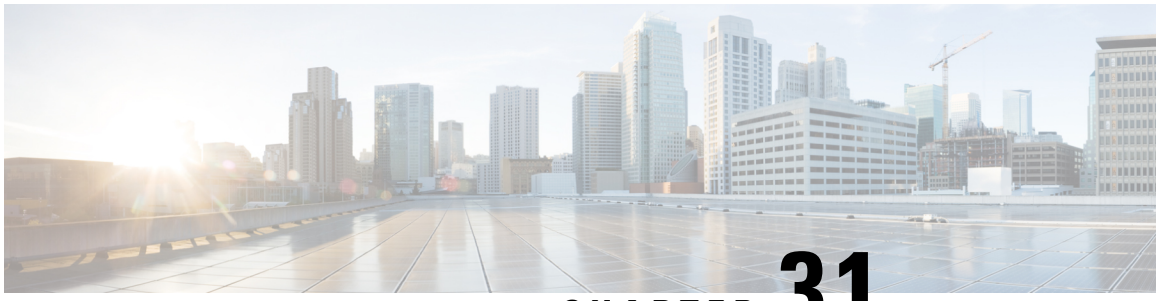

Bulk Statistics for Always-On PDU Session Support

The following statistics are introduced for the Always-On PDU Session Support feature.

Table 131: Bulk Statistics for Always-On PDU Session Support

Bulk Statistics	Description

always-on-pdu	Tracks the number of always-on PDU sessions.
Always-on-pdu-requested	Requests the always-on PDU session.
always-on-pdu-accepted	Accepts the always-on PDU session request.
Always-on-pdu-rejected	Rejects the always-on PDU session request.
pdusetup_req_alwayson_requested	Indicates the number of session establishment requests received with 'Always-On PDU Session Requested'.
pdusetup_acc_alwayson_allowed	Indicates the number of session establishment accept messages sent with the 'Always-On PDU Session Indication enabled.
pdusetup_acc_alwayson_not_allowed	Indicates that the number of session establishment accept messages sent with the 'Always-On PDU Session Indication' disabled.
pdumod_req_alwayson_requested	Indicates the number of session modification requests received with 'Always-On PDU Session Requested'.
pdumod_cmd_alwayson_allowed	Indicates the number of session modification commands sent with the 'Always-On PDU session indication' enabled.
pdumod_cmd_alwayson_not_allowed	Indicates the number of session modification commands sent with the 'Always-On PDU session indication' disabled.
pdumod_cmd_nw_init_alwayson_allowed	Indicates the number of network initiated session modification commands sent with the 'Always-On PDU session indication' enabled.
smf_session_counters	Indicates that the gauge updated to show the number of active always-on pdu sessions.



CHAPTER 31

Policy and User Plane Management

Feature Summary and Revision History

Summary Data

Table 132: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 133: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF is one of the control plane NFs that provide the Session Management service in the 5G core network. The SMF manages the PDU session lifecycle through the following session management procedures:

- PDU Session Establishment
- PDU Session Modification
- PDU Session Release

This chapter describes the policy and user plane management features.

- Policy Management—Policy Control Function (PCF) or the local configuration controls the policies managed on SMF. The PCF sends Policy and Charging Control (PCC) rules along with the applicable QoS and charging information to the SMF. The SMF uses this information to define QoS flows and apply QoS enforcement (via User Plane Function (UPF) and charging towards Charging Function (CHF). The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.
- User Plane Management—The user plane management on SMF includes selection of UPF and maintaining per session and node level user plane data. The SMF performs Path management of the UPF nodes. At a per session level, SMF publishes the Packet Detection Rules (PDRs), QoS Enforcement Rules (QERs), Forwarding Action Rules (FARs), and Usage Reporting Rules (URRs) to the UPF. Then, the SMF enforces the policy rules received from PCF or configured locally.

QoS Management on SMF

Feature Description

The primary functionality of the SMF is to manage the flow-based QoS model. SMF interacts with the Unified Data Management (UDM) and Policy Control Function (PCF) to get the subscribed and authorized QoS parameters for GBR and non-GBR flows and passes on the relevant information to UE (NAS), gNB (NGAP), and UPF (PFCP) so that all nodes on the network provide the desired QoS to the PDU session.

Use Cases

This section describes the various use case scenarios that can lead to creation, modification, and deletion of QoS-Profile and the corresponding actions taken.

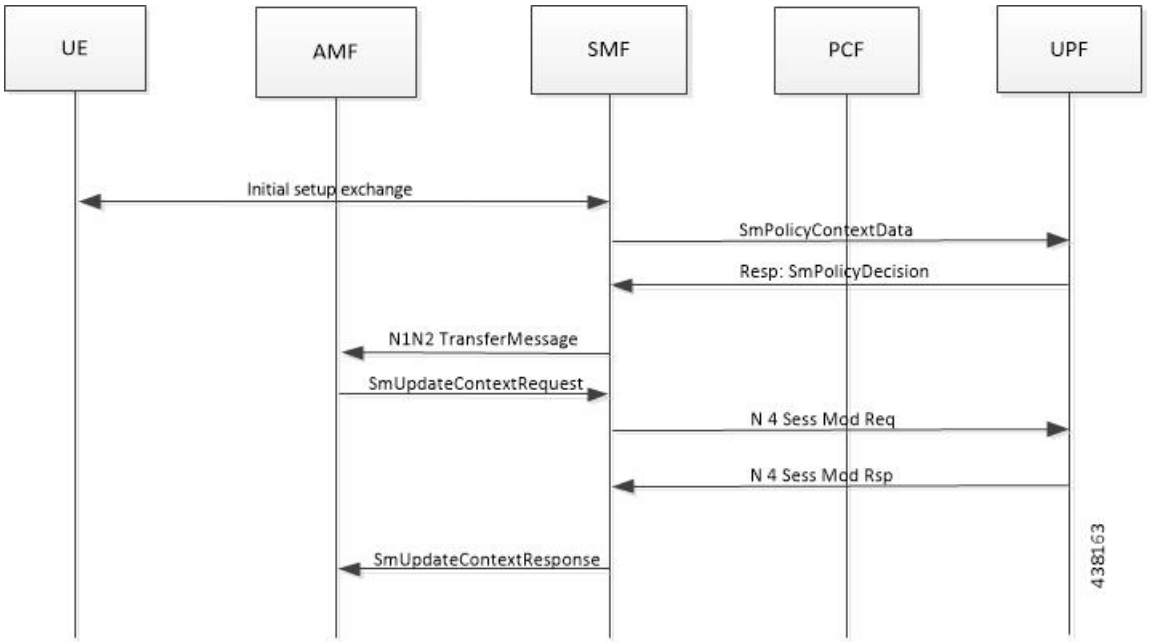
QoS-Profile associated to the PDU Context will be modified in the following scenarios:

- Response from PCF for SMPolicyContextData
- Update Notify from PCF
- Update response from PCF on behalf of Update request sent initially from SMF
- Update request from SMF will be triggered in the following cases:
  - UE triggered modify request

- AN triggered modify request
- UDM triggered modify request

Setup Creation

Figure 103: Setup Creation

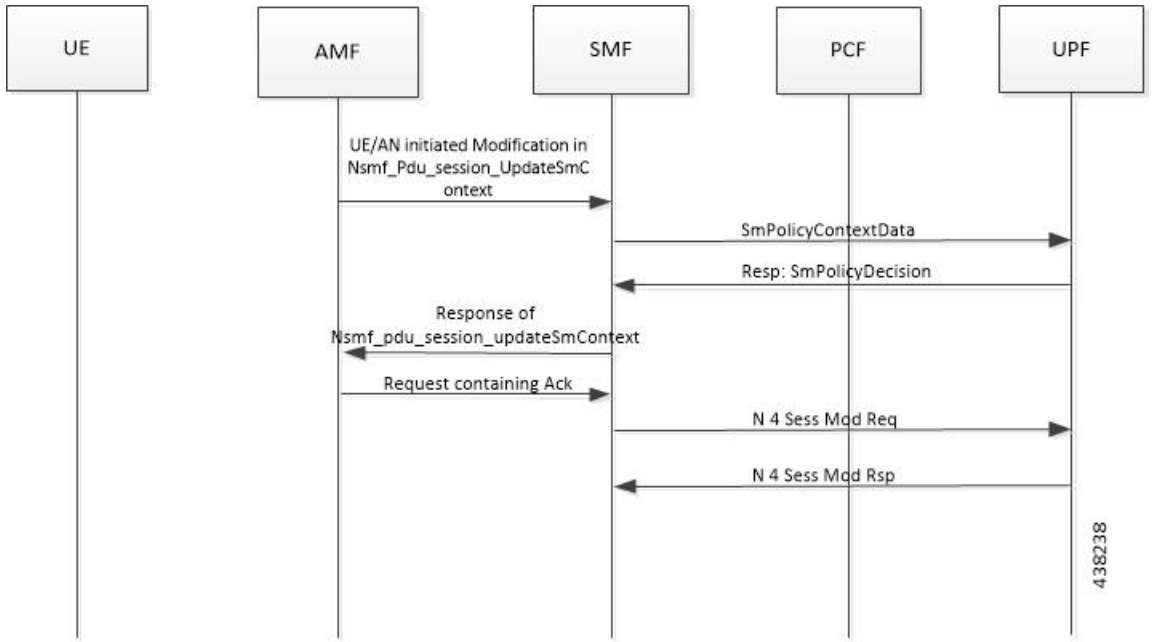


Based on the content received in SMPolicyDecision, SMF pushes the following towards various interfaces.

- UPF:
  - Set of PDR derived from PCC rules
  - Set of QER derived from QoS flows which in turn are derived from QosDescription/QosCharacteristics from PCF
  - One extra QER that will be shared will be derived from SessRules
- N1:
  - Set of QoS rules derived from QosFlows
  - Each QosRule has its associated packet filter
- N2:
  - Set of QoS Flow information

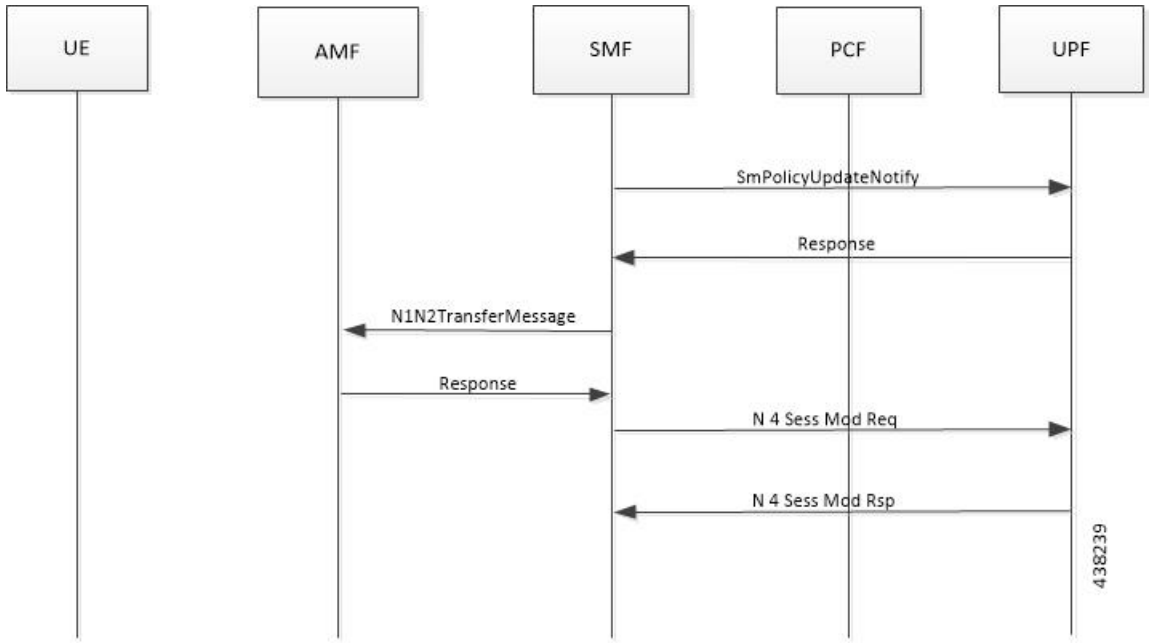
UE/AN-initiated Modify

Figure 104: UE/AN-initiated Modify



UDM/PCF-initiated Modify

Figure 105: UDM/PCF-initiated Modify



- N1:

- PDU Session Modification command will be triggered from SMF. It can change Session-AMBR and QoS rules.
- PDU Session Modification Request will be triggered from UE. It can change the QoS rules and maximum number of support-ed packet filters.

  In either case, the QoS rule change can happen from the following:

  - Packet filter add/delete/replace
  - Rule Precedence of QoS Rule
  - QoS Parameter – 5QI/MBR/GBR

- N2:
  - PDU Session Resource Modify Request will be triggered from SMF. It can change the existing QoS flow that is installed or delete the QoS flow already installed. If the Modify request is received, the parameters - ARP, GBR/MBR, Priority level, and so on, can change.
  - PDU Session Resource Notify will be triggered from AN. This happens when certain flow is to be released, not fulfilled any-more and fulfilled again.

Subscribed QoS

The UDM NF maintains the subscribed QoS for the UE in the Session Management Subscription Data. During the PDU setup procedure, the SMF posts an HTTP2 GET request (see 3GPP TS 29.503) for a resource URI "/{supi}/sm-data" to fetch the Session Management Subscription Data. The subscription data has a set of DNN configurations, one for each DNN which the subscriber is allowed to access. Each DNN configuration consists of the following parameters:

- sessionAMBR: The maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session.
- 5gQosProfile: The default 5G QoS Indicator (5QI) and default ARP values are provided to the SMF in the Session Management Subscription Data in this attribute of the DNN configuration.

The SMF saves the subscribed QoS parameters and sends this across to the PCF during the SM Policy Association Establishment procedure.

QoS Negotiation

The SMF negotiates the QoS with the PCF by initiating a Policy Association Establishment procedure as defined in 3GPP TS 23.502, Section 4.16.4. The sessionAMBR and 5gQosProfile parameters that are received from subscription are included in the Npcf_SMPolicyControl_Create request to PCF. The response from PCF may contain the following:

- Session Rules: A session rule consists of policy information elements that are associated with the PDU session. The QoS related information is Authorized session AMBR and Authorized default QoS.
  - Policy Charging and Control (PCC) Rules: The PCC rule includes the FlowDescription, FlowDirection, and RefQosData parameters among other information. There could be one or more PCC rules in the response from PCF.

- FlowDescription: This parameter contains packet filters for IP flows. For IP PDU Session Type, the Packet Filter Set supports packet filtering based on at least any combination of:
  - Source / Destination IP address or IPv6 prefix
  - Source / Destination port number
  - Protocol ID of the protocol above IP/Next header type
  - Type of Service (TOS) (IPv4) / Traffic class (IPv6) and mask
  - Flow Label (IPv6)
  - Security parameter index
- FlowDirection: This parameter indicates the direction of data traffic on which the rule has to be applied. This could be UPLINK, DOWNLINK, or BIDIRECTIONAL.
- RefQosData: This parameter refers to the QoS description to be applied to this PCC Rule. This matches the QosId of at least one of the QoS Description entries in the response from PCF.

- QoS Characteristics: The QoS characteristics include parameters such as:
  - Resource Type (GBR, Delay critical GBR, or non-GBR)
  - Priority Level
  - Packet Delay Budget
  - Packet Error Rate
  - Averaging Window
  - Maximum Data Burst Volume (for the Delay-critical GBR resource type only)

    This attribute in the response from PCF is meant to be used only for non-standard 5QI values. For standard 5QI values, the characteristics are already defined in 3GPP TS 23.501, Section 5.7.4.

- QoS Description: The QoS Description parameter consists of the following:
  - 5QI: Standard or non-standard from the QoS Characteristics attribute
  - Uplink and Downlink GBR
  - Uplink and Downlink MBR
  - Maximum Packet Loss Rate
  - QosId – Referenced in PCC rules
  - Default QoS Indication

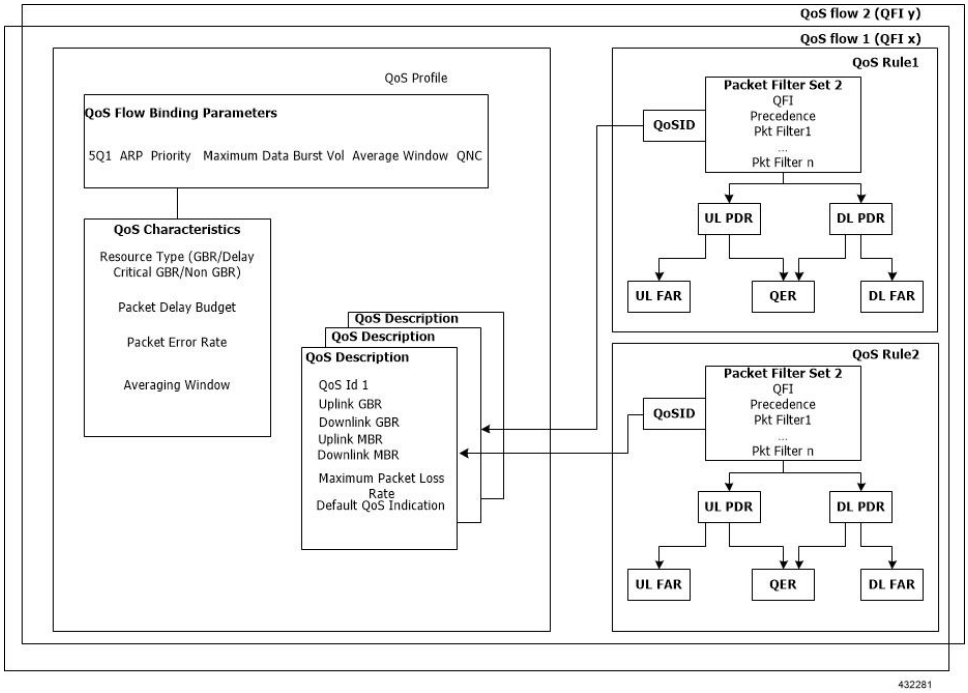
    There could be more than one QoS Description attribute in the response from PCF.

QoS Flow Management

The information, that is received from PCF in the Npcf_SMPolicyControl_Create response, is used to create and update QoS Flows in the SMF. Each QoS flow has a unique QoS Flow ID (QFI) and one or more PCC rules map to a single QoS flow.

The following figure illustrates how to manage the QoS information at the SMF.

Figure 106: QoS Information Management at SMF



Each QoS Flow in SMF is a combination of three sets of information:

- QoS profile: A QoS profile stores all QoS attributes for a particular QoS Flow.
  - Some QoS parameters known as the QoS flow binding parameters make a unique combination for one QoS Flow of one PDU Session. This means that, for a PDU session, each unique combination of these parameters represents a separate QoS Flow. These parameters are – 5QI, ARP, Priority, Maximum Data Burst Volume, Average Window and QNC.
  - If the 5QI for the QoS profile of a QoS Flow is non-standard, some additional QoS characteristics such as Resource Type, Packet Delay Budget, Packet Error rate, and Averaging Window are also saved in the QoS profile.
  - The QoS profile also maintains multiple QoS Descriptions, each with a unique QoSId for a specific PDU session. Each QoS Description contains the uplink and downlink GBR, uplink and downlink MBR, maximum packet loss rate and default QoS indication.
- QoS Rules: A QoS rule is a collection of packet filters that associates with a particular QoS Description in the QoS profile of the QoS flow. The packet filters directly map to the flow descriptions received in the PCC rules in the Npcf_SMPolicyControl_Create response from PCF. The QoS rules have a reference to the QoSId of the QoS Descriptions that the rules associate with.

- PDRs: Each QoS rule maps to two Packet Detection Rules (PDR) to be sent to the UPF. One PDR is for uplink direction and the other PDR is for downlink direction. The Service Data Flow (SDF) filters in the Packet Detection Information (PDI) attribute within the PDRs map the packet filters of the QoS rule. Each PDR then maps to a Forwarding Action Rule (FAR), which determines the forwarding action for the packets matching the SDF filters. Each PDR is also associated to a QoS Enforcement Rule (QER) which carries the QoS information and it maps to the QoS description associated with the QoS rule.

QoS Communication on 3GPP Interfaces

The negotiated QoS mainly needs to be communicated to the UE (N1 interface using NAS protocol), gNB (N2 interface using NGAP protocol), and UPF (N4 interface using PFCP protocol).

- N1 Interface: On the N1 interface, the session management messages are exchanged between UE and SMF through AMF. The NAS messages are encoded into an N1 container and sent to SMF or received from SMF.
  - All the negotiated/authorized QoS related information that needs to be sent out to the UE are found in the Authorized QoS rules and Session-AMBR attributes of the PDU SESSION ESTABLISHMENT ACCEPT message in an N1 container, during the PDU session establishment (see 3GPP TS 24.501, Section 8.3.2).
  - The PDU SESSION MODIFICATION REQUEST message from UE contains the Requested QoS Rules during the UE initiated QoS modification.
  - The Authorized QoS rules and Session-AMBR attributes are also present in the PDU SESSION MODIFICATION COMMAND message sent from SMF to UE during the PCF/SMF initiated QoS modification.
  - The format of the QoS Rule NAS attribute is defined in 3GPP TS 24.501, Section 9.10.4.9. This attribute mainly consists of the packet filter list, QFI, and QoS parameters on a per QoS rule basis. This information is available in the QoS rule within the QoS flow.
- N2 Interface: On the N2 interface, SMF sends an N2 container to the gNB through AMF. The N2 container is ASN.1 encoded data and consists of specific information elements of NGAP messages. All the QoS related information to gNB is encoded and sent/received in N2 containers to/from SMF. The NGAP IEs and the corresponding NGAP messages that will finally carry the IE from AMF to gNB are listed in 3GPP TS 29.502, Section 6.1.6.4.3.
  - During the PDU session setup, the SMF sends N1N2MessageTransfer to AMF with the N2 container in the PDU Session Re-source Setup Request Transfer IE. This IE contains PDU Session Aggregate Maximum Bit Rate and QoS Flow Setup Request List. The QoS Flow Setup Request List contains QoS Flow Level QoS Parameters (GBR flow information, 5QI, and so on). These are defined in 3GPP TS 38.413, Section 9.3.1.
  - Similar information (QoS Flow Level QoS Parameters) is also sent by SMF in the PDU Session Resource Modify Request Transfer IE in an N2 container during the PCF/SMF initiated QoS Modification procedure.

    The information required to create the N2 container in SMF is present in the QoS profile of a QoS flow as described in the previous section.
- N4 Interface: On the N4 interface, the SMF sends the QoS information in the form of Packet Detection Rule (PDR), Forwarding Action Rule (FAR), and QoS Enforcement Rule (QER).

- The PDR contains the SDF filters in the PDI IE. These SDF filters are the packet filters set in the QoS Rule of a QoS flow.
- The QER contains the QoS parameters as per the QoS Description to which the QoS rule is associated.

  The contents of PDR, FAR, and QER are defined in 3GPP TS 29.244.

QoS Modification

QoS modification may result in one of the following scenarios:

- QoS Flow Addition: Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Max Data Burst Volume, QNC). If there is no QoS Flow with the received combination of the flow binding parameters, SMF adds a new QoS flow and the received PCC rules will be mapped against the new QoS flow. As a result, the new QoS flow rules/QoS descriptions/PDR/QER are created and the corresponding interfaces (N1, N2, and N4) are updated by creating new flows.
- QoS Flow Modification: Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Maximum Data Burst Volume, QNC). If there exists a QoS flow with the same combination of binding parameters, the QoS profile, QoS rules, PDR, and QER for that QoS flow are updated on N1, N2 and N4 interfaces.

Handling of Authorized QoS for Default Bearer

Feature Description

The CHF server interacts with PCF to report the user quota exhaustion. Then, the PCF initiates a policy update request towards SMF to modify the authorized default Quality of Service (QoS) of a session rule. The QoS can be QoS Class Identifier (QCI) or 5G QoS Indicator (5QI), session Aggregate Maximum Bit Rate (AMBR), or both QCI/5QI and session AMBR.

Whenever the quota of user exhausts, this QoS modification results in downgrading:

- the DSCP marking of the data packets for the session
- the AMBR of the session

When you replenish the quota, the PCF reverts to the previous authorized QoS for the default bearer.

Be aware of the following changes whenever the QCI/5QI changes for the default flow or bearer.

- The QCI/5QI information is updated in the Event Data Record (EDR) generated for that session. Then, the SMF sends the updated bearer level information over Packet Forwarding Control Protocol (PFCP) message to support the EDR functionality.
- DSCP marking for the data packets is updated for all Packet Detection Rules (PDRs) pertaining to the default bearer or flow.
- Any QCI information sent in LI packets are updated.

- Rulebase change and Ruledef activation or deactivation work as expected along with 5QI change and session AMBR change.
- Any modified QoS is sent in Charging Data Request (Update) message to the CHF. Also, change in QCI/5QI in the authorized QoS is treated as a QoS change trigger for charging and CDR-U is sent.

How it Works

This section provides detailed changes in SMF to support change of QCI/5QI value in authorized QoS once the PDU session is established.

Default-Bearer QoS Handling for 4G and WiFi Sessions

The following procedure explains how the SMF handles the modification of authorized default QoS in 4G and WiFi sessions.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed QCI/5QI in AuthorizedDefaultQoS and/or a different session AMBR value.
2. The SMF initiates Update Bearer Request towards S-GW for the default bearer.
   a. In the Update Bearer Request, Bearer Context IE is included for the default bearer and the corresponding Bearer QoS is updated with the changed QCI value.
   b. For the 4G session, the extended Protocol Configuration Options (ePCO), if supported, is included in the Update Bearer Request message. The ePCO includes 5G Authorized QoS Flow Information with updated QCI value for the default flow when the interworking (IWF) is enabled for the session. Otherwise, PCO IE is sent with the same details.
   c. For the WiFi session, Additional Protocol Configuration Options (APCO) is included in the Update Bearer Request message. The APCO contains 5G Authorized QoS Flow Information with updated QCI value for the default flow.
3. The SMF accepts the Update Bearer Response from S-GW.
4. On the N4 interface, the following changes are done:
   a. New instance of the BearerLvlInfo IE is included with the changed QCI value for default bearer tunnel.
   b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
   c. FAR associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

Default-Bearer QoS Handling for 5G Sessions

The following procedure explains how the SMF handles the modification of authorized QoS for the default bearer in a 5G session.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed 5QI in AuthorizedDefaultQoS and/or a different session AMBR value.

2. The SMF initiates N1N2MessageTransfer procedure with AMF to send N1 PDU Session Modification Command and N2 PDU Session Resource Modify Request Transfer IE in this message.
   a. In the N1 message, the default QoS flow is modified in Authorized QoS Flow Description IE to update the 5QI value.
   b. In the N1 message, the Mapped EPS Bearer Context IE is modified to update the QCI of the default bearer.
   c. In the N2 message, the QoS flow level QoS parameter for the default flow is modified to update the 5QI value.
3. The SMF accepts the SMContextUpdate Request from AMF with the responses for the N1 and N2 requests sent in N1N2Message Transfer message.
4. On the N4 interface, the following changes are done:
   a. New instance of the BearerLvlInfo IE is included with the changed 5QI to QFI mapping.
   b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
   c. Forwarding Action Rule (FAR) associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

Default-Bearer QoS Handling During WiFi Handovers

The following procedure explains how the SMF handles the modification of authorized default QoS during WiFi handover and other handovers.

1. The SMF sends SMPolicy Update Request to the PCF at the end of each handover procedure. For example, when the PCF arms different policy triggers, the SMF sends SMPolicy Update Request to the PCF. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.
2. For all handovers (excluding WiFi-NR/EPS and NR/EPS-WiFi), the SMF sends SMPolicy Update Request to the PCF indicating the RAT type change. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.

The handovers involving WiFi are different from the other handovers. The SMF triggers SMPolicy Update Request towards PCF during the handover and not after the handover. For the handovers involving WiFi, the target RAN installs the flows and bearers as new instead of an update. The SMF sends the latest QCI received in the response from PCF while installing the default flow and bearer during the handover.

Default-Bearer QoS Modification During Failure Handling

For a 5G session, the modification of QCI/5QI typically does not fail on the N1 or N2 interface as the default flow is a non-GBR flow and no resource reservation is required for the QCI/5QI modification. However, if the modification procedure fails due to no N1 or N2 responses from AMF, the modification is rolled back and the session continues with the old QCI/5QI and session AMBR values. If the N2 rejects the flow modification, the session is deleted as it cannot remain without the default flow.

For a 4G session, the Update Bearer response does not fail for default bearer modification. However, if the Update bearer Response is missing or if it fails, the modification is rolled back and the session continues with the old 5QI and session AMBR values.

For both 4G and 5G sessions, if the N4 update fails or the response is not received, then the SMF takes the action according to the UPF failure handling template configuration. For 4G and WiFi sessions, if there is a failure on the N4 interface, another Update Bearer Request is sent with the old 5QI and AMBR values to S-GW and ePDG respectively.

The failure handling mechanism remains the same for the PCF-initiated modification procedure.

Limitations

The Authorized QoS Handling for Default Bearer feature has the following limitations:

- The SMF supports only the standard QCI/5QI change in authorized default QoS IE of the Session Rules. It does not support any change to the Guaranteed Bit Rate (GBR) QCI/5QI of authorized QoS. The SMF rejects any request for modification of QCI/5QI of a QoS data associated with Policy and Charging Control (PCC) rule.
- The SMF does not support QCI/5QI change for dynamic rules.
- The SMF supports QCI/5QI change only for predefined and static rules that are associated to the default bearer. If a predefined rule is associated with a non-default flow or bearer, the SMF does not support QCI/5QI change for that rule.
- The combination of QoS flow binding parameters, such as 5QI, ARP, and so on, for the authorized QoS never remains the same as that of a dedicated bearer or flow. That is, change in QCI/5QI should not result in the default flow having the binding parameters similar to another flow.
- The SMF does not support changes to any other binding parameter including Allocation and Retention Priority (ARP) except the QCI/5QI (with or without session AMBR) in the Session Rules.
- When the QCI/5QI changes, the existing default bearer flow is modified towards N1, N2, and N4 interfaces. In this case, the SMF does not delete the existing flow instead creates a new flow.

Authorized QoS Handling OAM Support

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

Statistics Support

The SMF maintains the label "SESSRULE_CHANGE" to indicate any changes to the AMBR value, QCI/5QI value, or a combination of both AMBR and QCI/5QI values.

SMF Affinity

The SMF Affinity support is required in the CN architecture to facilitate stateless architecture.

When a session management procedure is ongoing for a subscriber session in some SMF service instance and another event from the network comes for the same subscriber in the meantime. Then, the SMF protocol layer micro-services such as "smf-rest-ep" and "smf-protocol" direct these events towards the concerned SMF

service instance. This ensures that all network events pertaining to an ongoing procedure of a subscriber session are handled by the same SMF service instance until the completion of the procedure.

Upon completion of the procedure, the subscriber session information is updated in the database and the session affinity towards the SMF service instance is removed. Subsequent network events can be handled by any of the available SMF service instances, by fetching the relevant subscriber session information from the database.

Dynamic Configuration Change Support

Feature Description

The Dynamic Configuration Change Support feature allows new sessions, or subsequent messages of existing sessions, with the updated configuration values.

This feature supports the following SMF configurations:

- SMF Profile
- SMF Service Profile

SMF provides flexibility to support Maintenance Operational Procedure for certain SMF Profile/Service-Profile configuration parameters. This Maintenance Operational Procedure operation helps to keep the SMF system in maintenance mode so that it doesn't impact the system by rejecting the new sessions. Also, Maintenance Operational Procedure provides flexibility to operators to clear subscribers manually by executing **clear subscriber all** command.

SMF updates configuration parameters change to NRF by sending "NFUPdate" using PUT Method.

How it Works

This section describes the Maintenance Operational Procedure and how dynamic change in configuration works for the supported SMF configurations.

Maintenance Operational Procedure

1. Shutdown (offline) SMF by executing **mode offline** CLI command under SMF Profile.

   SMF sends NFUpdate with Method PUT and NFStatus as “UNDISCOVERABLE”
2. Clean up the sessions using **clear subscriber sess all** CLI command.
3. Change the configurations and remove **mode offline** CLI command.

   SMF sends NFUpdate with Method PUT and NFStatus as “Registered”.

SMF Profile and SMF-Service Profile

The following table describes how dynamic change in configuration works for the supported SMF configurations.

Configuration parameters	Dynamic Change	Impact on Existing Sessions	NRF Update	Maintenance Operational Procedure
locality	Allowed	Sessions will start using the newer values.	Not Required	Allowed
node-id	Not Applicable	No Impact	Not Applicable	Not Applicable
fqdn	Allowed	SMF always fetches the latest FQDN value for sessions while interacting with UDM.	Allowed	Allowed
allowed-nssai	Allowed	Sessions will start using the newer values.	Allowed	Allowed
plmn-id	Allowed	Sessions will start using the newer values.	Allowed	Allowed
service name, schema, service-id, version	Allowed	Sessions will start using the newer values.	Allowed	Allowed
http-endpoint	Allowed	Sessions will start using the newer values.	Allowed	Allowed
icmpv6-profile	Allowed	Sessions will start using the newer values.	Not Required	Not Required
compliance-profile	Allowed	SMF might perform parse-failure because of incompatibility issues between SMF and other NFs for various SBI interfaces.	Not Required	Not Required
access-profile	Allowed	Sessions will start using the newer values.	Not Required	Not Required
subscriber-policy	Allowed	Sessions will start using the newer values.	Not Required	Not Required

Configuring Dynamic Configuration Change Support

Use the following configuration to enable offline mode of operation under SMF profile.

```
configure
  profile smf profile_name
    mode offline
    end
```

NOTES:

- **mode**: Specifies the mode of operation.

- **offline**: Specifies the mode is offline and new sessions are rejected.

Verifying Dynamic Configuration Change Support Configuration

Use the **show running-config profile smf** CLI command to verify if the feature is enabled. When enabled, the following field will be displayed as part of the show command output:

- mode offline

Dynamic PCC Rules Enforcement

Feature Description

SMF uses either the Policy and Charging Control (PCC) rules from Policy Control Function (PCF) or the locally configured policy rules to control the policy management. The PCF sends the PCC rules along with the applicable QoS and charging information to the SMF. The SMF uses this information to define the QoS flows and apply the QoS enforcement (via UPF) and charging towards CHF.

The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.

The following sections provide information on the features that are implemented for the dynamic policy management.

Supported Features Negotiation

The SMF and the PCF negotiate the supported features during Policy Context Creation and during PDU session establishment. Based on the negotiated features, the PCF provides the relevant information.

The following table lists the features that can be negotiated as defined in the 3GPP specification 29.512.

Table 134: Supported Negotiated Features

Feature Number	Feature Name	Description
1	TSC	This feature indicates support for traffic steering control in the (S)Gi-LAN or routing of the user traffic to a local Data Network identified by the DNAI per Application Function (AF) request. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.6.2.20.
2	ResShare	This feature indicates the support of service data flows that share resources. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.7.4.
4	ADC	This feature indicates the support of application detection and control.
6	NetLoc	This feature indicates the support of the Access Network Information Reporting for 5GS.
7	RAN-NAS-Cause	This feature indicates the support for the detailed release cause code information from the access network.

The SMF sends supportedFeatures attribute in the Npcf_SMPolicyControl_Create message, and further includes a bitmap representing the supported features. The PCF also sends the supportedFeatures attribute in the response message. The response should either match or be a subset of the request.

The string contains a bitmask indicating supported features in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents the support of the features as described in the preceding table. The most significant character representing the highest-numbered features appears first in the string, and the character representing features 1–4 appears last in the string. The list of features and their numbering (starting with 1) are defined separately for each API.

Provisioning and Management of Session AMBR and Default QoS

For the N4 interface, the SMF sends the QoS information in the form of:

- Packet Detection Rule (PDR)
- Forwarding Action Rule (FAR)
- QoS Enforcement Rule (QER)

The SessionAMBR includes the maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session. The SMF sends the session level QER for non-GBR flows along with existing QER to the UPF.

The SMF receives sessionRule from PCF in SmPolicyDecision during PDU session creation. The sessionRule consists of authSessAmbr and authDefQos. The authorized AMBR consists of the Uplink (UL) and Downlink (DL) MBR at a session level and authDefQos contains the 5Qi, ARP, and other QoS binding parameters for the default QoS flow.

The SMF performs the following actions:

- Any PCC rules received from the PCF that have an associated QoS Desc with the same binding parameters as received in authDefQos are tagged with the default QoS flow.
- On the N4 interface, the UL and DL Packet Detection Rules (PDRs) are created for each PCC rule that is associated with the default QoS flow. For session AMBR enforcement, the SMF creates a QoS Enforcement Rule (QER) with appropriate AMBR and associates it with all PDRs for non-GBR rules.
- On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR and 5Qi values. The Session AMBR is also sent in this message.
- On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the AMBR and the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFI.
- The SMF supports the UDM-initiated Session AMBR modification. In this case:
  - The SMF sends Npcf_SMPolicyControl_Update to the PCF along with the new subscribed session AMBR within the "subsSessAmbr" attribute and the SE_AMBR_CH policy control request trigger within the "repPolicyCtrlReqTriggers". On receiving the change of session AMBR, the PCF provisions the new authorized session AMBR to the SMF in the response.
  - Update the QERs on N4 interface for Session AMBR enforcement.
  - Initiate N1N2MessageTransfer towards the AMF with Sess AMBR in PDU SESSION MODIFICATION COMMAND message in N1 interface and PDU Session Resource Modify Request transfer IE in N2 container having the new AMBR.

Provisioning of Policy Revalidation Time

Feature Description

The PCF instructs the SMF to trigger PCF interaction to request PCC rule from the PCF if not provided yet. The PCF performs this operation by providing revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute in SmPolicyDecision. The PCF can change the revalidation time by including a new value for the "revalidationTime" attribute. The PCF can also disable the revalidation function by removing RE_TIMEOUT policy control request trigger if it has been provided.

If the SMF receives the existing revalidation time or the new revalidation time, the SMF stores the received value and starts the timer based on it. Then, the SMF sends the PCC rule request before the indicated revalidation time. If the RE_TIMEOUT policy control request trigger is removed, the SMF stops the timer for revalidation.

Note When the RE_TIMEOUT is removed, the revalidation time value previously provided to the SMF is no longer applicable.

How it Works

Revalidation time is a string of the format "date-time" as defined in OpenAPI specification. The SMF, on receiving the revalidation time in "revalidationTime" attribute and RE_TIMEOUT trigger in "policyCtrlReqTriggers" attribute, starts a timer for the difference duration (revalidationTime – currentTime – 5 seconds buffer). Once the timer expires, the SMF initiates the PCF interaction to request PCC rules.

Standard Compliance

The Policy Revalidation Time feature complies with 3GPP TS 29.512, v15.2.0.

UPF Node Selection and Control

Feature Description

The SMF selection of a UPF node is based on certain selection criteria from a list of all UPFs having active association with the SMF, and serving the desired Network Slice Selection Assistance Information (NSSAI) and Data Network Name (DNN).

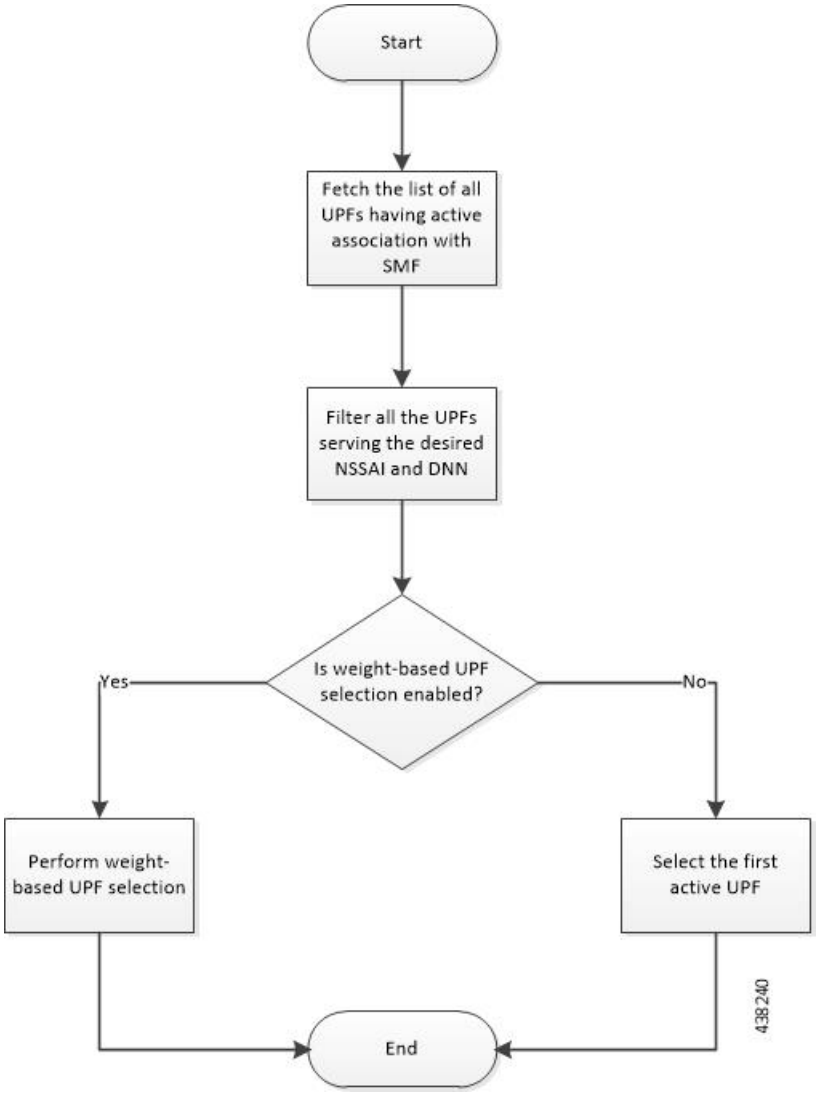
How it Works

The SMF and UPF association setup and IP management involves the following:

1. During the N4 Association Setup procedure initiated by peer UPF, the SMF validates the local configuration present.
2. The IP pools configured under DNN are divided into chunks and the IPAM module provides a chunk to the SMF during N4 Association.
3. The SMF publishes the obtained chunks to the corresponding UPF nodes in the N4 Association Update message.

The SMF selects a UPF node using the local configuration.

The following figure depicts how the UPF node selection is performed.



1. The SMF obtains a list of all UPFs with active association and filters the list to get all the UPFs supporting the NSSAI and DNN for this session.
2. The SMF checks whether the PCF has provided a TrafficControlData along with PCCRule during policy context creation. If this condition is met, the SMF filters the UPFs from the fetched list to get a list of UPFs supporting the required DNAI.
3. The SMF performs the UPF selection based on the capacity and priority of the UPF server.

Note The NSSAI and DNN are known to the SMF during session establishment before UPF selection.

Limitations

Post nodemgr POD restart, UPF association should be re-established for subsequent PDU session establishments to be successful.

Configuring the UPF Selection

This section describes how to configure UPF node selection.

Configuring the UPF node selection involves configuring criteria-based UPF selection.

Configuring Criteria-based UPF Selection

Use the following configuration to configure the selection of locally configured UPF.

The UPF profile contains a list of UPFs configured in the SMF. The selection mechanism uses the capacity and priority assigned to the UPF in the UPF profile.

```
configure
  profile network-element upf upf_name
     capacity service_capacity
     priority priority_value
     end
```

NOTES:

- **capacity** *service_capacity*: Indicates the static weight relative to other UPFs of the same type. *server_capacity* must be an integer value in the range of 0-65535. Default: 10.
- **priority** *priority_value*: Indicates the static priority relative to other UPFs of the same type. *priority_value* must be an integer value in the range of 0-65535. Default: 1

Verifying the Criteria-based UPF Selection Configuration

This section describes how to verify the criteria-based UPF selection configuration.

The following configuration is a sample output of the **show configuration** command:

```
profile network-element nrf nrf1
http-endpoint base-url http://1.1.1.111:8082
…
profile network-element upf upf2
capacity 10
priority 1
n4-peer-address ipv4 1.2.3.4
n4-peer-port 8805
keepalive 60
dnn-list [ dnn1 intershat cisco.com ]
…
```

Provisioning and Management of Additional QoS Flows

The PCF can create, modify, or delete multiple GBR and non-GBR PCC rules.

The following scenarios are possible:

1. Multiple non-GBR and GBR PCC rules are activated during PDU session establishment. In this case:
   a. The SMF creates the QoS flow according to the QoS flow binding principle as described in the QoS Management section.

b. On the N4 interface, the UL and DL PDRs are created for each PCC rule that is associated with all the flows. For flow-level QoS enforcement, the SMF creates QERs with the MFBR and GFBR (for GBR flows) values and associates it with each PDR of a flow.

c. On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR, GFBR, and 5Qi values. The packet filters associated with each QoS rule are sent on the N1 interface in the "Authorized QoS Rules" attribute.

d. Different types of packet filters are supported on both the N4 and the N1 interfaces. This list includes:

```
Packet filter component type identifier
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 Match-all type
0 0 0 1 0 0 0 0 IPv4 remote address type
0 0 0 1 0 0 0 1 IPv4 local address type
0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type
0 0 1 0 0 0 1 1 IPv6 local address/prefix length type
0 0 1 1 0 0 0 0 Protocol identifier/Next header type
0 1 0 0 0 0 0 0 Single local port type
0 1 0 0 0 0 0 1 Local port range type
0 1 0 1 0 0 0 0 Single remote port type
0 1 0 1 0 0 0 1 Remote port range type
```

e. On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFIs for each of the flows. The "GBR QoS Flow Information" field of the IE contains the MFBR and GFBR of the GBR flows.

2. Modification of PCC rules after PDU session establishment. In this case, the following scenarios are observed:

a. Modification, addition, and removal of packet filters of one or more PCC rules:

1. In this case, the SDF filters of the PDR on the N4 interface are changed by invoking N4 session modification.

2. The SMF initiates N1N2MessageTransfer towards the AMF with "Authorized QoS Rules" attribute in PDU SESSION MODIFICATION COMMAND message in N1 interface. The rule operation code in this attribute is one of the following:

```
0 1 1 Modify existing QoS rule and add packet filters
1 0 0 Modify existing QoS rule and replace all packet filters
1 0 1 Modify existing QoS rule and delete packet filter
```

b. Change in QoS associated with one or more PCC rules:

1. The SMF performs QoS flow binding evaluation which in turn results in the following operations:

1. Addition of a new QoS flow results in change of QFI on the N4 interface for some of the PDRs.

2. Movement of a PCC rule from one QoS flow to another QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.

3. Removal of a QoS flow when the last PCC rule in that flow is moved to a different QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.

2. In the preceding cases, on the N1 interface the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

```
0 0 1 Create new QoS flow description
0 1 0 Delete existing QoS flow description
0 1 1 Modify existing QoS flow description
```

3. On the N2 interface, QoS Flow Level QoS parameters of the PDU Session Resource Modify Request transfer IE carry the modified GFBR, MFBR, 5Qi and so on. For any flow removal, the QoS Flow to re-lease List is included in this IE.

c. PCC rule removal:

1. In this case, the SMF removes all the PDRs associated with a QoS flow on the N4 interface.
2. On the N1 interface, the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

```
0 1 0 Delete existing QoS flow description
```

3. On the N2 interface, the PDU Session Resource Modify Request transfer IE carries the QoS Flow to release List.

QoS Enforcement

The SMF enforces QoS at PCC rule (SDF) level, QoS flow level, and session level by creating one QER:

- per PCC rule level to enforce MBR/GBR as per the associated QoS Desc supplied by PCF and associated to the given PCC rule.
- at QoS flow level which has aggregated MBR/GBR of all the PCC rules associated with a QFI.
- at session level to enforce the Session AMBR for all non-GBR QoS flows.

Once these QERs are created, the SMF associates:

- the session level QER to all PDRs belonging to the non-GBR QoS category.
- the SDF level QER to each individual PCC rule.

For any QoS modification including movement of the PCC rules from one flow to another and QoS modification within flow, the SMF modifies the GFBR/MFBR (or Session AMBR) and updates the QERs accordingly on the N4 interface.

Policy Control Request Triggers

The PCF provides one or more policy control request trigger(s) by including the triggers in the "policyCtrlReqTriggers" attribute(s) in the SmPolicyDecision data structure.

During the lifetime of the PDU session, the PCF updates or removes the policy control request triggers. To update the trigger, the PCF provides a new complete list of applicable policy control request triggers by including the trigger(s) in the "policyCtrlReqTriggers" attribute.

The PCF removes all previously provided triggers by providing a "policyCtrlReqTriggers" attribute set to NULL value. Upon reception of a policy control request trigger with this value, the SMF does not inform PCF of any trigger except for those triggers that are always reported and does not require provisioning from the PCF.

Whenever the PCF provisions the trigger, unless otherwise specified in the trigger's value definition, the SMF sends the corresponding currently applicable values (for example, access type, RAT type, user location information, and so on) to the PCF within the UeCampingRep data structure in the response of the HTTP POST message. In this case, the "repPolicyCtrlReqTriggers" attribute is not included.

The list of supported triggers is as follows:

Trigger	Description
RES_MO_RE	A request for resource modification has been received by the SMF. This is a mandatory trigger. **Note** This request is sent from SMF to PCF when UE/AMF requested QoS modification is triggered.
UE_IP_CH	UE IP address change. This is a mandatory trigger.
DEF_QOS_CH	Default QoS Change. This is a mandatory trigger.
SE_AMBR_CH	Session AMBR Change. This is a mandatory trigger.
SAREA_CH	Location Change about the Serving Area in N11 update.
SCNN_CH	Location Change about the Serving CN node. See the following section for details on how the SMF supports this trigger during the different handover scenarios.
RE_TIMEOUT	Indicates that the SMF has generated the request because there has been a PCC revalidation timeout (that is, Enforced PCC rule request as defined in Table 6.1.3.5.-1 of 3GPP TS 29.503).

Support SCNN_CH Trigger in Handovers

The SMF supports the serving network change trigger in the following handovers:

- **Inter AMF Handover**: If the "SCNN_CH" is provisioned, when the SMF detects a change of serving Network Function (for example, the AMF), the SMF includes the "SCNN_CH" within the "repPolicyCtrlReqTriggers" attribute and the current serving Network Function in the "servNfId" attribute. When the serving Network Function is an AMF, the SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to 4G handover**: When the UE handed over from the 5GS to EPC/E-UTRAN, the SMF includes, if the "SCNN_CH" policy control request trigger is provisioned and met, the "servNfId" attribute including the S-GW identification within the "anGwAddr" attribute.
- **4G to 5G handover**: The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **WiFi to 5G handover**: The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to WiFi handover**: When the UE handed over from the 5GS to EPC non-3GPP access, the SMF includes, if the "SCNN_CH" policy control request trigger is provisioned and met, the ePDG identification within the "anGwAddr" attribute included in the "servNfId" attribute.

Gating Control

Feature Description

Gating control is the capability to block or allow IP packets belonging to a certain IP flow, based on the decisions by the PCF. The PCF could, for example, make gating decisions based on session events (start and stop of service) reported by the AF.

The AF instructs the PCF to temporarily block the user traffic corresponding to a specific PCC rule on uplink or downlink direction, or both the directions.

To enable the PCF gating control decisions, the AF reports session events (for example, session termination, modification) to the PCF. For example, session termination, in gating control, triggers the blocking of packets or "closing the gate".

Note Gating Control applies only for service data flows of IP type.

How it Works

The Gating Control feature works in the following manner:

1. PCF sends flowStatus attribute in TrafficControlData referenced by the PCC rule. The value of this attribute is set to "enabled", "disabled", "enable_uplink", or "enable_downlink" based on the PCF decision.
2. On receiving this attribute, the SMF instructs the UPF to open or close the GATE for the UL or DL Packet Detection Rule (PDR), or both UL and DL PDRs for the associated PCC rule. The Gate Status Information Element (IE) in Create QoS Enhancement Rule (QER) or Update QER associated with the PDR is set to OPEN or CLOSED.
3. If there is any subsequent change, the PCF triggers a N4 modification request to change the GATE status.

Standard Compliance

The Gating Control feature complies with 3GPP TS 29.512, v15.2.0.

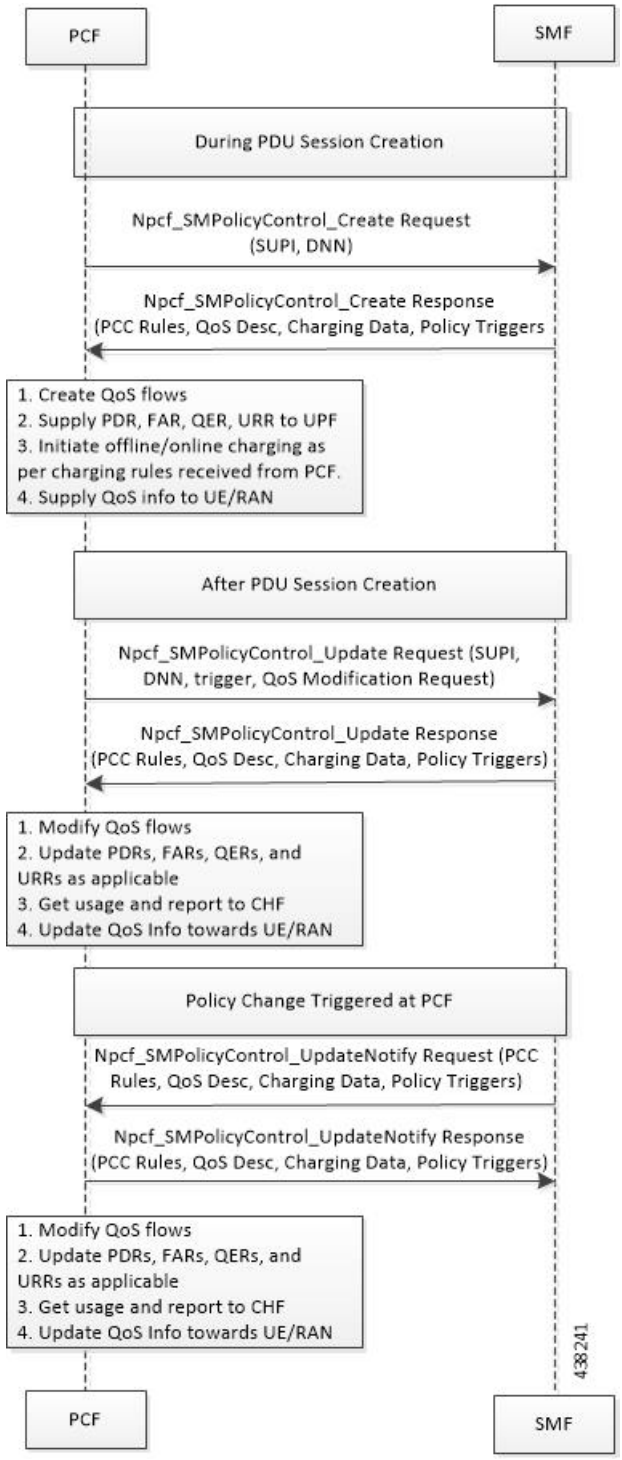
How it Works

The SMF requests the policy information from PCF. The PCF in turn provides the policy rules during and after PDU session creation to enable the dynamic policy application. Dynamic policy management involves the following operations:

- Policy Context Creation: This operation is performed at the time of PDU session create and the PCF sends the PCC rules and the associated QoS, Charging and other policy data in the response message.
- Policy Context Update: For any RAN-initiated or UE-initiated policy updates and for notification of trigger events, the SMF initiates a policy context update. In response, the PCF sends the changed policy data that impacts the QoS and charging.
- Policy Context Update Notification: During the lifecycle of a PDU session, the PCF can initiate a policy update based on interaction with the AF or local configuration changes at PCF. The SMF handles the updated policy rules when received in a notification from the PCF.
- Policy Context Delete: At the end of a PDU session, the SMF terminates the Policy Context with PCF.

The following figure illustrates the dynamic policy management procedure for a PDU session.

Figure 107: Dynamic Policy Management Call Flow



Standards Compliance

The Dynamic PCC Rules Enforcement feature complies with the 3GPP TS 29.512, Release 15.2.0.

Limitations

The Dynamic PCC Rules Enforcement feature has the following limitations:

- SMF supports only the following combination of operations:
  - Creation of new PCC Rule with new QoS descriptor to create new QoS Flow
  - Addition of new PCC Rule to an existing QoS Flow
  - Removal of PCC rule
  - Updating of GBR/MBR parameters associated with the rule
  - Session AMBR Changes
  - Session AMBR Changes and PCC Rules cannot be combined in the same update operation
- The current implementation supports only QoS Descriptors with standard 5QI and ignores the non-standard ones. If all the QoS Desc received are non-standard, then all are ignored and the default one created by SMF is used.

Configuring the Dynamic PCC Rules Enforcement Feature

This section describes how to configure the Dynamic PCC Rules Enforcement feature.

Configuring the Dynamic PCC Rules Enforcement feature involves the following steps:

1. Creating QoS Profile
2. Configuring QoS Parameters
3. Defining QoS Profile in DNN Profile Configuration

Creating QoS Profile

This section describes how to create an instance of a quality of service (QoS) profile.

```
configure
   profile qos qos_profile_name
   end
```

NOTES:

- **qos** *qos_profile_name*: This command creates a quality of service profile and provides access to the QoS Profile Configuration mode to use the commands to configure the QoS parameters. See the qos-profile section of the Command Line Interface Reference for command information. *qos_profile_name* must be an alphanumeric string uniquely identifying the QoS profile.

Configuring QoS Parameters

This section describes how to configure the QoS parameters.

```
configure
   profile qos qos_profile_name
      ambr { ul uplink_ambr | dl downlink_ambr }
      arp {  preempt-cap preemption_capability  | preempt-vuln
preemption_vulnerability | priority-level priority_level}
      max data-burst burst_volume
      priority qos_priority
      qi5 5qi_value
      end
```

NOTES:

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**: Defines the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap** *preemption_capability*: Specifies the preemption capability flag. Options are:
  - MAY_PREEMPT: Bearer may be preempted
  - NOT_PREEMPT: Bearer cannot be preempted
- **arp preempt-vuln** *preemption_vulnerability*: Specifies the preemption vulnerability flag. Options are:
  - PREEMPTABLE: Bearer may be preempted
  - NOT_PREEMPTABLE: Bearer cannot be preempted
- **arp priority-level** *priority_level*: Defines the Allocation and Retention Priority (ARP) for the service data. The default value of *priority_level* is 8.
- **max data-burst** *burst_volume*: Defines the maximum data burst volume. *burst_volume* must be an integer value in the range of 1–4095.
- **priority** *qos_priority*: Specifies the 5QI priority level. *qos_priority* must be an integer value in the range of 1–127.
- **qi5** *5qi_value*: Specifies the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi_value* must be an integer value in the range of 0–255.

Defining QoS Profile in DNN Profile Configuration

This section describes how to configure the QoS profile in the existing DNN profile configuration.

```
configure
   profile dnn dnn_profile_name
      qos-profile qos_profile_name
      end
```

NOTES:

- **qos-profile** *qos_profile_name*: This command defines locally configured default QoS profile. This profile is configured under the existing DNN Profile Configuration. *qos_profile_name* must be the name of the configured QoS profile.

Verifying the Dynamic PCC Rules Enforcement Feature Configuration

This section describes how to verify the Dynamic PCC Rules Enforcement feature configuration.

Use the following show command to verify the feature configuration details.

show full-configuration

The following is an example of this show command output.

```
show full-configuration
profile dnn dnn1
qos-profile qos1
!
profile qos qos1
ambr ul 1024
ambr dl 1024
qi5 128
arp priority-level 8
arp preempt-cap NOT_PREEMPT
arp preempt-vuln NOT_PREEMPTABLE
priority 9
max data-burst 2048
exit
```

Troubleshooting Information

This section provides information for troubleshooting any issues that may arise during the feature operation.

The SMF maintains various logs such as trace logs, event logs, and so on. Use **kubectl get pods -n** *namespace* CLI command to check all the pods and the services that are currently running. Then, use **kubectl logs** *podname* **-n** *namespace* command to display the log in a pod.

If you encounter any error during the operation of this feature, use the SMF service logs for a particular subscriber session to identify the issues and determine the solution to your problem.

Static PCC Rules Support

Feature Description

Static PCC rules are configured in the SMF. These rules can be activated immediately upon PDU session establishment. Static rule is identified by the ruledef configuration using the **action priority** CLI command.

The local configuration on SMF represents the rulebase which is sent to the UPF during session establishment. The SMF uses the configuration representing the PCC rules, QoS Desc, and Charging Data received from PCF to perform QoS flow binding. This configuration is present in the UPF as well. The SMF does not send the PDRs, QERs, and FARs, instead sends only the rulebase name in a default PDR (referred as rulebase PDR) over the N4 interface. The UPF generates the PDRs, FARs, QERs, and URRs for predefined rules based on the rulebase configuration.

Important The Static PCC Rules Support on SMF is applicable to both 4G and 5G calls.

Relationships

This feature utilizes the functionalities provided by PDU Session Lifecycle feature.

How it Works

PCF must send the rulebase name to enable the static PCC rule support on SMF.

When the PCF provides the rulebase name, the SMF performs the following steps during the PDU session creation:

1. The SMF sends Npcf_SMPolicycontrolCreate message to PCF. In response to this message, the PCF may send SMPolicyDecision with a PccRule. If the rule ID of the PccRule is in cbn# rulebase name format, the SMF assumes that the rule id is representing a rulebase name.
2. The SMF sends the rulebase name to the UPF in PFCP Session Establishment Request in a proprietary IE within Create PDR IE.

Note The SMF sends this name only in the default PDR which does not have any SDF filters. No other PDR, FAR, QER, and URR are sent to the UPF for the static rules. The UPF can derive the same from the rulebase name.

Pre-processing During Configuration

Once the Active Charging Service configuration is done (including rulebase, associated ruledefs, and charging actions), SMF processes the configured values and derives PCC Rules, QoSData, and ChargingData from the configured values. The following principles are used to create these entities:

1. QoSData:
   a. Each configured charging action results in a QoSDesc creation.
   b. The **flow-limit-bandwidth** configured under charging action provides the GBR/MBR for the QoSData.
   c. The QCI and ARP configured in charging action constitute the 5QI and ARP of the QoSData. If no QCI and ARP are configured, the 5QI and ARP of the default QoS flow are associated with this QoSData.
2. ChargingData:
   a. The **billing-action** configuration under charging action determines whether offline charging is enabled in the created ChargingData.
   b. The **cca charging credit** configuration under charging action determines whether online charging is enabled in the created ChargingData.
   c. The rating group and service ID of the ChargingData are provided by content-id and service-identifier configuration under charging action.

3. PCCRule:
   a. Each ruledef under a rulebase results in creation of a PCCRule.
   b. The **packet-filter** configured under charging action is used for the FlowInformation in the PCCRule.
   c. The QoSData and ChargingData associated with this ruledef in the rulebase configuration form the refQoS and refChg for this PCCRule.

All the created PCCRules, QoSData, and ChargingData are saved per rulebase.

During PDU Session Creation

1. During PDU session creation, PCF sends the rulebase name (value configured under upf-apn is selected if the PCF does not send it) as PCCRule with ID set to cbn# configured rulebase name. It may also send any predefined rule to be activated as another PCCRule with ID set to crn# configured ruledef name. All such PCC rules will have only the RuleId attribute present.
2. On receiving such a request, SMF selects the constructed PCCRules, QoSData, and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On the N4 interface, the SMF sends the rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase".
4. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
5. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create the corresponding QER and URR.
6. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
7. For all static and activated predefined rules, QoSRules are sent on N1 interface if packet-filters were configured.
8. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

During PDU Session Modification

1. During PDU session modification, PCF sends the rulebase name as PCCRule with ID set to cbn#configured rulebase name. In case of predefined rule PCF can activate new rule crn#configured ruledef name or delete the existing rule (crn#"nil"). All such PCC Rules will have only the RuleId attribute present.
2. On receiving new rule addition request, SMF selects the constructed PCCRules, QoSData and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On receiving an existing rule deletion request, if the SMF received a ruledef name with nil value or a rulebase name different from the existing one, the SMF deletes the QoS flows which correspond to previous rulebase name or ruledef in QoSModel.

4. On N4 interface, SMF sends the new rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase" and RemovePDR with PDR ID which correspond to the old rulebase name.
5. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
6. For all deactivated predefined rules, SMF sends RemovePDR with PDR ID which corresponds to the predefined rule.
7. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create or delete the corresponding QER and URR.
8. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
9. For all static and activated/deactivated predefined rules, QoSRules are sent on N1 interface if packet-filters were configured.
10. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated/deactivated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

Limitations

The Dynamic PCC Rules Enforcement feature has the following limitations:

- SMF supports only the following combination of operations:
  - Creation of new PCC Rule with new QoS descriptor to create new QoS Flow
  - Addition of new PCC Rule to an existing QoS Flow
  - Removal of PCC rule
  - Updating of GBR/MBR parameters associated with the rule
  - Session AMBR Changes
  - Session AMBR Changes and PCC Rules cannot be combined in the same update operation
- The current implementation supports only QoS Descriptors with standard 5QI and ignores the non-standard ones. If all the QoS Desc received are non-standard, then all are ignored and the default one created by SMF is used.

Configuring the Static PCC Rules Support

This section describes how to configure the Static PCC Rules Support on SMF.

The configuration for static and predefined rules is based on the ECS configuration of the StarOS based P-GW. This is to ensure that the UPF can work seamlessly with the SMF.

Configuring the Static PCC Rules Support involves the following steps:

1. Configuring ACS
2. Configuring Charging Action

3. Configuring Packet Filter
4. Configuring ACS Ruledef
5. Configuring ACS Group of Ruledefs
6. Configuring Rulebase and Predefined Rule Prefix
7. Configuring ACS Rulebase (ACS Configuration Mode)
8. Configuring URR ID
9. Configuring GTPP Group
10. Configuring Access Point Name (APN)
11. Associating GTPP Group with APN
12. Configuring ACS Rulebase (APN Configuration Mode)
13. Defining UPF APN Profile in DNN Profile Configuration
14. Configuring QoS Parameters
15. Associating Default Session Rule to DNN Profile

Configuring ACS

ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.

Important In this release, only one active charging service can be configured per system.

This section describes how to configure ACS.

```
configure
   active-charging service service_name
   end
```

NOTES:

- **active-charging service** *service_name*: Specifies the name of an Active Charging Service. *service_name* must be an alphanumeric string of 1 to 15 characters.
- If the named ACS does not exist, it is created, and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured. If the named ACS already exists, the CLI mode changes to the ACS Configuration Mode. The ACS Configuration mode is used to manage ACS or enhanced charging service (ECS) configurations.

Configuring Charging Action

This section describes how to configure charging action. The charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, and so on. The charging action will also determine the metering

principle—whether to count retransmitted packets and which protocol field to use for billing (L3, L4, L7, and so on).

The charging action configuration is used to define the QoS and charging related parameters associated with ruledefs.

```
configure
   active-charging service service_name
      charging-action charging_action
       allocation-retention-priority priority  [ pci pci_value  | pvi pvi_value

        billing-action egcdr
        cca charging credit [ rating-group coupon_ id ] [
preemptively-request ]
        content-id content_id
        flow action { discard [ downlink | uplink ] | redirect-url
redirect_url | terminate-flow }
        flow limit-for-bandwidth { { direction { downlink | uplink }
peak-data-rate bps peak-burst-size bytes violate-action { discard |
lower-ip-precedence } [ committed-data-rate bps committed-burst-size bytes
 [ exceed-action { discard | lower-ip-precedence } ] ] } | { id id } }
        nexthop-forwarding-address ipv4_address/ipv6_address
        qos-class-identifier qos_class_identifier
        service-identifier service_id
        tft packet-filter packet_filter_name
        tft-notify-ue
        tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value } [ downlink |
uplink ]
```

NOTES:

- **charging-action** *charging_action_name*: Specifies the name of a charging action. *charging_action_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.
- If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.
- **allocation-retention-priority** *priority* **[pci***pci_value* **| pvi** *pvi_value* **: Configures the Allocation Retention Priority (ARP).** *priority* **must be an integer value in the range of 1-15.**
  - **pci** *pci_value* : **Specifies the Preemption Capability Indication (PCI) value. The options are:**
    - MAY_PREEMPT - Flow can be preempted. This is the default value.
    - NOT_PREEMPT - Flow cannot be preempted
  - **pvi** *pvi_value*: Specifies the Preemption Vulnerability Indication (PVI) value. The options are:
    - NOT_PREEMPTABLE - Flow cannot be preempted. This is the default value.
    - PREEMPTABLE - Flow can be preempted

- **billing-action**: Configures the billing action for packets that match specific rule definitions.
- **cca charging credit**: Enables or disables Credit Control Application (CCA) and configures the RADIUS/Diameter prepaid charging behavior.
- content-id: Configures the rating group.
- flow action: Specifies the action to take on packets that match rule definitions.
- flow limit-for-bandwidth: Configures the QoS parameters such as MBR, GBR, and so on.
  - peakdatarate(MBR): Default is 3000 bps
  - peakburstsize: Default is 3000 bytes
  - committedDataRate(GBR): Default is 144000 bps
  - committedBurstSize: Default is 3000 bytes
- **nexthop-forwarding-address** *ipv4_address/ipv6_address* ,: Configures the nexthop forwarding address.
- **qos-class-identifier** *qos_class_identifier* : Configures the **QoS Class Identifier** (QCI) for a charging action. *qos_class_identifier* must be an integer value in the range of 1-9 or from 128-254 (Operator specific).
- **service_identifier** *service_id*: Configures the service identifier to use in generated billing records.*service_id* must be an integer value in the range of 1-2147483647.
- **tft packet-filter** *packet_filter_name*: Specifies the packet filter to add or remove from the current charging action. *packet_filter_name* must be the name of a packet filter, and must be an alphanumeric string of 1 to 63 characters.
- **tft-notify-ue**: Control the TFT updates towards the UE based on certain trigger conditions.
- **tos**: Configures the Type of Service (ToS) octets.

Configuring Packet Filter

This section describes the commands that are used to configure packet filter.

```
configure
  active-charging service service_name
    packet-filter packet_filter_name
       direction { bi-directional | downlink | uplink }
      ip local-port { = port_number | range start_port_number to end_port_number
}
       ip protocol = protocol_number
      ip remote-port { = port_number | range start_port_number to end_port_number
}
       ip tos-traffic-class = { type-of-service | traffic class } mask {
= mask-value}
       priority priority
       end
```

NOTES:

- **packet-filter** *packet_filter_name*: Configures the packet filters to be sent to UE. *packet_filter_name* must be the name of the packet filter, and must be an alphanumeric string of 1 to 15 characters.
- **direction { bi-directional | downlink | uplink }**: Configures the direction in which the packet filter has to be applied. The default value is **bi-directional.**
- **ip local-port**: Configures the IP 5-tuple local port(s) for the current packet filter.
- **ip protocol**: Configures the IP protocol(s) for the current packet filter.
- **ip remote-address**: Configures the IP remote address(es) for the current packet filter.
- **ip remote-port**: Configures the IP remote port(s) for the current packet filter.
- **ip tos-traffic-class**: Configures Type of Service (TOS)/Traffic class under charging action in the Packet filter mode.
- **priority** *priority*: Configures the current packet filter's priority.

Configuring ACS Ruledef

A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.

This section describes how to create, configure, or delete ACS rule definitions.

```
configure
   active-charging service service_name
      ruledef ruledef_name
         ip any-match [ = | != ] [ TRUE | FALSE ]
         ip dst-address { operator { { ipv4_address | ipv6_address } | {
ipv4_address/mask | ipv6_address/mask} | address-group ipv6_address } | { !range |
 range } host-pool host_pool_name }
         multi-line-or all-lines
         rule-application { charging | post-processing | routing }
         end
```

NOTES:

- **ruledef** *ruledef_name*: Specifies the ruledef to add, configure, or delete. *ruledef_name* must be the name of an ACS ruledef, and must be an alphanumeric string of 1 to 63 characters, and can contain punctuation characters. Each ruledef must have a unique name. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.
- If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
- If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef. The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).
- **ip any-match [= | !=] [TRUE | FALSE]:** This command defines the rule expressions to match IPv4/IPv6 packets. The *operator* and *condition* in the command specifies the following:
  - *operator*
    - !=: Does not equal

- < =: Equals

- *condition*
  - FALSE
  - TRUE

- **ip dst-address {** *operator* **{ {** *ipv4_address* **|** *ipv6_address* **} | {** *ipv4_address/mask* **|***ipv6_address/mask* **} | address-group** *ipv6_address* **} | { !range | range } host-pool** *host_pool_name* **}**: This command allows defining rule expressions to match IP destination address field within IP headers.
  - *ipv4_address* **|** *ipv6_address*: Specifies the IP address of the destination node for outgoing traffic. *ipv4_address* **|** *ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
  - *ipv4_address/mask* **|** *ipv6_address/mask*: Specifies the IP address of the destination node for outgoing traffic. *ipv4_address/mask* **|** *ipv6_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.
  - *address-group ipv6_address*: Specifies a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2-byte range input can be configured together within a given IPv6 address.
  - **host-pool** *host_pool_name*: Specifies the name of the host pool. *host_pool_name* must be an alphanumeric string of 1 to 63 characters.
  - The *operator* in the command specifies the following:
    - !=: Does not equal
    - <: Lesser than or equals
    - =: Equals
    - >=: Greater than or equals

- **multi-line-or all-lines**: This command allows a single ruledef to specify multiple URL expressions. When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.
- **rule-application { charging | post-processing | routing }**: This command specifies the rule application for a rule definition**.**
  - **charging**: Specifies that the current ruledef is for charging purposes.
  - **post-processing**: Specifies that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.
  - **routing**: Specifies that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled.

Configuring ACS Group of Ruledefs

A group-of-ruledefs can contain optimizable ruledefs. Ruledef group optimization depends on the optimization ability of ruledefs in the group-of-ruledefs, and the optimization configuration of the group in a rulebase.

Upon adding a new ruledef, the following checks occur:

- Determines if the new ruledef is part of any existing group of ruledefs
- Identifies if the new ruledef requires optimization

Use the following configuration to combine a set of ruledefs together to apply the same charging action on them.

```
configure
   active-charging service service_name
      group-of-ruledefs ruledef_group_name
         add-ruledef priority ruledef_priority ruledef ruledef_name
         end
```

NOTES:

- **group-of-ruledefs** *ruledef_group_name* **:** Specifies the ruledef group name to add, configure, or delete. This command allows up to a maximum of 128 group of ruledef configurations.
- **add-ruledef:** This command allows you to add or remove ruledefs from a group-of-ruledefs. This command allows up to a maximum of 128 ruledef configurations.
- **priority:** Specifies the priority of the ruledef in the current group of ruledefs. *ruledef_priority* is an integer from 1 through 10000.
- **ruledef** *ruledef_name*: Specifies name of the ruledef to add to the current group-of-ruledefs. *ruledef_name* must be the name of an ACS ruledef, and must be an alphanumeric string of 1 to 63 characters.

Configuring Rulebase and Predefined Rule Prefix

Rulebase and predefined rule prefix configuration is mandatory for static rule installation from PCF. The SMF supports the predefined rule installation with prefix and without prefix. The SMF also supports the group-of-ruledef installation for both predefined and static rules.

Use the following configuration to configure the rulebase prefix and predefined rule prefix.

```
configure
   profile network-element pcf pcf_service_name
      predefined-rule-prefix predef_rule_prefix
      rulebase-prefix rulebase_prefix
      end
```

NOTES:

- **predefined-rule-prefix** *predef_rule_prefix* **:** Specifies the predefined rule prefix to be added. For example, the prefix for predefined rule is **cbr**.
- This is an optional configuration for the predefined rule. When there is no prefix defined within the PCF network element profile, the predefined rule application behaves as defined in the 3GPP TS 29.244 specification.

- **rulebase-prefix** *rulebase_prefix* **:** Specifies the rulebase prefix to be added. For example, the prefix for rulebase is **rbn**. This is a mandatory configuration for the static rule.

Configuring ACS Rulebase (APN Configuration Mode)

This section describes how to enable and configure an ACS rulebase to be used for subscribers who use the configured APN.

```
configure
   apn apn_name
      active-charging rulebase rulebase_name
      end
```

NOTES:

- **active-charging rulebase** *rulebase_name*: Specifies the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.

Configuring URR ID

This section describes how to configure the Usage Reporting Rules (URR) ID for the rating and service groups.

```
configure
   active-charging service service_name
      urr-list list_name
         rating-group rating_id service-identifier service_id_value urr-id
urr_id_value
  end
```

NOTES:

- **urr-list** *list_name*: Specifies the name of the URR list, and must be an alphanumeric string of 1 to 63 characters.
- **rating-group** *rating_id*: Specifies the rating ID used in charging. *rating_id* must be an integer value in the range of 0-2147483647.
- **service-identifier** *service_id_value*: Configures the service identifier value. *service_id_value* must be an integer value in the range of 0-2147483647.
- **urr-id** *urr_id_value*: Configures URR identifier for rating/service group. u*rr_id_value* must be an integer value in the range of 1-8388607.
- The URR ID configuration is per rating group and service ID. For different rating group and service ID combinations, use the URR ID configuration command as many times as needed.

Configuring GTPP Group

This section describes the commands that are used to configure GTPP group.

```
configure
   gtpp group group_name
```

```
gtpp trigger { time-limit | volume-limit }
end
```

NOTES:

- **gtpp group** *group_name*: Specifies the GTPP group name. *group_name* must be an alphanumeric string of 1 to 63 characters.
- **gtpp trigger { time-limit | volume-limit }**: Configures triggers for CDR.
  - **time-limit**: Enables time-limit trigger for the CDR.
  - **volume-limit**: Enables volume-limit trigger for the CDR.

Configuring Access Point Name (APN)

This section describes how to create APN templates. This APN configuration represents the access point configuration in the UPF and further facilitates configuring a rulebase name within.

```
configure
   apn apn_name
   end
```

NOTES:

- **apn** *apn_name*: Specifies a name for the APN template as an alphanumeric string of 1 to 62 characters and is case insensitive.

Associating GTPP Group with APN

This section describes how to associate the GTTP group with the configured APN.

```
configure
   apn apn_name
      gtpp group group_name
      end
```

NOTES:

- **gtpp group** *group_name*: Associates the defined GTPP group with the already configured APN.

Configuring ACS Rulebase (ACS Configuration Mode)

This section describes how to create, configure, or delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

Rulebase configuration is the one that combines all the specified configurations together to construct the static and predefined PCC rules.

```
configure
   active-charging service service_name
      rulebase rulebase_name
         action priority action_priority { [ dynamic-only ] |
```

```
static-and-dynamic | timedef timedef_name ] { group-of-ruledefs
ruledefs_group_name | ruledef ruledef_name } charging-action charging_action_name [
 monitoring-key monitoring_key ] [ description description ] }
         cca quota { holding-time holding_time content-id content_id |
retry-time retry_time [ max-retries retries ] }
         cca quota time-duration algorithm { consumed-time seconds [
plus-idle ] | continuous-time-periods seconds | parking-meter seconds } [
content-id content_id ]
         credit-control-group cc_group_name
         dynamic-rule order { always-first | first-if-tied }
        egcdr threshold { interval interval [ regardless-of-other-triggers
 ] | volume { downlink | total | uplink } bytes }
         route priority route_priority ruledef ruledef_name analyzer { dns |
file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms
 | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [
advanced | basic-and-advanced ] | smtp | tftp | wsp-connection-less |
wsp-connection-oriented } [ description description ]
         tcp check-window-size
         tcp mss tcp_mss { add-if-not-present | limit-if-present }
         tcp packets-out-of-order { timeout timeout_duration | transmit [
after-reordering | immediately ] }
         end
```

NOTES:

- **rulebase** *rulebase_name*: Specifies the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.
- **action priority** *action_priority* **{ [dynamic-only] | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[monitoring-key** *monitoring_key* **] [description** *description* **] }**: Configures the priority order in which ruledefs are matched and the associated charging action.
  - *priority* must be an integer value in the range of 1-65535.
  - *monitoring_key* must be an integer value in the range of 100000-4000000000.
- **cca quota { holding-time** *holding_time* **content-id** *content_id* **| retry-time** *retry_time* **[max-retries** *retries* **] }**: Configures the quota for the online charging.
  - *holding_time*: must be an integer value in the range of 1-4000000000
  - *content_id*: must be an integer value in the range of 1-2147483647
  - *retry_time*: must be an integer value in the range of 0-86400
  - *retries*: must be an integer value in the range of 1-65535
- **cca quota time-duration algorithm { consumed-time** *seconds* **[plus-idle] | continuous-time-periods** *seconds* **| parking-meter** *seconds* **} [content-id** *content_id* **]**
  - consumed-time: must be an integer value in the range of 1-4294967295
  - content-id: must be an integer value in the range of 1-2147483647
  - continuous-time-periods: must be an integer value in the range of 1-4294967295

    - parking-meter: must be an integer value in the range of 1-4294967295

- **credit-control-group** *cc_group_name*: Configures the online charging parameters used by this rulebase. *cc_group_name* must be an alphanumeric string of 1 to 63 characters.
- **dynamic-rule order**: Configures the order of dynamic rule matching vs the static rules in a rulebase.
- **egcdr threshold { interval** *interval* **[regardless-of-other-triggers] | volume { downlink | total | uplink } bytes }**: Configures the threshold for offline charging.
    - **interval**: must be an integer value in the range of 60-40000000.
    - **downlink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.
    - **uplink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.
    - **total**: must be an integer value in the range of 100000-4000000000.
- **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced | basic-and-advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**: This command is used only on UPF.
    - *route_priority* must be an integer value in the range of 0-65535.
    - *ruledef_name* must be an alphanumeric string of 1 to 63 characters.
- **tcp check-window-size**: This command is used only on UPF.
- **tcp mss** *tcp_mss*: This command is used only on UPF. *tcp_mss* must be an integer value in the range of 496-65535.
- **tcp packets-out-of-order { timeout** *timeout_duration* **| transmit [after-reordering | immediately] }**: This command is used only on UPF.
    - *timeout_duration* must be an integer value in the range of 100-30000. Default value is 5000.

Defining UPF APN Profile in DNN Profile Configuration

This section describes how to configure the UPF APN profile in the existing DNN Profile Configuration.

```
configure
   profile dnn dnn_profile_name
      upf apn apn_name
      end
```

NOTES:

- **upf apn** *apn_name*: This command enables UPF APN profile configuration. This profile is configured under the existing DNN profile configuration. *apn_name* must be the name of the APN template, and must be an alphanumeric string of 1 to 62 characters.

Configuring QoS Parameters

This section describes how to configure the QoS parameters.

```
configure
   profile qos qos_profile_name
      ambr { ul uplink_ambr | dl downlink_ambr }
      arp {  preempt-cap preemption_capability  | preempt-vuln
preemption_vulnerability | priority-level priority_level}
      max data-burst burst_volume
      priority qos_priority
      qi5 5qi_value
      end
```

NOTES:

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**: Defines the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap** *preemption_capability*: Specifies the preemption capability flag. Options are:
  - MAY_PREEMPT: Bearer may be preempted
  - NOT_PREEMPT: Bearer cannot be preempted
- **arp preempt-vuln** *preemption_vulnerability*: Specifies the preemption vulnerability flag. Options are:
  - PREEMPTABLE: Bearer may be preempted
  - NOT_PREEMPTABLE: Bearer cannot be preempted
- **arp priority-level** *priority_level*: Defines the Allocation and Retention Priority (ARP) for the service data. The default value of *priority_level* is 8.
- **max data-burst** *burst_volume*: Defines the maximum data burst volume. *burst_volume* must be an integer value in the range of 1–4095.
- **priority** *qos_priority*: Specifies the 5QI priority level. *qos_priority* must be an integer value in the range of 1–127.
- **qi5** *5qi_value*: Specifies the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi_value* must be an integer value in the range of 0–255.

Verifying the Static PCC Rules Support Feature Configuration

This section describes how to verify the Static PCC Rules Support configuration.

Use the following show command to verify the feature configuration details.

show full-configuration

The following is an example of this show command output.

```
active-charging service acs
charging-action ca1
  arp priority-level 15 preempt-cap MAY_PREEMPT preempt-vuln PREEMPTABLE
  cca charging credit preemptively-request
  content-id 320001
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 1000000
 violate-action discard committedDataRate 2000000 committed-burst-size 2000000 exceed-action
 lower-ip-precedence
```

```
  nexthop-forwarding-address fa00:965a:c263:25::16/128
  qos-class-identifier 9
  service-identifier 32000
  tft packet-filter pf1
  tft-notify-ue
  tos af11 downlink
rulebase rb1
  cca quota time-duration algorithm parking-meter 1000 content-id 18000
  credit-control-group cg1
  dynamic-rule order first-if-tied
  egcdr threshold volume total 400000
  tcp packets-out-of-order transmit immediately
  action priority 95 timedef ruledef rd6 charging-action ca6 description ruledef
  action priority 96 ruledef rd3 charging-action ca5
  action priority 97 group-of-ruledefs grd3 charging-action ca4 monitoring-key 200000
  action priority 98 static-and-dynamic group-of-ruledefs grd2 charging-action ca2
  action priority 99 dynamic-only ruledef rd1 charging-action ca1 monitoring-key 100000
  action priority 100 dynamic-only group-of-ruledefs grd1 charging-action ca1 monitoring-key
 100000 description gruledefs
  route priority 1 ruledef rd1 analyzer dns description dns
exit
packet-filter pk1
  direction uplink
  ip local-port = 23
  ip protocol = 23
  ip remote-address = 10.10.10.0/24
  ip remote-port = 23
  ip tos-traffic-class = 23 mask = 10
  priority  4
exit
ruledef prepaidBgl
  multi-line-or all-lines
  rule-application charging
  ip any-match = TRUE
  ip server-ip-address range host-pool 12
  ip dst-address = 10.10.10.10
exit
urr-list urrlocal
  rating-group 1 service-identifier 1 urr-id 2
  rating-group 1 service-identifier 3 urr-id 2
exit
exit
```

Use the following show command to verify the group-of-ruledefs configuration details.

show running-config

The following is an example of this show command output.

```
show running-config
profile network-element pcf pcf1
rulebase-prefix   rbn
predefined-rule-prefix cbr
!
active-charging service acs1
group-of-ruledefs IPV6-whtlst-https_2300
  add-ruledef priority 1 ruledef IPV6-whtlst-https_2300_01
  add-ruledef priority 2 ruledef IPV6-whtlst-https_2300_02
  add-ruledef priority 3 ruledef IPV6-whtlst-https_2300_03
  add-ruledef priority 4 ruledef IPV6-whtlst-https_2300_04
  add-ruledef priority 5 ruledef IPV6-whtlst-https_2300_05
  add-ruledef priority 6 ruledef IPV6-whtlst-https_2300_06
  add-ruledef priority 7 ruledef IPV6-whtlst-https_2300_07
  add-ruledef priority 8 ruledef IPV6-whtlst-https_2300_08
```

```
  add-ruledef priority 9 ruledef IPV6-whtlst-https_2300_09
  add-ruledef priority 10 ruledef IPV6-whtlst-https_2300_10
  add-ruledef priority 11 ruledef IPV6-2dns-whtlst-https_2300_01
  add-ruledef priority 12 ruledef IPV6-2dns-whtlst-https_2300_02
  add-ruledef priority 13 ruledef IPV6-2dns-whtlst-https_2300_03
exit
group-of-ruledefs rdg1
  add-ruledef priority 10 ruledef rd2
  add-ruledef priority 12 ruledef rd1
exit
exit
```

Predefined PCC Rules

Feature Description

Most of the concepts applicable for static rules also apply for predefined rules. The configuration set, mechanism for QoS binding and pre-constructed QoS model remain the same.

Important Predefined PCC Rules are applicable to both 4G and 5G calls.

Predefined Rules vs Static Rules

This section lists the differences between the predefined and static rules.

- Predefined rule is identified by the **dynamic-only** keyword in the action priority associated with a ruledef under rulebase configuration.
- Predefined rules are not activated automatically but are enabled or disabled by PCF on a per rule basis. The PCF sends a PCC rule with the ruledef name alone or ruledef and rulebase names together as the rule ID to activate the predefined rule and sends the PCC rule map with null entry for the ruledef previously activated to deactivate a predefined rule.
- The QoS binding and modelling is not done for predefined rules at the time of configuration unlike the static rule. Instead during PDU session activation/modification the ECS configuration of activated ruledefs are considered to create or change the QoS model applicable for the session.
- On N4 interface, one PDR and corresponding FAR per ruledef activated by the PCF is sent to the UPF with ruledef name in the Activate predefined Rule IE and rulebase name is sent in Rulebase IE in default PDR. On rule removal, the corresponding PDR is removed.

Note The PCF sends the predefined rules, and activates these rules only if the UPF APN is configured with "rulebase" name. Otherwise, the PCF must send the rule name along with the "rulebase" name.

Combined Application of Static, Predefined, and Dynamic Rules

All three static, predefined, and dynamic rules can coexist for a session. In such a case:

- Pre-constructed QoS model is prepared only for static rules. During PDU session activation/modification, any dynamic and predefined rules are evaluated to modify the QoS model and accordingly modifications are done on N1, N2, and N4 interfaces.
- If the rating-group and service ID for a dynamic rule are the same as that of a configured predefined and static rule, then the URR ID for the static and predefined rule is retained even for the dynamic rule.

Support for Configuring the Bandwidth ID

Feature Description

The SMF expects the user to configure the bandwidth limitation, for both downlink and uplink packets, in all charging actions, even if the bandwidth limitation configuration is the same for all the charging actions.

To optimise these configurations, the SMF allows the user to define a bandwidth ID to include all bandwidth related configurations and associate the bandwidth ID under the charging actions.

If the bandwidth value is changed, the new subscribers use the configured bandwidth values while the existing subscribers continue to use the old values.

Limitations

The SMF allows up to 64 k flow ID configurations within the bandwidth-policy.

Configuring Bandwidth ID

Use the following configuration to define the bandwidth ID within the charging action.

```
configure
   active-charging service service_name
      bandwidth-policy policy_name
      flow limit-for-bandwidth id bandwidth_id group-id group_id
      group-id group_id direction { downlink | uplink } peak-data-rate
peak_data_rate peak-burst-size peak_burst_size violate-action { discard |
lower-ip-precedence } [ committed-data-rate committed_data_rate
committed-burst-size committed_burst_size [ exceed-action { discard |
lower-ip-precedence } ] ]
      exit
   active-charging service service_name
   charging-action charging_action_name
      flow limit-for-bandwidth bandwidth_id
      end
```

- **flow limit-for-bandwidth id** *bandwidth_id* : Defines a bandwidth ID to include all the bandwidth related configurations within the charging action for predefined and static rules.

  bandwidth_id is an integer ranging from 1 to 65535.

- **group-id** *group_id*: This command specifies the group ID as an integer ranging from 1 to 65535.

The group ID identifies the QoS parameters such as MBR, GBR, and so on. Each group ID is mapped to a particular bandwidth ID.

- If the bandwidth ID is configured and the individual uplink and downlink limit-for-bandwidth are also configured in the charging actions, then the bandwidth ID configuration takes the precedence.

Verifying Bandwidth ID Configuration

Use the following show command to verify the bandwidth ID configuration.

show config-error

This show command helps in identifying any invalid configurations such as the configured bandwidth ID being removed but still defined in the charging action. For such invalid configurations, this show command displays appropriate errors as shown in the following example output:

show-config-error

```
ERROR COMPONENT      ERROR DESCRIPTION
-------------------------------------------------------------------------------------------
RuleBase        Default bandwidth policy does not exist in rulebase <rba1> for charging
action <ca1> .Dropping ruleDef <rda1>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda60>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda61>
ChargingAction  Packet filter <pkt1234> configured for charging action <ca4> associated
with rulebase <rb1> does not exist
BandWidthPolicy Uplink peak data rate less than commited data rate in charging action
<ca6>Dropping ruleDef <rd6>
```

Generating UE Camping Report for PCF

Feature Description

PCF needs to be aware of UE location, RAT type, access type, and other details to provision relevant policies during the PDU session life cycle. To facilitate this, during PCF initiated policy update procedure, the SMF sends "UeCampingRep" attribute in the response message based on the triggers enabled by PCF.

The SMF sends the UeCampingRep to PCF as per the Table 5.5.2.2-2 defined in 3GPP specification 29.512. When validation of all the PCF provided rules succeed, the SMF sends the UeCampingRep in the update response message to the PCF.

If validation of any of the rules fail, then the SMF sends the ueCampingRep in “PartialSuccessReport” as defined in 4.2.3.2 section of 3GPP specification 29.512.

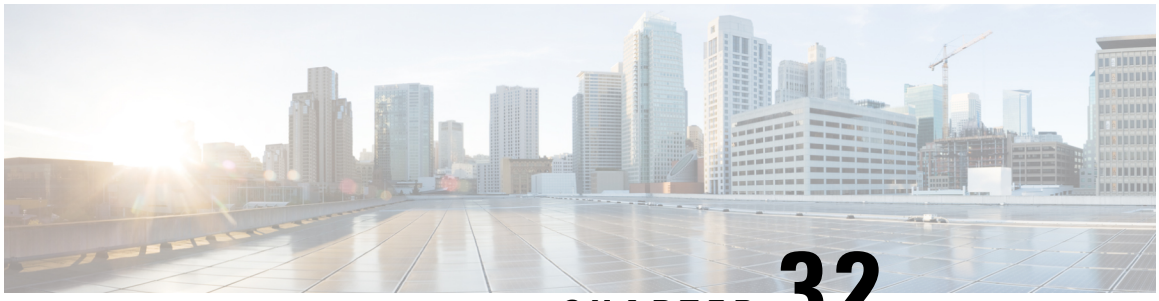
The fields in the "UeCampingRep" IE are populated based on the following triggers set by PCF.

- Access type (AC_TY_CH)
- RAT change (RAT_TY_CH)
- User location change (SAREA_CH)
- PLMN Change (PLMN_CH)

The SMF supports the following attributes:

- accessType
- ratType
- servingNetwork
- userLocationInfo

Important The SMF currently does not support the ueTimeZone attribute.



CHAPTER 32

RADIUS Client

Feature Summary and Revision History

Summary Data

Table 135: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required

Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 136: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

In 5G architecture, serving network authenticates the Subscription Permanent Identifier (SUPI) during authentication and key agreement between UE and the network. In addition, the secondary authentication can also be performed for data networks outside the mobile operator domain. For this purpose, various EAP-based authentication methods and associated credentials can be used among which, RADIUS protocol is one of the widely used authentication protocols.

The RADIUS Client feature, which is integrated with SMF Network Function, enables generic Cloud Native 5G RADIUS functionality to be used for the authentication purpose. When RADIUS Client feature is enabled, the SMF performs secondary authentication with the configured external AAA server (for example, RADIUS Server) as per 3GPP TS 23.501.

NOTE: Only RADIUS protocol is currently used for secondary authentication.

RADIUS Client feature supports the following functionality:

- Server Selection
- Monitor Server and Dead Server Detection
- Timeout and Retry

Server Selection

RADIUS servers are configured with IP:Port as the key. The "algorithm" CLI specifies the fail-over/load-balancing algorithm to select the RADIUS server to which the request (authentication/accounting) must be sent. Servers that are marked "dead" are not considered for selection until they are marked "alive". The supported algorithms are first-server and round-robin.

- First-server: Specifies that the request must be sent to RADIUS server with the highest priority. If this server becomes unreachable, the request is sent to the server with the next highest configured priority. This is the default algorithm.
- Round-robin: Specifies that the request must be sent based on load balancing in circular queue fashion. The server that is last used is stored to maintain the round-robin selection. The order of the list is based on the configured relative priority of the servers.

Monitor Server and Dead Server Detection

MonitorServer revisits the server database and marks the server which has not received response beyond the configured "timeout" value after the first request is sent to it. The server is marked "dead" and remains in

dead-state for seconds configured as "deadtime". After the "deadtime" elapses, the server's dead-variable is reset to again mark it as up and ready to process requests. If the server is still not reachable, it is marked "dead" as part of the next request response timeout routine.

Timeout and Retry

After a server is selected and request is sent to the server, an entry is maintained in the request queue until response is received from the RADIUS server or until timeout occurs. MonitorRequests is called to check on the requests queue for response timeouts and retry. It walks through all the entries and checks if any request timeout value configured as "responseTimeout" is hit. For such requests, if the number of retries is less than the configured "maxRetries" value, the request is resent to the RADIUS server. Else, if the "maxRetries" count is reached, the request is deleted from the request queue. After a request is deleted, even if response comes for such requests, the response is discarded and not sent to the user.

Architecture

RADIUS Integration in Mobile CNAT Architecture

The Mobile CNAT architecture has four distinct layers:

1. Cloud - Host OS + Kubernetes installation.
2. Runtime - These are the "plugins" to Kubernetes provided by the Cloud. This includes the container runtime (Docker version) and Kubernetes plugins for Volume (storage), Networking, and Load-Balancing.
3. Orchestration - Kubernetes functionality. Kubernetes provides abstractions for provided plugins (Networking/Volumes/Load-Balancing) so the CNAT components do not need to have knowledge of them.
4. Mobile CNAT Components - Application layer where the applications are built for Mobility depending only on Kubernetes as much as possible.

For more details about Mobile CNAT architecture, visit the following link:
https://wwwin-github.cisco.com/pages/mobile-cnat-infrastructure/architecture/arch/cnat_architecture.html

5GC Network Functions (NFs), such as PCF, SMF, and so on, run in the "Application/CNAT Component" layer of this architecture. RADIUS Client is integral part of SMF and PCF NFs.

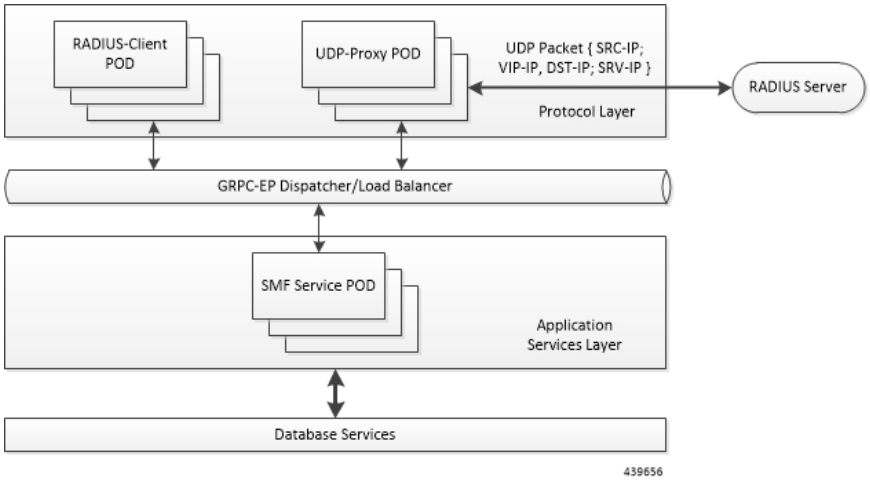
RADIUS Client Integration in SMF

SMF Network Function comprises of loosely coupled micro-services. Micro-service decomposition is based on the following 3-layered architecture:

1. Layer 1: Protocol and Load Balancer Services (Stateless)
2. Layer 2: Application services (Stateless)
3. Layer 3: Database Services (Stateful)

RADIUS Client POD is integrated as part of the "Protocol" layer.

The following figure illustrates the integration of RADIUS Client in SMF.



Radius-EP App (RADIUS-Client POD): RADIUS Client functionality is added in a new POD. It is responsible for handling RADIUS protocol-specific functions such as authentication, accounting, and so on.

NOTE: In this release, only Authentication is supported.

SMF Service App (SMF Service POD): SMF Service App is responsible for providing PDU session service. During session bring-up, SMF service decides if secondary authentication is required or not and acts accordingly.

UDP-Proxy App (UDP-Proxy POD): UDP-Proxy App is enabled with host-networking and helps with sending and receiving of packets using external Virtual-IPs. All RADIUS packets are transmitted out and received from an outside cluster using this app.

How it Works

This section describes about authentication method applied by RADIUS.

RADIUS Authentication Method

RADIUS uses the following authentication methods:

- User-Name: Only MSISDN-based user-authentication is supported. The GPSI/MSISDN value is set as the User-Name in RADIUS Authentication requests (with stripped-off "msisdn-" string). Other methods such as PAP, CHAP, MSCHAP, and so on, are not supported in this release.
- **User-Password: RADIUS server's "secret" key is used as password of the user.**

RADIUS Client - Dictionary

The primary purpose of the dictionary is to map descriptive names to attribute numbers in a packet. For efficiency reasons, each packet contains an encoded version of an attribute. The encoded version is binary data and is non-readable. The secondary function is to define data types for an attribute. On the client side, the dictionary file is used to determine the attribute type and encoding or decoding of attribute values are

based on the type. For example, to determine that the attribute should be interpreted as a User-Name attribute of type string when the header contains Type field as 1. Each RADIUS attribute contains a header with Type, Length, and Value fields. For standard attributes, the type is fixed and for VSA attributes the type is 26. In case of VSA attributes, there are two headers - the outermost is a normal RADIUS attribute header, and the inner header contains information like VSAType, Length, Vendor-Id, and Attribute Value.

The dictionary file is defined based on the RFC .dct file format. The following is an example of RADIUS dictionary file:

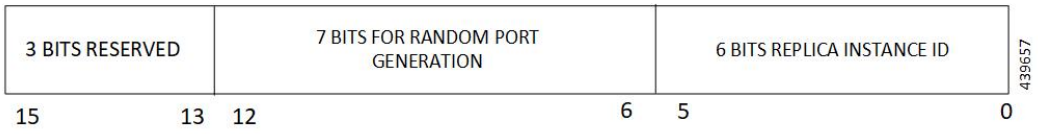
```
# radius standard attributes, vsa with enum values
# format is based on rfc .dct files

# Standard attributes
ATTRIBUTE   User-Name        Standard(1)             string
ATTRIBUTE   User-Password     Standard(2)             octets
ATTRIBUTE   Service-Type          Standard(6)             integer
VALUE       Service-Type              Login-User              1
VALUE       Service-Type               Framed-User             2
VALUE       Service-Type               Callback-Login-User     3
VALUE       Service-Type               Callback-Framed-User4
VALUE       Service-Type               Outbound-User           5
VALUE       Service-Type               Administrative-User     6
VALUE       Service-Type               NAS-Prompt-User         7
VALUE       Service-Type               Authenticate-Only       8
VALUE       Service-Type               Callback-NAS-Prompt   9
VALUE       Service-Type               Call-Check              10
VALUE       Service-Type               Callback-Administrative11

# VSA
ATTRIBUTE   3GPP-IMSI                           3GPP-VSA(1)     string
ATTRIBUTE   3GPP-IMSI-MCC-MNC       3GPP-VSA(8)     string
ATTRIBUTE   3GPP-User-Location-Info                 3GPP-VSA(22)    UeLocType
ATTRIBUTE   3GPP-MS-Time-Zone               3GPP-VSA(23)    octets
```

The first column denotes if it is an ATTRIBUTE entry or VALUE entry to indicate an attribute or enum value of an attribute respectively. The second column contains name of the attribute in case of both ATTRIBUTE and VALUE entries. For ATTRIBUTE entries, the third column denotes if the attribute is a Standard attribute with attribute type number, or in case of VSA attribute it contains the VendorName with vendor attribute type number. For VALUE entries, the third column contains the enum description. The last column denotes the data type of attribute in case of ATTRIBUTE or the enum value of an attribute in case of VALUE entry.

Basic RADIUS attribute types are integer, string, octets, ipaddr, and vsa. If new attribute types are needed, encode/decode functions should be defined in the backend for the newly defined types.

RADIUS Client – UDP Source Port Generation Logic

The following logic is used for generating UDP source Port.



3 Bits - Reserved for future use

6 Bits - Max 64 Replicas instances

7 Bits - Max 128 Source ports per instance

x 256 IDs - Max 32 Outstanding RADIUS Requests per instance

13 Bits Total- Max 8000 Source ports per instance

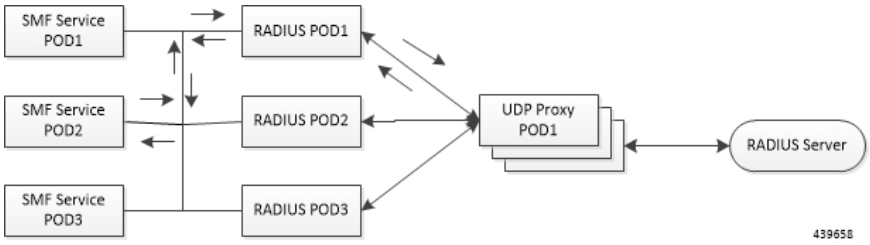
x 256 IDs - Max 2 million Outstanding RADIUS Requests per cluster

RADIUS Client – POD Replica Support

Multiple RADIUS PODs can be spawned based on the need. Replicas work as follows:

- SMF Service requests are sent to any of the RADIUS POD using cluster's load-balancing method. RADIUS POD, which receives the request, initiates access-request packet and uniquely reserves a UDP source Port using the "instance-id" logic.
- UDP-Proxy, when it receives the response back, finds the actual instance of RADIUS POD by decoding the UDP-Dest-Port value, and unicasts the packet to respective RADIUS POD.

The following figure illustrates the way POD replica works.



RADIUS Client – Attributes Encoding

The following attributes in the access-request packet are supported in this release.

ATTRIBUTE	Reference Specification	Encoding Type
USER-NAME	RFC2865 - 5.1	String
PASSWORD	RFC2865 - 5.2	Encrypted String
CALLING-STATION-ID	RFC2865 - 5.31	String
CALLED-STATION-ID	RFC2865 - 5.30	String
NAS-IP-ADDRESS	RFC2865 - 5.4	IPv4 Address
NAS-IDENTIFIER	RFC2865 - 5.32	String
SERVICE-TYPE	RFC2865 - 5.6	Octets - 4 bytes
FRAMED-PROTOCOL	RFC2865 - 5.7	Octets - 4 bytes
NAS-PORT-TYPE	RFC2865 - 5.41	Octets - 4 bytes
NAS-PORT	RFC2865 - 5.5	Octets - 4 bytes
3GPP-IMSI	3GPP 29.061 - 16.4.7.2-1	String
3GPP-CHARGING-ID	3GPP 29.061 - 16.4.7.2-2	Octets - 4 bytes
3GPP-PDP-TYPE	3GPP 29.061 - 16.4.7.2-3	Octets - 4 bytes

ATTRIBUTE	Reference Specification	Encoding Type
3GPP-CHARGING-GATEWAY-ADDR	3GPP 29.061 - 16.4.7.2-4	IPv4 Address
3GPP-GPRS-NEG-QOS-PROFILE	3GPP 29.061 - 16.4.7.2-5	Special Encoded Octets
	3GPP 29.274 - 8.7	
3GPP-SGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-6	IPv4 Address
3GPP-GGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-7	IPv4 Address
3GPP-IMSI-MCC-MNC	3GPP 29.061 - 16.4.7.2-8	String
3GPP-GGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-9	String
3GPP-NSAPI	3GPP 29.061 - 16.4.7.2-10	String
3GPP-SELECTION-MODE	3GPP 29.061 - 16.4.7.2-12	String
3GPP-CHARGING-CHARACTERISTICS	3GPP 29.061 - 16.4.7.2-13	String
3GPP-SGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-18	String
3GPP-IMEISV	3GPP 29.061 - 16.4.7.2-20	String
3GPP-RAT-TYPE	3GPP 29.061 - 16.4.7.2-21	Octet - 1 byte
3GPP-USER-LOCATION	3GPP 29.061 - 16.4.7.2-22	Special Encoded Octets
	3GPP 29.274 - 8.21-4	
	3GPP 29.274 - 8.21-5	
3GPP-MS-TIMEZONE	3GPP 29.061 - 16.4.7.2-23	Special Encoded Octets
	3GPP 29.274 - 8.44	
3GPP-NEGOTIATED-DSCP	3GPP 29.061 - 16.4.7.2-26	Octet - 1 byte

- USER-NAME

  Description: String value encoded as per RFC 2865.

  - 5G call: GPSI value is used, with stripped-off "msisdn-"
  - 4G call: MSISDN value is used, with stripped-off "msisdn-"

  NOTE: PAP, CHAP, and MSCHAP authentication methods are not supported in this release.

- PASSWORD

  Description: Encrypted string value encoded as per RFC 2865.

For both 5G and 4G calls, selected RADIUS server's "secret" is set as user-password.

- CALLING-STATION-ID

  Description: String value encoded as per RFC 2865.

  5G call: GPSI value is used, with stripped of "msisdn-"

  4G call: MSISDN value is used, with stripped of "msisdn-"

- CALLED-STATION-ID

  Description: String value encoded as per RFC 2865.

  For both 5G and 4G calls, DNN value is set as called-station-id.

- NAS-IP-ADDRESS

  Description: IPv4 address value encoded as per RFC 2865.

  For both 5G and 4G calls, user-configured RADIUS Client interface-type's VIP-IP is used.

- NAS-IDENTIFIER

  Description: String value encoded as per RFC 2865.

  For both 5G and 4G calls, user-configured nas-identifier attribute value is used.

- SERVICE-TYPE

  Description: 4-byte Octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, "FRAMED (2)" value is set.

- FRAMED-PROTOCOL

  Description: 4-byte Octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, "GPRS-PDP-CONTEXT (7)" value is set.

- NAS-PORT-TYPE

  Description: 4-byte Octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, "WIRELESS-OTHER (18)" value is set.

- NAS-PORT

  Description: 4-byte Octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, the base value of respective instance is used. That is:

  0x40 00 00 00 is set for replica-0

  0x40 00 00 01 is set for replica-1

- 3GPP-IMSI

  Description: String value encoded as per 3GPP TS 29.061.

  5G call: SUPI value is used.

  4G call: IMSI value is used.

- 3GPP-CHARGING-ID

  Description: 4-byte octet (int) value encoded as per 3GPP TS 29.061.

For both 5G and 4G calls, charging-ID is set.

- 3GPP-PDP-TYPE

  Description: 4-byte octet (int) value encoded as per 3GPP TS 29.061.

  For both 5G and 4G calls, pdp-type is set as follows:

  - 0 = IPv4
  - 2 = IPv6
  - 3 = IPv4v6

- 3GPP-CHARGING-GATEWAY-ADDR

  Description: 4-byte octet (IPv4-address) value encoded as per 3GPP TS 29.061.

  For both 5G and 4G calls, charging gateway address is set.

- 3GPP-GPRS-NEG-QOS-PROFILE

  Description: Octets (special encoding) value encoded as per 3GPP TS 29.061 & 29.274.

  For 5G call, the values from default-qos profile of the system are used and the encoding is performed as follows:

Table 137: Non-GBR case

1-2	<Release indicator>- = "15" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-9	UL Session-AMBR length (UTF-8 encoded)
10-m	UL Session-AMBR (UTF-8 encoded)
(m+1) - (m+2)	DL Session-AMBR length (UTF-8 encoded)
(m+3) – n	DL Session-AMBR (UTF-8 encoded)

Table 138: GBR case

1-2	<Release indicator> = "15" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-9	UL MFBR length (UTF-8 encoded)
10-m	UL MFBR (UTF-8 encoded)
(m+1)-(m+2)	DL MFBR length (UTF-8 encoded)
(m+3)-n	DL MFBR (UTF-8 encoded)

(n+1)-(n+2)	UL GFBR length (UTF-8 encoded)
(n+3)-o	UL GFBR (UTF-8 encoded)
(o+1) – (o+2)	UL GFBR length (UTF-8 encoded)
(o+3) - p	DL GFBR (UTF-8 encoded)

For 4G call, the values from the default-qos profile of the system are used and the encoding is performed as follows:

Table 139: Non-GBR case

1-2	<Release indicator>- = "08" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-11	UL Session-AMBR (UTF-8 encoded)
12-15	DL Session-AMBR (UTF-8 encoded)

Table 140: GBR case

1-2	<Release indicator> = "08" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-11	UL MBR (UTF-8 encoded)
12-15	DL MBR (UTF-8 encoded)
16-19	UL GBR (UTF-8 encoded)
20-23	DL GBR (UTF-8 encoded)

- 3GPP-SGSN-ADDRESS

  Description: 4-byte octet (IPv4-address) value encoded as per 3GPP TS 29.061.

  For 5G call, the AMF address is set.

  For 4G call, the S-GW address is set.

- 3GPP-GGSN-ADDRESS

  Description: 4-byte octet (IPv4-address) value encoded as per 3GPP TS 29.061.

  For both 5G and 4G call, SMF-Service IP is set.

- 3GPP-IMSI-MCC-MNC

  Description: String value encoded as per 3GPP TS 29.061.

  For 5G call, SUPIs MCC and MNC values are set.

For 4G call, IMSIs MCC and MNC values are set.

MCC is first 3 bytes, MNC is next 2 or 3 bytes.

If MCC value is any of the following, then MNC will be of 3 bytes, else MNC will be of 2 bytes.

300 302 310 311 312 313 316 334 338 342 344 346 348 354 356 358 360 365 376 405 708 722 732

- 3GPP-GGSN-MCC-MNC

  Description: String value encoded as per 3GPP TS 29.061.

  For both 5G and 4G call, configured MCC and MNC value of SMF is used.

  MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-SGSN-MCC-MNC

  Description: String value encoded as per 3GPP TS 29.061.

  For 5G call, AMFs MCC and MNC values are set.

  For 4G call, SGWs MCC and MNC values are set.

  MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-NSAPI

  Description: String value encoded as per 3GPP TS 29.061.

  For 5G call, QFI value from the defaultQos profile is set.

  For 4G call, EPS bearer ID is set.

- 3GPP-SELECTION-MODE

  Description: String value encoded as per 3GPP TS 29.061.

  For both 4G and 5G call, value is set to "0".

- 3GPP-CHARGING-CHARACTERISTICS

  Description: String value encoded as per 3GPP TS 29.061.

  For both 4G and 5G call, generic charging character is set.

- 3GPP-IMEISV

  Description: String value encoded as per 3GPP TS 29.061.

  For 5G call, PEI value is set.

  For 4G call, IMEI value is set.

- 3GPP-RAT-TYPE

  Description: 1-byte octet encoded as per 3GPP TS 29.061.

  For 5G call, value "NR (10)" is set.

  For 4G call, value "EUTRAN (6)" is set.

- 3GPP-USER-LOCATION

  Description: Special encoded octet value encoded as per 3GPP TS 29.061.

  For 5G call, the following encoding logic is used:

1	Location-Type Only TAI = 136 Only NCGI = 135 Both TAI + NCGI =137
2-6	TAI-Encoding (if present)
7-14	NCGI-Encoding (if present)

TAI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4-5	TAC value	

NCGI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4	SPARE	NCI
5-8	NR Cell Identifier (NCI)	

For 4G call, the following encoding logic is used:

1	Location-Type
	Only TAI = 128
	Only ECGI = 129
	Both TAI + ECGI =130
2-6	TAI-Encoding (if present)
7-13	ECGI-Encoding (if present)

TAI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4-5	TAC value	

ECGI Encoding header:

1	MCC digit 2	MCC digit 1

2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4	Spare	ECI
5-7	EUTRAN Cell Identifier (ECI)	

- 3GPP-MS-TIMEZONE

  Description: Special encoded octet value encoded as per 3GPP TS 29.061.

  Timezone string (for example: -07:00+1) is encoded as two-byte value mentioned below:

  First byte timezone – NA

  Second byte daylight – two bits used (00-0, 01-+1, 10-+2, 11 – Unused)

1	TIMEZONE
2	DAYLIGHT SAVING 0, or +1 or +2

- 3GPP-NEGOTIATED-DSCP

  Description: 1-byte octet encoded as per 3GPP TS 29.061

  For both 5G and 4G calls, DSCP configuration from DNN qos-profile configuration is used.

  Sub -> DNN profile -> QosProfile -> DSCPMap -> Qi5 value check -> ARP priority check

Call Flows

SMF - RADIUS Authentication Call Flow

The following figure illustrates the end to end call flow between SMF server and RADIUS-EP functionality.

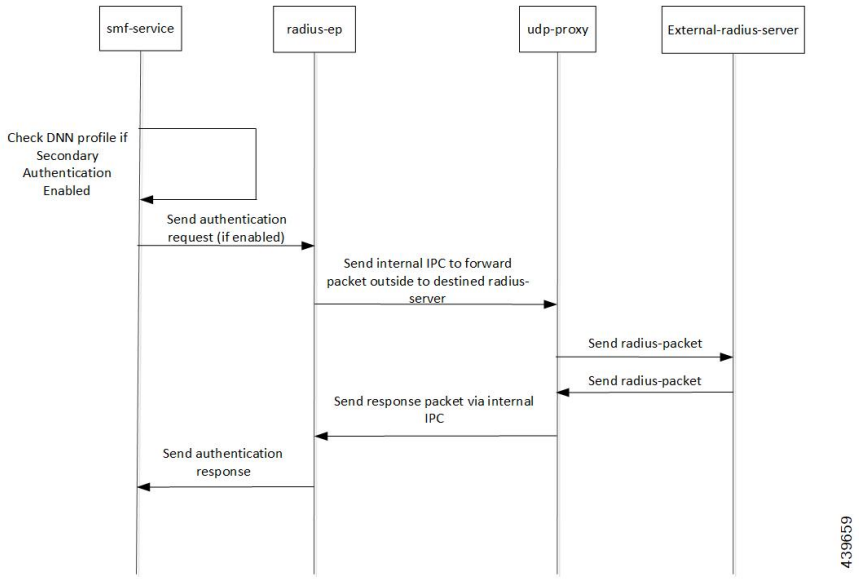


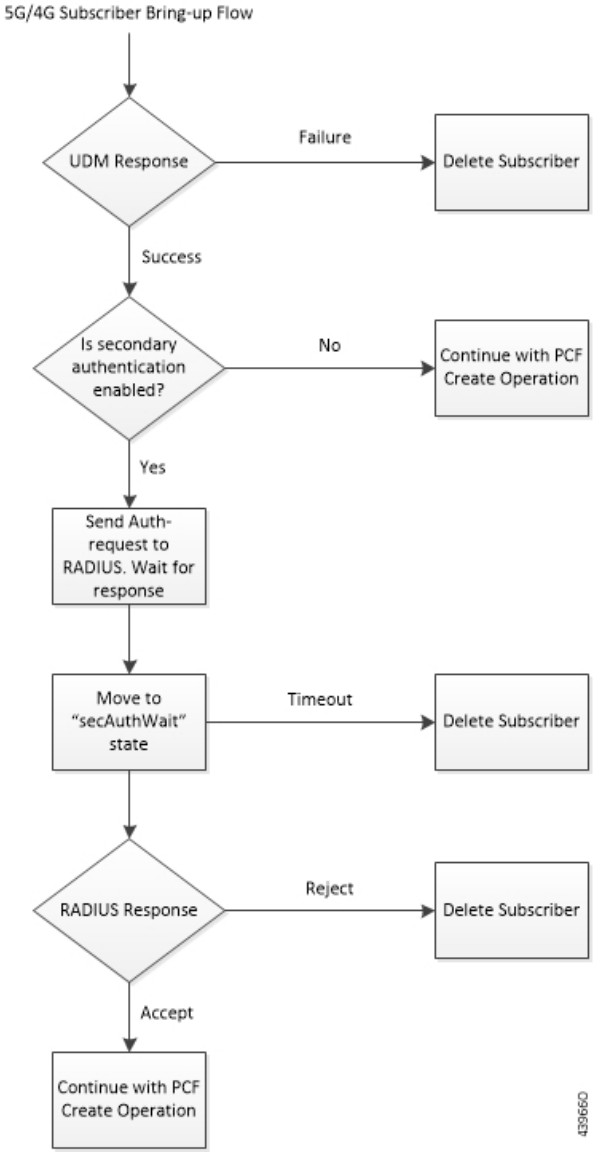
Table 141: RADIUS Authentication Call Flow

Step	Description
1	Bring up RADIUS-POD: Add respective endpoint configuration, with VIP-IP same as protocol-ep VIP-IP. Add radius-server information to profile-radius configuration.
2	Add “secondary authentication radius” configuration to required DNN profiles.
3	During session-bringup, after successful UDM validation, DNN profile checks if secondary authentication is enabled: • If not enabled, continue with PCF. • If enabled, send IPC to Radius-POD to authenticate the subscriber.
4	RADIUS-POD prepares the access-request packet that is destined to a configured radius-server, sends the packet to UDP Proxy POD to proxy the packet out.
6	UPD Proxy POD creates a socket (if not already present) and sends out packet to the radius-server.
7	Radius-server validates access-request. If accepted, responds “access-accept”. Else, responds “access-reject”.
8	UDP Proxy responds to respective Radius-ep instance.
9	Radius-ep instance validates the response, fetches framed-ip (if present) and updates smf-service.
10	Smf-service, upon success response from radius-ep, continues with PCF flow. Else, disconnects the subscriber.

SMF - Secondary Authentication Flow

The following flowchart explains the smf-service handling of secondary authentication of 4G/5G subscribers. After successful UDM Subscriber-Notification response, smf-service invokes secondary authentication if enabled in the DNN-profile configuration. Currently, only RADIUS method is supported. It does a sync-wait for RADIUS-response and continues with PCF create upon successful response. If secondary authentication fails, subscriber is deleted.

Figure 108: SMF - Secondary Authentication Flow



Standards Compliance

The RADIUS Client feature complies with the following standard:

- RFC 2865: Remote Authentication Dial in User Service (RADIUS)

Limitations and Restrictions

The RADIUS Client feature has the following limitations:

- AAA group concept is not supported.
  - Global RADIUS profile configuration is supported, which is applicable to all DNNs.
- Authorization and Accounting is not supported.
- User authentication based on PAP, CHAP, MSCHAP, and so on, is not supported. Only MSISDN-based user authentication is supported in this release.
- RADIUS Client interfaces' VIP-IP is mandatory configuration for RADIUS Client to work.
- Currently, only one VIP-IP is supported.
- VIP-IP must be same as the UDP-PROXY PODs IP.
- Currently, RADIUS POD-level VIP-IP is not applicable.

Configuring the RADIUS Client Feature

This section describes how to configure the RADIUS Client feature.

Configuring the RADIUS Client feature involves the following steps:

1. Configuring RADIUS Server
2. Configuring RADIUS Server Selection Logic
3. Configuring RADIUS NAS-Identifier
4. Configuring RADIUS Detect-dead-server
5. Configuring RADIUS Dead-time
6. Configuring RADIUS Max-retry
7. Configuring RADIUS Timeout
8. Configuring RADIUS POD
9. Configuring RADIUS NAS-IP
10. Configuring Secondary Authentication Method

Configuring RADIUS Server

This section describes how to configure the RADIUS Server.

```
configure
   profile radius
      server ipv4_address auth_port
         secret secret_key
         priority priority_value
         commit
```

NOTES:

- **profile radius**: Enters RADIUS configuration mode.
- **server** *ipv4_address auth_port*: Specifies IPv4 address and authorization port of RADIUS server.
- **secret** *secret_key*: Specifies the secret key.
- **priority** *priority_value*: Specifies the priority of server.
- **commit**: Commits the configuration.

Configuration Example

```
profile dnn intershat
 ...
 authentication secondary radius
exit
```

Configuring RADIUS Server Selection Logic

This section describes how to configure the RADIUS Server selection logic.

```
configure
   profile radius
      algorithm first-server
      algorithm round-robin
      commit
```

NOTES:

- **profile radius**: Enters RADIUS configuration mode.
- **algorithm first-server**: Sets the selection logic as highest priority first. This is the default behavior.
- **algorithm round-robin**: Sets the selection logic as round-robin order of servers.
- **commit**: Commits the configuration.

Configuration Example

```
profile radius
 server 1.2.3.4 1812
  secret   $8$73a0i4G3ILj0Np+8tn2QOoWDj3QkB+oefPc2ZK6RE6A=
  priority 1
 exit
 server 1.2.5.6 1812
  secret   $8$VccEEUVou7m5ptA9WZRPR7KDmxQ/L3KlJ3QqgHjexkk=
  priority 2
 exit
exit
```

Configuring RADIUS NAS-Identifier

This section describes how to configure the RADIUS NAS-Identifier.

```
configure
   profile radius
      attribute nas-identifier value_in_string
      commit
```

NOTES:

- **profile radius**: Enters RADIUS configuration mode.
- **attribute nas-identifier** *value_in_string*: Sets the nas-identifier value that is used while encoding.
- **commit**: Commits the configuration.

Configuration Example

```
profile radius
 algorithm round-robin
exit
```

Configuring RADIUS Detect-dead-server

This section describes how to configure the RADIUS Detect-dead-server.

```
configure
   profile radius
      detect-dead-server response-timeout value_in_seconds
      commit
```

NOTES:

- **profile radius**: Enters RADIUS configuration mode.
- **detect-dead-server response-timeout** *value_in_seconds*: Sets the timeout value that marks a server as "dead" when packet is not received for *value_in_seconds*. **Default = 10 secon**ds.
- **commit**: Commits the configuration.

Configuration Example

```
profile radius
 attribute
  nas-identifier CiscoSmf
 exit
exit
```

Configuring RADIUS Dead-time

This section describes how to configure the RADIUS Dead-time.

```
configure
   profile radius
      deadtime value_in_minutes
      commit
```

NOTES:

- **profile radius**: Enters RADIUS configuration mode.
- **deadtime** *value_in_minutes*: Sets the time to elapse between RADIUS server marked unreachable and when we can re-attempt to connect. Default = 10 minutes.
- **commit**: Commits the configuration.

Configuration Example

```
profile radius
 detect-dead-server response-timeout 100
exit
```

Configuring RADIUS Max-retry

This section describes how to configure the RADIUS Max-retry.

```
configure
   profile radius
      max-retry value
      commit
```

NOTES:

- **profile radius**: Enters RADIUS configuration mode.
- **max-retry** *value*: Sets the maximum number of times system will attempt retry with RADIUS server. Default = 5.
- **commit**: Commits the configuration.

Configuration Example

```
profile radius
 deadtime 15
exit
```

Configuring RADIUS Timeout

This section describes how to configure the RADIUS Timeout.

```
configure
   profile radius
      timeout value_in_seconds
      commit
```

NOTES:

- **profile radius**: Enters RADIUS configuration mode.
- **timeout** *value_in_seconds*: Sets the time to wait for response from RADIUS server before re-transmitting. Default = 3 seconds
- **commit**: Commits the configuration.

Configuration Example

```
profile radius
 max-retry 2
exit
```

Configuring RADIUS POD

This section describes how to configure the RADIUS POD.

```
configure
   endpoint radius-dns
      replicas number_of_replicas
      commit
```

NOTES:

- **endpoint radius-dns**: Enters endpoint radius-ep configuration mode.
- **replicas** *number_of_replicas*: Sets the number of replicas required.
- **commit**: Commits the configuration.

Configuration Example

```
profile radius
 timeout 4
exit
```

Configuring RADIUS NAS-IP

This section describes how to configure the RADIUS NAS-IP

```
configure
   endpoint radius-dns
      interface radius-client
         vip-ip ipv4_address
         commit
```

NOTES:

- **endpoint radius-dns**: Enters endpoint radius-ep configuration mode.
- **interface radius-client**: Enters the radius-client interface-type configuration mode.
- **vip-ip** *ipv4_address*: Sets the NAS-IP value, which is also used as source-ip in UDP requests toward RADIUS server.
- **commit**: Commits the configuration.

Configuration Example

```
endpoint radius-dns
 replicas 3
exit
```

Configuring Secondary Authentication Method

This section describes how to configure the secondary authentication method.

```
configure
   profile dnn dnn_name
      authentication secondary radius
      commit
```

NOTES:

- **profile dnn** *dnn_name*: Enters the DNN Profile configuration mode.
- **authentication secondary radius**: Enables the "secondary-authentication" under the DNN profile and sets method as "RADIUS".
- **commit**: Commits the configuration.

Configuration Example

```
endpoint radius-dns
interface radius-client
```

```
  vip-ip 10.86.73.89
 exit
exit
```

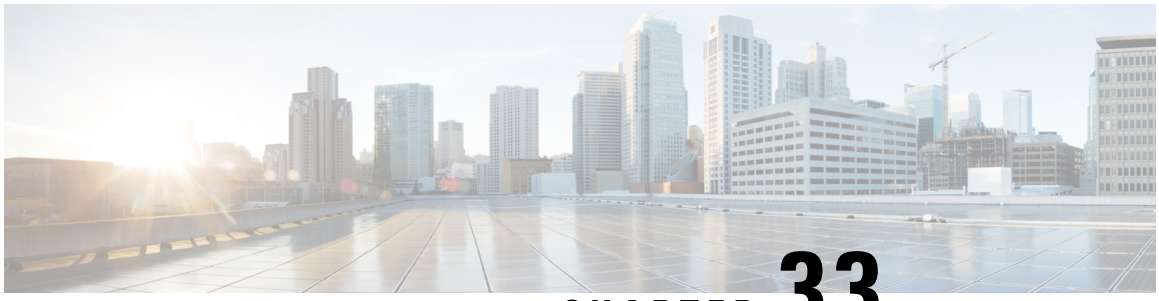
RADIUS Client OA&M Support

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

Statistics

Following statistics are available related to RADIUS functionality:

- SMF-Service:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
- RADIUS-EP:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
  - Number of RADIUS packets sent
  - Number of RADIUS packets received



CHAPTER 33

Resource Management

Feature Summary and Revision History

Summary Data

Table 142: Feature Summary

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 143: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The UE IP address and ID allocation and management (resource management) feature is used by the SMF service and supported by the NodeMgr.

The Master NodeMgr initializes the following in Redis-DB:

- IP pools for all DNN profiles
- Running counter for ID
- Free list for ID

The NodeMgr hosts the resource management server functionality and exposes the APIs for:

- IP allocation and management
  - IP allocation
  - IP release
  - IP reallocation (release the current IP and allocate new IP for UE)
- ID allocation and management
  - ID allocation
  - ID release
  - ID reallocation (release the current ID and allocate new ID)

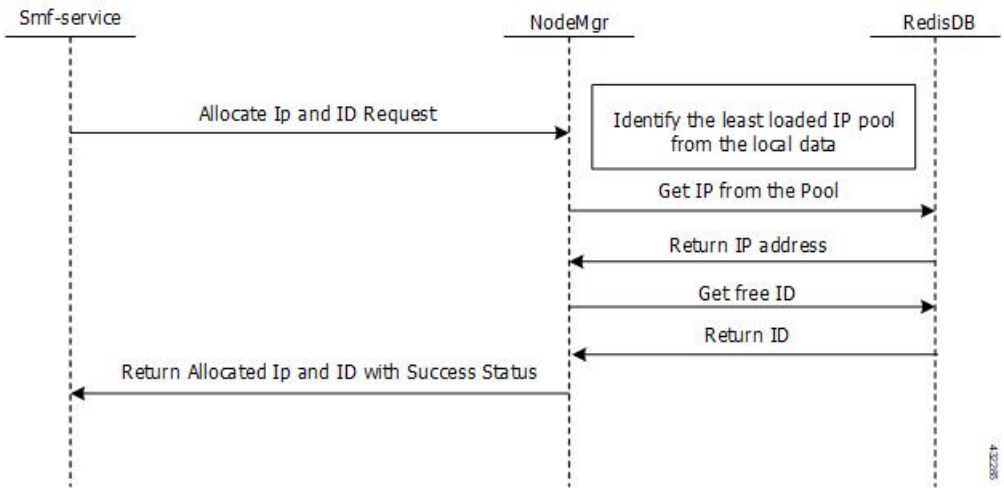
The SMF service runs the resource management client to use the Rmgr services.

Call Flows

IP and ID Allocation

The following call flow illustrates the IP and ID allocation.

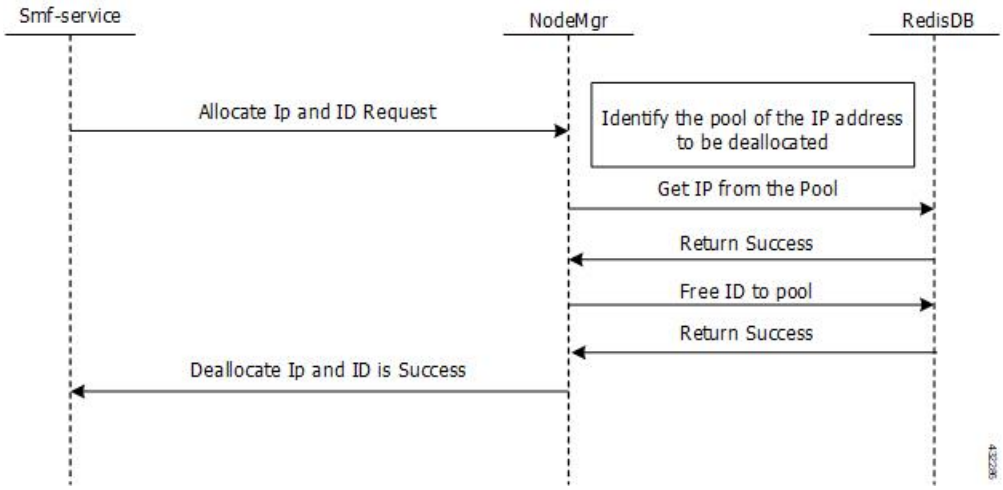
Figure 109: IP and ID Allocation Call Flow

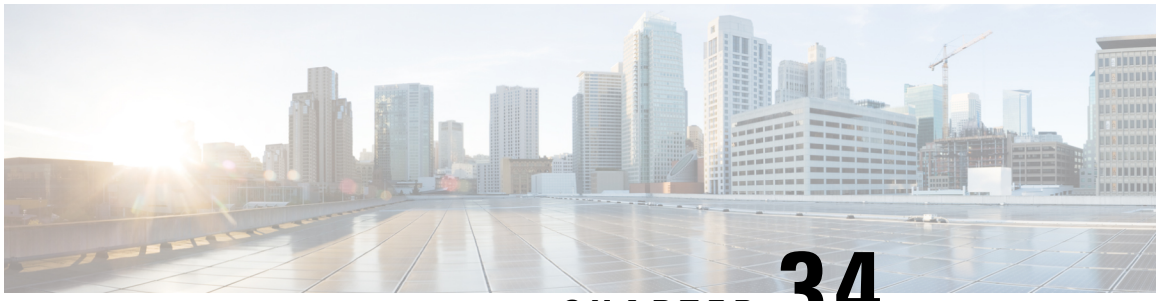


IP and ID Deallocation

The following call flow illustrates the IP and ID deallocation.

Figure 110: IP and ID Deallocation Call Flow





CHAPTER 34

Router Solicit and Router Advertisement

This chapter covers the following topics:

Feature Summary and Revision History

Summary Data

Table 144: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 145: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

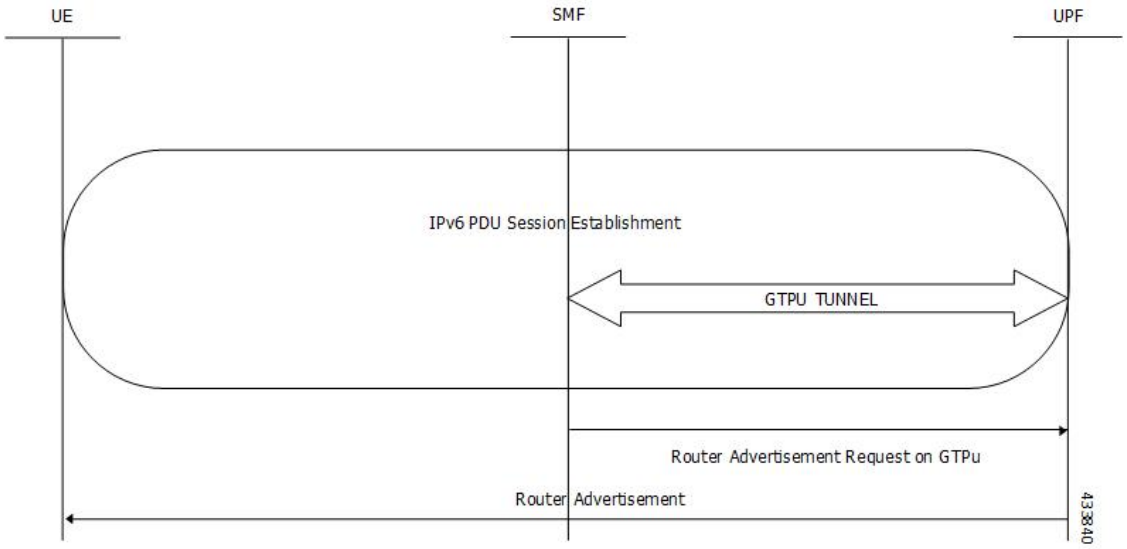
To comply to IPv6 Stateless Auto-configuration, SMF supports ICMPv6 Router Solicit and Advertisement.

The following ICMPv6 options are supported in Router Advertisement:

- Prefix Information - Allocated UE IPv6 Prefix is sent.
- MTU - Value is taken from configuration. Default is 1500.
- Source Link Layer Address: Value is taken from configuration local virtual mac.

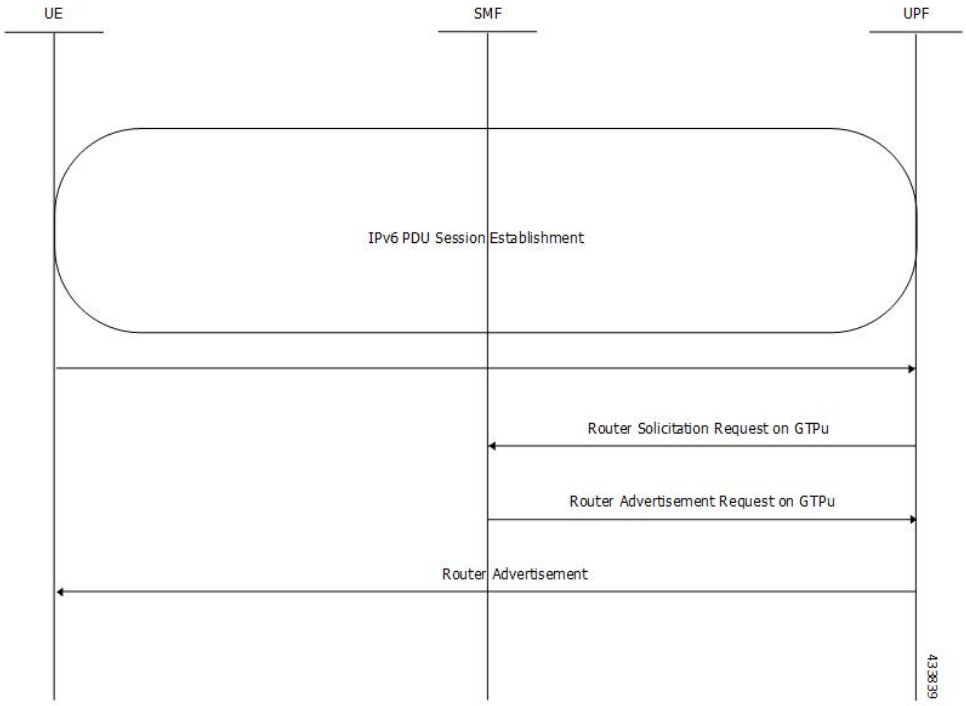
Unsolicited Router Advertisement

SMF sends unsolicited router advertisement on successful PDU session establishment to share the allocated IPv6 prefix to UE. RA message is sent over the GTPU tunnel, which is created between the SMF and UPF during the Session Establishment procedure. SMF also installs PDRs and FARs on the UPF to enable routing for RS/RA messages.



Solicited Router Advertisement

To get the allocated IPv6 prefix, UE can send a router solicit message. On receiving router solicit message, SMF sends router advertisement message towards UE containing the allocated UE IPv6 prefix.



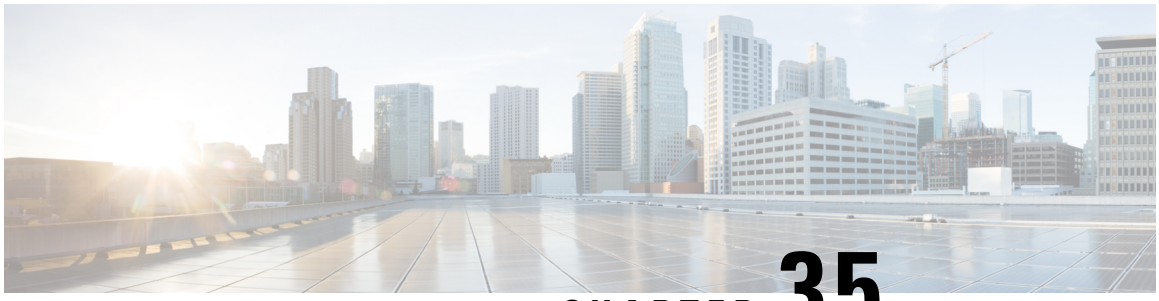
ICMPv6 Profile Configuration

The following configuration is used to configure Router Advertisement parameters:

```
scheduler(config-icmpv6-profile-icmp1# show full
icmpv6-profile icmp1
local-virtual-mac ac:de:48:00:11:22
hop-limit          64     default 255
router-lifetime    100 (seconds) default 65535
reachable-time     30 (milliseconds) default 0
retrans-timer      1 (milliseconds) default 0
mtu                1500 default 1500
!



dnn-profile dnn1
remote-virtual-mac fa:00:4c:a8:22:05 default(00:14:22:01:23:45)
ipv6-pool name pool1
      prefix          2001:300:4001::/48
      prefix-lifetime 3456 (seconds) default 4294967295

!
!
smf-profile prof
service name srv1
  associate-icmpv6-profile icmp1
!
!
```

NOTES:

- /48 is the only prefix supported in this release.



CHAPTER 35

Session and Service Continuity Mode

This chapter covers the following topics:

Feature Summary and Revision History

Summary Data

Table 146: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 147: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

Session and Service Continuity

The Session and Service Continuity (SSC) support in 5G system architecture enables to address the various continuity requirements of different applications and services for the User Equipment (UE). The 5G system supports different SSC modes. The SSC mode associated with a PDU session does not change during the lifespan of a PDU session. The following three modes are specified:

- With SSC mode 1, the network preserves the connectivity service provided to the UE. For the case of PDU session of IPv4 or IPv6 or IPv4v6 type, the IP address is preserved.
- With SSC mode 2, the network may release the connectivity service delivered to the UE and also may release the corresponding PDU session(s). For the case of IPv4 or IPv6 or IPv4v6 type, the release of the PDU session induces the release of IP address(s) that had been allocated to the UE.
- With SSC mode 3, changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through new PDU session anchor point is established before the previous connection is terminated in order to allow for better service continuity. For the case of IPv4 or IPv6 or IPv4v6 type, the IP address is not preserved in this mode when the PDU session anchor changes.

Session and Service Continuity Mode Selection

The SSC mode selection policy is used to determine the type of session and service continuity mode associated with an application or group of applications for the UE. The SMF receives the list of supported SSC modes and the default SSC mode per DNN per S-NSSAI as part of the subscription information from the UDM.

To select the SSC mode, when UE sends SSC mode in PDU session establishment request, it is checked against subscriber data and local SMF configuration and allowed SSC mode is determined.

Important In this release, SMF supports only SSC mode-1.

Priority for Choosing Session and Service Continuity Mode

Priority #1: Subscriber data from UDM has highest priority. UDM sends DefaultSscMode and AllowedSscMode.

Priority #2: Local SSC mode configuration data present in DNN profile which contains ssc-mode and allowed-ssc-mode.

Session and Service Continuity Mode Selection Method

The SSC mode has the following selection methods:

- The SMF verifies if UE sent SSC mode is part of either default ssc mode or allowed ssc mode in order of priority mentioned above. If it is found then PDU establishment procedure continues, otherwise PDU session establishment reject message will be sent to UE with allowed ssc modes in reject message.
- If the SMF does not receive SSC mode from UE, then default ssc mode in the order of above priority is chosen and used to establish PDU session.
- Since current release only supports SSC Mode-1, in case UE sends any other modes, PDU session establishment will be rejected.

NOTES:

When UE requests SSC mode-2 or mode-3, as long as the UE's subscription (in the order of priority: UDM/Local configuration on SMF) allows SSC mode-1 along with SSC mode-2/3, SMF will send *PDU session establishment* reject with 5GSM cause: 68 (Not supported SSC mode) and Allowed SSC mode as 01. This approach is used to allow the UE to retry with SSC mode-1. As per 3GPP spec: 24.501, 5GSM cause: 68 to be sent when the requested SSC mode is not supported by the subscription.

To honor PDU session establishment, SMF expects SSC mode either via UDM subscription or via local configuration. Otherwise, irrespective of SSC mode reception from UE, if SMF doesn't have SSC mode as part of UDM subscription or via local configuration, SMF would reject PDU session establishment with 5GSM cause: 31 (Request rejected and unspecified).

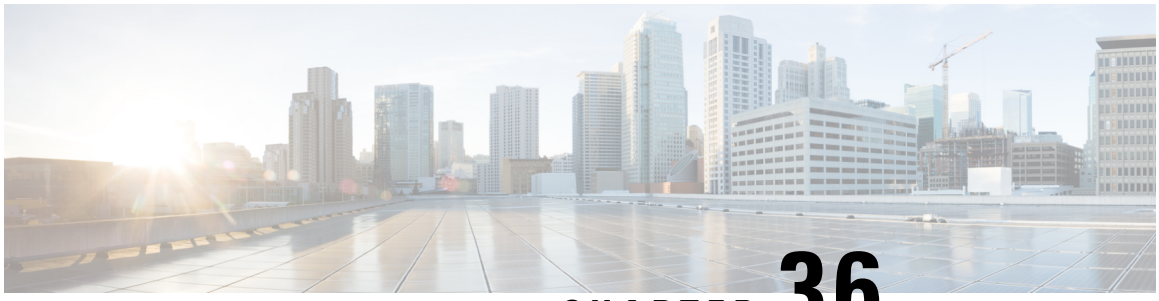
Configuration

To configure the SSC Mode in SMF DNN profile, use the following configuration:

```
config
   profile dnn dnn_name
      ssc-mode 1 allowed-ssc-mode 2
         commit
commit complete
```

To remove the configuration of the SSC Mode from SMF DNN profile, use the following configuration:

```
config
   profile dnn dnn_name
      no ssc-mode
      commit
commit complete
```



CHAPTER 36

SMF Charging

Feature Summary and Revision History

Summary Data

Table 148: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 149: Revision History

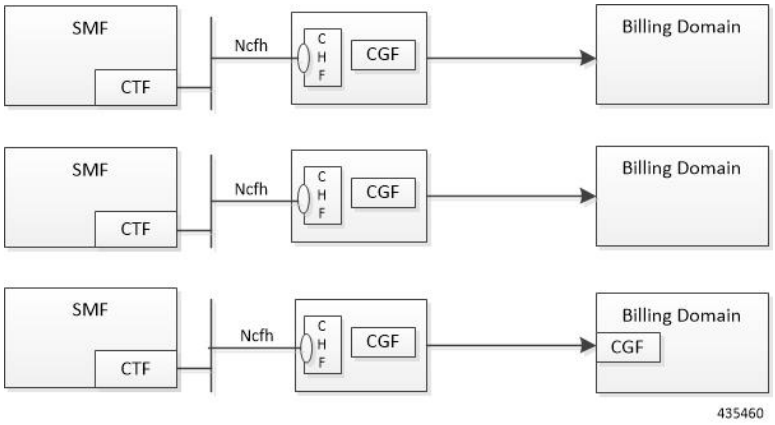
Revision Details	Release
First introduced.	Pre-2020.02.0

Overview

The SMF acts as a Charging Transfer Function (CTF). The CTF generates charging events toward the Charging Function (CHF), which is responsible for generating Charging Data Records (CDRs).

This SMF NF interacts with various interfaces such as N40, N4, N7, and N10, facilitating charging in entirety. Currently, the Cisco SMF uses the Nchf/N40 interface to generate charging events.

Figure 111: SMF as a Charging Transfer Function



The SMF Charging feature supports the following functionality:

- Converged Online and Offline charging.
- PDU session charging using the service-based interface.
- Network slice instance charging.
- Charging information collection per PDU session for UEs served under 3GPP access.
- Each PDU session is assigned a unique identity number for billing purposes.
- Data volumes on both the uplink and downlink directions are counted separately. The data volumes reflect the data as delivered to and forwarded from the user.
- The charging mechanism provides the date and time information when the PDU session starts.
- The SMF handles Charging Characteristics specific to a subscription or a subscribed DNN.
- The SMF identifies data volumes, elapsed time, or events for individual service data flows (flow-based charging). One PCC rule identifies one service data flow.
- SMF allows usage reporting of a service or a detected application per rating group or per combination of the rating group and service ID. This reporting level can be activated per PCC rule.
- Quota management is done per Rating Group (RG) per PDU session.
- SMF supports charging for IP-based PDU session types.

Converged Charging

The 5G system supports converged charging for offline and online charging scenarios.

The SMF performs converged charging for each of the following:

- Charging data that is related to PDU session.
- Charging data that are related to service-data flows within a PDU session.

The scope of convergent charging in this implementation includes quota management and usage reporting. For convergent charging, the SMF interacts with the CHF for charging data related to PDU sessions. The Charging Data Request and the Charging Data Response messages are exchanged between the SMF and the CHF based on session-based charging (SCUR scenarios). The Charging Data Request is issued by the SMF only when conditions that are related to chargeable events are met.

Chargeable Events

PCC rules can be activated, deactivated, and modified at any time during the PDU session lifetime.

The following attributes can be modified by the PCF in a dynamic PCC rule active in the SMF:

- Charging Key
- Service Identifier
- Measurement Method

Activities on PCC rules and QoS flows are not chargeable events. However, change of charging rule in PCC rules lead to chargeable events such as:

- Start of service data flow
- Termination of service data flow, for the last service data flow for the original PCC rule

The charging key (that is, rating group) is used to request online charging quota.

Charging Identifier

The charging identifier corelates charging information between the SMF and CHF during the duration of a PDU session. The SMF generates and assigns a charging identifier when a PDU session is established. The charging identifier is unique for that PDU session and is used in all messages that are exchanged in that PDU session.

Charging Information

The SMF collects the following charging information for converged online and offline charging:

- Usage of access and core network resources: Describes the amount of data that is delivered to and forwarded from the UE.
- Usage duration: Time interval from PDU Session Establishment to PDU Session Release.
- User: UE information used by the user for a PDU session.
- Data network: Data network address as determined by the DNN.
- Start time: PDU session start time.

- User location: HPLMN and VPLMN reporting area.

For service-data flows (flow-based charging), the SMF collects the following information:

- PDU session description.
- Data that are transmitted in uplink and downlink directions based on the rating-group information, or a combination of rating-group and service ID during volume-based charging.
- Duration of service data flow based on the rating group, or a combination of rating-group and service ID during event-based charging.
- Events and timestamps based on rating-group or based on a combination of the rating-group and service ID during event-based charging.

The SMF collects charging information for service data flows per UPF, within a PDU session, based on the rating-group or based on a combination of rating-group and service ID.

How it Works

Charging Session

The SMF supports converged session-based charging (SCUR) as specified in 3GPP TS 32.290, Section 5.3.2.3.

The SMF establishes charging session with the CHF with the Charging Data Request and Response (Initial) exchange. During the life of the PDU session, usage is reported with Charging Data Request/Response (Update) exchange. After the session is released, Charging Data Request/Response (Termination) messages are exchanged.

Offline Charging and Online Charging

Charging is enabled for a session based on the input that is received from the PCF.

For offline charging, the SMF sends Charging Data Request Initial toward the Charging Function (CHF) based on the presence of charging descriptors and refChgData field set in the smPolicyDecision message from the PCF in SmPolicyControlCreate response.

On determining if charging is required during initial session establishment or post-session establishment, charging is enabled for the PDU session. Once charging is enabled, SMF sends the Charging Data Request (Initial) Message toward the CHF.

The SMF determines Volume/Time threshold value either locally or from Charging Data Response. These values are used to update Volume/Time threshold IE in URR and to set the reporting trigger accordingly. The measurement method that is used in URR is derived from charging data.

For online charging, the SMF receives the Volume/Time Threshold and Quota values from the CHF. These values are received in the Charging Data Response (Initial) or using a Charging Data Request (Update) during a PDU Session Establishment. The SMF relays these Volume/Time Threshold and quota values to the UPF in the corresponding URR.

NOTE: The threshold values from CHF always override the locally configured values.

The following table maps the IEs that are shared with the UPF during Create/Update URR during online/offline charging scenarios:

IE	Online	Offline	Derived From
Volume Limit	Yes	Yes	CHF Response/Local Configuration
Time Limit	Yes	Yes	CHF Response/Local Configuration
Volume Quota	Yes	No	CHF Response
Time Quota	Yes	No	CHF Response
Quota Holding Time	Yes	—	CHF Response
Monitoring Time	Yes	Yes	• Local configuration for offline charging • CHF response for online charging
Reporting Trigger	Yes	Yes	The respective triggers that are set as shown in the following table.

Reporting Trigger	Derived From
Volume Threshold Trigger	If Volume threshold is set
Time Threshold Trigger	If Time threshold is set
Volume Quota Trigger	If Quota Exhausted trigger is set from CHF
Time Quota Trigger	If Quota Exhausted trigger is set from CHF
LIUSA Trigger	If URR contains Linked URR

Quota Management

The SMF requests quota from the CHF upon meeting any of the following conditions:

- The Rating Group (RG) is installed for the first time and the charging method is Online for the dynamic rule.
- The start of traffic trigger is initiated from the UPF for the RG in the case of static or predefined rules.
- A specific trigger type, as defined in the 3GPP specification 32.255, is received in the usage report for the online charging service from the UPF.

The SMF uses the **quota request always** CLI command to request the quota always. This CLI command is available in the Charging Profile configuration mode. Upon configuring this CLI command, the SMF always requests for quota when reporting the usage to the CHF for the online services. The quota requesting ends when the charging service stops.

Irrespective of the **quota request [always | standard]** CLI configuration, the quota request is disabled for the trigger type "qht" configured through the **quota suppress triggers** CLI command.

For command details, see the Charging Profile Configuration, on page 547 section in the *SMF Charging* chapter of this guide.

Service Units for Quota Management

The SMF sends Charging Data Request (CDR) to the Charging Function (CHF) for the service to be granted authorization to start, and to reserve the number of units. While triggering the CDR, the SMF requests volume

(uplink, downlink, total) and time quota from CHF to support VoLTE and other use cases. The values of the requested units for static rules are obtained from the Diameter configuration under Active Charging Service. For the dynamic audio or video rules, the values for the requested service units are configured through the **requested-service-unit** CLI command in the Charging Profile Configuration mode. For command details, see the Charging Profile Configuration, on page 547 section in the *SMF Charging* chapter of this guide.

Support for Validity Time

The SMF uses time quota value and its corresponding trigger on N4 interface to arm the UPF about the time when the SMF needs the reporting of validity time.

The CHF arms the SMF to report the usage for the rating group when the timer associated with the validity_time expires.

Based on the presence of Validity Quota and Time Quota, the SMF behaves as specified in the following ways:

- When the CHF sends only the Time Quota and not the Validity Quota, the SMF relays the CDR-U to the CHF and reports as Quota_EXHAUSTED upon receiving the usage report from the UPF.
- When the CHF sends only the Validity Quota and not the Time Quota, the SMF relays the CDR-U to the CHF and reports as VALIDITY_TIME upon receiving the usage report from the UPF.
- When the CHF sends both the Validity Quota and the Time Quota, the SMF determines the lower value of time_quota and validity_time, and then relays the CDR-U to the CHF accordingly. The SMF sends the "VALIDITY_TIME" trigger when the validity_time is lesser than the time_quota value. Similarly, when the validity_time is greater than the time_quota value, the SMF sends the "Quota_EXHAUSTED" trigger.

CHF Selection

The CHF selection, that is, CHF address determination by the SMF is performed during PDU Session Establishment. This selection is based on the following in order of priority:

1. PCF provides one or more CHF addresses as part of the PCC rule.
2. UDM-provided charging characteristics.
3. NRF-based discovery.
4. SMF locally provisioned charging characteristics.

NOTE: The local configuration is currently used to get CHF IP/port.

Charging Activities at SMF

URR Generation Toward N4

The SMF receives charging-data and usage-monitoring-data from the PCF. Based on this information, the SMF derives URR toward N4. In case the SMF is configured with volume/time limit at the session level, the SMF creates session-level URR.

Handling of Initial Event in Charging Component

The session context of SMF is configured with trigger/threshold as per the default described in 3GPP TS 32.255. It overrides the same based on configuration present in the charging profile. The same values can be

further overridden by CHF Charging Data Response Initial. Currently, trigger/threshold cannot be overridden when in PDU Establishment state.

The charging profile is referenced from the charging-characteristic profile. The CC profile is taken from UDM subscription for PDU session. If the CC profile is not mentioned in the UDM response, it is taken from the DNN profile.

After trigger/threshold/quota are determined, the SMF N4 Setup Request with set of Create URRs are derived from charging-data with one session-level URR.

If the session-level reporting is determined, the session-level URR is associated to each SDF URR.

The following triggers are supported:

- Volume/Time trigger at session/RG level
- AMBR change
- QoS change
- Quota threshold and quota exhausted
- Quota handling time
- Tariff time change

Obtaining Threshold Values at SMF

Threshold values, during online charging, are always obtained from the CHF. Whereas the threshold values, during offline charging, are obtained either from the CHF or from the charging profile configuration.

If charging profile is not determined during PDU establishment, the SMF refers to the charging profile from the DNN profile. Once the Charging Profile is determined, the SMF uses the determined Charging Profile to obtain the threshold values for Session/SDF URR.

The configuration has threshold values at a session level or rating-group level. The rating-group level threshold values are generic and not about a rating-group. These threshold values are overwritten by CHF response.

NOTE: The CHF response has various triggers. If some trigger is present at the session level or rating-group level, and if the volume or time threshold value is not available, then these values are assumed to be disabled at the corresponding level.

Trigger Determination at SMF

The SMF has triggers enabled by default, as specified in 3GPP TS 32.255, Section 5.2.1.4.

These triggers can be overwritten at a session level by trigger configurations present in the charging profile. Further, these triggers can also be overwritten by CHF responses.

Trigger configuration in charging profile is only applicable at a session level. It is not applicable for rating-groups.

NOTE: The CHF response has various triggers. If some triggers are present at a session or rating-group level and other triggers are not present, then these triggers are assumed to be disabled.

Reporting Category

The charging trigger can be of two reporting categories – Immediate and Deferred. The usage report of the immediate category must be reported to the CHF immediately. For reporting events that must be deferred,

the SMF will store the usage report locally, and will publish either when the next trigger of the immediate category is invoked, or when the storage limit is exhausted.

When reporting stored usage reports to the CHF, the usage report is triggered because of the trigger type in UsedUnitCategory and the message is triggered because of the trigger type in ChargingDataRequest.

Sometimes, a scenario can have two triggers hit at the same time. AMBR_Change and QoS Change can happen at the same time. In which case, all the triggers as applicable at the RG level or session level will have multiple trigger values.

A trigger can be enabled at the RG level, and for some RG it can be immediate reporting and for others it can be deferred reporting. When a trigger event is hit, various usage reports will have a corresponding category filled respectively in usedUnitContainer.

Deferred CDR will be relayed in the following scenarios:

- An immediate category event happens.
- Maximum number of charging conditions are crossed.
- Configured number of maximum deferred reporting is crossed.

Maximum Charging Characteristics (CC) is reset whenever there are push CDRs. This could be because of maximum CC limits being crossed or because of immediate category reporting.

NOTE: Currently, SMF does not support two charging descriptors with the same rating group.

Handling Reporting Level

The reporting category is classified into the following:

- Rating Group (RG) level: The RG is mandatory at this level.
- Service ID level: The RG and service ID is mandatory at this level.
- Sponsor ID level: The RG and Sponsor ID is mandatory at this level.

The reporting level is conveyed to the SMF from PCF in the Charging Data Request. If the reporting-level is RG, RG is the primary key. If the reporting level is Service_level or SponserLevl, the primary key becomes RG and Service ID or RG or Sponsor ID respectively. The SMF drops the charging descriptors from the PCF if the above requirement is not satisfied.

Re-Authorization

The CHF triggers Reauthorization of charging descriptors using Charging Notify request. Reauthorization is implemented at the session-level or at a RG-level for both online and offline charging.

The SMF processes the reauthorization details (which contain an array of RG, ServiceId, QuotaMgmtIndicator) received in CHF Notify and retrieves the charging descriptors associated with the current PDU session. Any unmatched reauthorization item is skipped.

For the charging descriptors identified for reauthorization, the SMF queries for usage reports from UPF and sends it to the CHF.

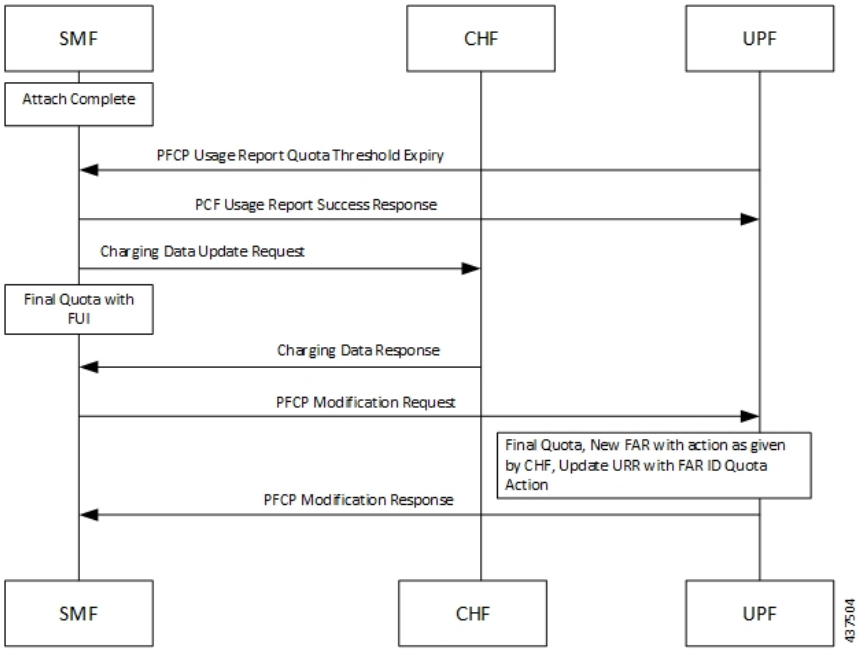
As part of the CHF response, the SMF detects any change in quota/threshold information and performs N4 Session Modification to update URRs.

Final Unit Indication Support

The SMF supports Final Unit Indication (FUI) in the Charging Data Initial/Update Response from CHF as per 3GPP TS 32.291, Section 6.1.6.2.1.12.

On receiving FUA, the SMF installs new FAR and associates it's FAR-ID in the URR, in the FAR ID Quota Action IE. If a FAR with same parameters exists, the SMF uses it's FAR-ID in the Create/Update URR. The UPF initiates appropriate actions set in FAR after quota exhaustion.

Currently, the SMF only supports Terminate and Redirect FU actions.



NOTES:

- At any instance, CHF provides granted unit (Quota) to the SMF along with FUI.
- When SMF receives the granted unit with FUI, the SMF creates FAR toward N4 and associates it to the corresponding URR which carries the Quota information.
- UPF on receiving FAR associated with the URR, the corresponding FAR action is implemented when the quota exhausts.

Static and Predefined Rules for Charging

Configuration of static/predefined rules is similar to the procedures on SMF and UPF. The layout of configured is as follows:

1. Rulebase: A one-to-many rule base is configurable. For a single PDU session, a single rule base can be activated at a given time. The rule base can be activated at SMF by the PCF by sending the rule base name in the PCC rule.
2. Ruledef: Each rule base can have one-to-many ruledef configurations. A ruledef can either be of static or predefined type. Each ruledef is assigned to a charging action.
3. Charging Action: Contains QoS and charging information.

The SMF derives charging data for each charging action in the rule base. Charging action associated to static rules in the rule base is immediately derived and updated in the PDU context. Charging action associated to predefined rules is derived and updated when the said predefined rule is activated at SMF from PCF.

The charging action derived URR has the following behavior:

- Online charging is identified by the "**cca charging credit**" configuration under charging action.
- Offline charging is identified by the "**billing action egcdr**" configuration under charging action.
- Armed triggers for volume-limit and time-limit are under the gtpp group configuration, under APN. The UPF automatically detects these values and sends the respective usage reports.
- The SMF, unlike the dynamic case, does not send the Create URR immediately for charging data that is derived from configured rules.
- Only when charging action is configured with "**cca charging credit preemptively-request**", the SMF sends the Create URR message. In all other cases, the SMF does not send the Create URR.

  NOTE: This CLI is not qualified in the current release.
- For URR derived from configured rules, the SMF generates URR-ID from "**urr-list**". This configuration has one URR-ID for each set of RG and service ID.

  Therefore, when the UPF sends the usage report for a URR ID, the SMF does not identify the corresponding URR, RG/service ID to be used for reporting toward the CHF.
- Using the online charging method, the UPF sends usage report with trigger "Start". The SMF uses CHF to derive the quota for the RG and relays the same information to the UPF in the Update URR message.
- The UPF threshold can be configured at a rule base level. It creates a rulebase-level URR that is linked to all ruledef-level URR within the rule base.

Modification Scenarios in Charging

PCF Update

The PCF performs the following actions during a modification scenario:

- Addition of PCC rules
- Modification of reference data
- Deletion of PCC rules
- Content update in charging data - using Measurement method

CHF Response

The CHF response, during an exchange, sends updated volume and time thresholds and quota. The SMF relays the updated URR toward N4.

A change in threshold/trigger/quota triggers an Update URR, which leads to the N4 relay.

The Update URR is sent based on the following triggers:

- Volume/time threshold
- Volume/time quota

- Tariff time change
- Quota holding time, and so on

URR Linking

- If session-level volume/time value is configured locally or is received from the CHF, the SMF creates session-level URR and links it to all URR corresponding to offline charging descriptors.
- If multiple charging descriptors received by PCF are of the same rating group, the SMF creates extra URR and links it to all URR derived from charging descriptors of the same rating group.

URR Format

The URR ID format is as given below:

- URR ID is 32 bit.
- MSB (32nd) bit for static/predefined URRs is set to 1, and for dynamic URRs is set to 0.
- First four LSB bits are set for interface type.
  - 1 for offline
  - 7 for online
- Bit 4-31 is for URR ID number.

  For example: Dynamic first URR if ID is 1:

  0x00 00 01 01 Offline

  0x00 00 01 07 Online

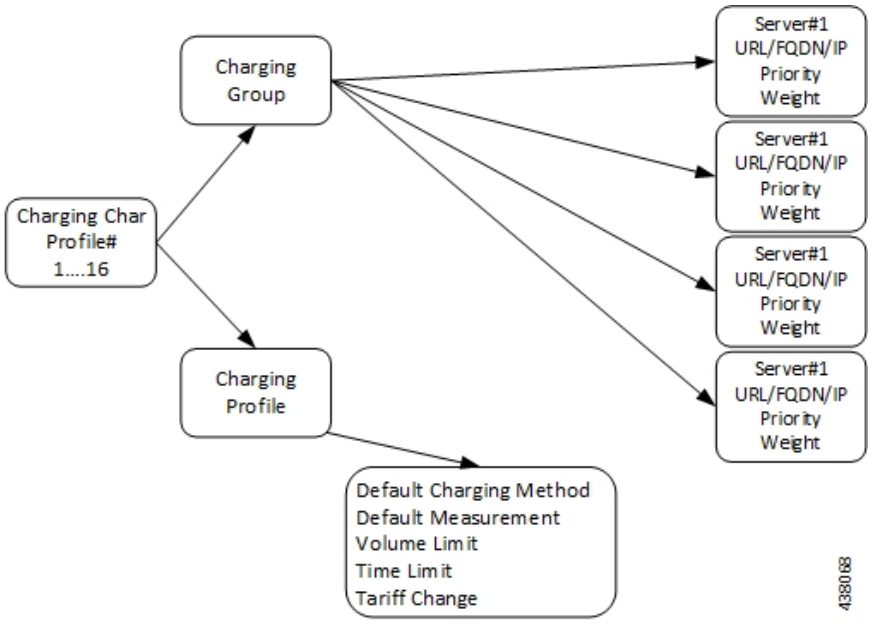
  Static/Predefined first URR if ID is 1:

  0x80 00 01 01 Offline

  0x80 00 01 07 Online

Local Configuration

The following figure illustrates how local configuration works.



NOTES:

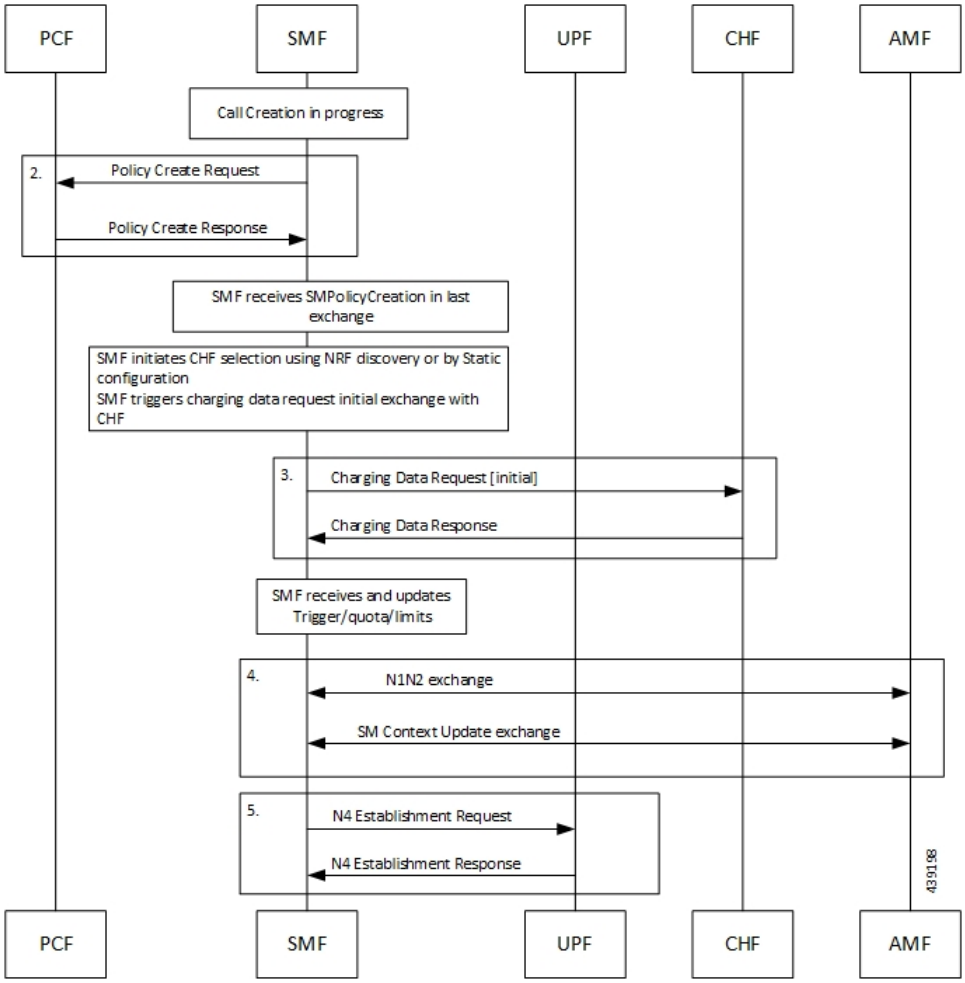
1. The SMF supports up to 16 charging characteristic profiles.
2. Each CC profile comprises of charging group and charging profile.
3. The charging server group and charging profile are linked to the DNN profile. Currently, the charging profile supports configuration for trigger and thresholds.

Call Flows

This section presents the following call flows:

PDU Session Establishment

The following figure illustrates the call flow of PDU session establishment.



Step	Description
1.	Call Setup
2.	SMF performs a Policy Create exchange with PCF. In this exchange, the SMF might receive Charging Data that is associated to a PCC Rule. This indicates that charging is enabled for the session in progress. It is possible that PCF has enabled Static/Predefined rules. These rules can be also enabled with charging, based on the configuration.
3.	Once charging is detected at SMF, it initiates a Charging Data Request Initial exchange with CHF. In this exchange SMF may receive the following from CHF: • CC triggers at session or RG level • Session level Time or Volume limits • Time or Volume limits at RG level • Quota at RG level
4.	N1N2 Exchange and SM Context Update Exchange

Step	Description
5.	SMF initiates N4 session establishment request exchange with UPF, and in the same request it relays information that is related to charging in the Create URRs.

Standards Compliance

The SMF Charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290

3GPP June 2019 Compliance for Charging Interface

The SMF is compliant with the 3GPP June 2019 specification TS 32.290 version 15.3.0.

For the June release the messages goes over the version "v2" as indicated below in URI format.

```
nchf-convergedcharging/v2/chargingdata
```

The CLI command for compliance configuration is: **service nchf-convergedcharging**. If this CLI command or version is not configured, the default version from 3GPP December 2018 is applied.

With the 3GPP June 2019 compliance, the following new information elements (IE) are added:

- Authorized QoS
- Subscribed QoS
- IEs in QoSData
- Serving Network Function ID

Configuring SMF Charging

SMF Charging involves the following configurations:

- DNN Profile Configuration
- Charging Characteristics Profile Configuration
- Charging Profile Configuration

DNN Profile Configuration

Use the following configuration to configure a DNN profile for SMF Charging.

```
configure
  profile dnn profile_name
    charging-profile profile_name
    network-element-profiles { amf | chf | pcf | udm } profile_name
    end
```

NOTES:

- **charging-profile**: Specifies the Charging Profile configuration.
- **network-element-profiles**: Specifies the network element profile. Network element profile can be one of the following:
  - **amf**: Specifies the AMF network element profile.
  - **chf**: Specifies the CHF network element profile.
  - **pcf**: Specifies the PCF network element profile.
  - **udm**: Specifies the UDM network element profile.
- *profile_name* must be a string.

Charging Characteristics Profile Configuration

Use the following configuration to configure charging characteristics profile for SMF Charging.

```
configure
  profile charging-characteristics cc_value
     charging-profile profile_name
     end
```

NOTES:

- *cc_value*: Specifies the charging characteristics value which is an integer from 1 to 16.

Charging Profile Configuration

Use the following configuration to configure the charging profile parameters for SMF charging.

```
configure
  profile charging profile_name
     limit [ rating-group ] { duration duration_value | volume volume_value }
     max-charging-condition max_cc_value
     max-deferred-urr max_urr_value
     method { none | offline | online }
     quota request [ always | standard ]
     quota suppress triggers [ qht ]
     reporting-level { offline | online { [rating-group] | rating-group
| service-id }
    requested-service-unit time seconds volume downlink downlink_value uplink
 uplink_value total total_value
     tight-interworking-mode { false | true }
     triggers session session_level_triggers
     end
```

NOTES:

- **limit**: Specifies the threshold limit.
- **duration**: Specifies the duration threshold for charging. The threshold value ranges from 0 through 2147483647.

- **volume**: Specifies the volume threshold for charging. The threshold value ranges from 0 through 9223372036854775807.
- **rating-group**: Specifies the volume and duration threshold for a Rating Group.
- **max-charging-condition** *max_cc_value*: Specifies the maximum number of changes to the charging condition. *max_cc_value* must be an integer ranging from 0 through 500. The default value is 20.
- **max-deferred-urr** *max_urr_value*: Specifies the maximum number of deferred USU containers. *max_urr_value* must be an integer ranging from 0 through 200. The default value is 50.
- **method**: Specifies the charging method. The default charging method is offline.
- **quota request [always | standard]**: Controls the requesting of quota from the CHF for online charging services based on the configuration. If the **quota request always** is configured, the SMF always requests for quota. If the **no quota request** or **quota request standard** CLI command is configured, then the SMF requests the quota for specific trigger types as defined in standard, which is the default behaviour.
- **quota suppress triggers [qht]**: Suppresses the quota from the CHF upon configuring the usage report trigger type "qht".
- **reporting-level**: Specifies the reporting level configuration to be used for offline and online charging.

  The default value is [rating-group] level.
- **requested-service-unit**: Configures the value for the requested service units.
  - **time** *seconds*: Configures the time quota value in seconds from 1 through 4000000000.
  - **downlink** *downlink_value*: Configures the downlink volume in bytes from 1 through 4000000000.
  - **uplink** *uplink_value*: Configures the uplink volume in bytes from 1 through 4000000000.
  - **total** *total_value*: Configures the total volume in bytes from 1 through 4000000000.
- **tight-interworking-mode**: Configuration to enable tight interworking mode for online/offline charging methods.
- **triggers**: List of triggers to be configured.
- **session** *session_level_triggers*: Specifies the list for Session Level Triggers. The list of Session Level Triggers is as follows:
  - **repor3gpp-ps-change**
  - **ambr-change**
  - **max-number-of-changes-in-charging-conditions**
  - **plmn-change**
  - **qos-change**
  - **rat-change**
  - **serv-node-change**
  - **tarrif-time-change**
  - **ue-pra-change**

- **ue-time-change**
- **upf-add**
- **upf-rem**
- **user-loc-change**

The following is a sample configuration for SMF Charging:

```
configure
   charging-server ch1
      fqdn abc.com
      capacity 10 (default : 10)
      priority 1 (default: 1)
      ip-address 127.0.0.1
      port 1234
      !
      !
   dnn-profile dnn1
      charging-server-name [ chserv1 ]
      charging-profile chProf1
      !
   profile charging ch1
      limit volume tot 2000
      limit duration 20
      limit rating-group volume tot 4000
      limit rating-group duration 40
      triggers session [ ambr-change qos-change]
   max-charging-condition 20
      max-deferred-urr 100
      reporting-level service-id
      requested-service-unit time 20 volume downlink 8000 uplink 2000 total 10000
      !
   profile charging-characteristics 1
   charging-profile ch1
   !
```

Static PCC Rules Configuration

For information on Configuring Static PCC Rules for Charging, refer to *Configuring the Static PCC Rules Support on SMF* section in the *Policy and User Plane Management* chapter.

The following is an example Static PCC Rule configuration:

```
configure
active-charging service acs
   credit-control group 1
      diameter ignore-service-id true
      pending-traffic-treatment forced-reauth drop
      pending-traffic-treatment noquota pass
      quota holding-time 10
      usage-reporting quotas-to-report based-on-grant report-only-granted-volume
      exit
   urr-list urrlocal
      rating-group 320011 service-identifier 10 urr-id 1
   charging-action ca95
      billing-action egcdr
      cca charging credit
      content-id         320011
      service-identifier 10
```

```
    exit
    charging-action test
      cca charging credit preemptively-request //This is not in scope of current release
    exit
    rulebase rb1
       action priority 10 ruledef rd95 charging-action ca95
       action priority 11 dynamic-only ruledef rd93 charging-action ca93
    exit

gtpp group group1
   gtpp egcdr service-data-flow threshold interval 1234
      gtpp egcdr service-data-flow threshold volume downlink 13000
      gtpp egcdr service-data-flow threshold volume uplink 17000
      gtpp egcdr service-data-flow threshold volume total 22222
   exit
```

Mapping of Charging Scenario on Various Interfaces

Feature Description

SMF supports charging on the N7, N40, and N4 interfaces. Based on the charging data information that SMF receives, it provides reporting level support for online and offline charging. The behavior of SMF changes according to the messages received on the N7, N4, and N40 interfaces.

How it Works

SMF provides the different reporting levels for online and offline charging with the following rules:

- Configured rules are derived from the static or predefined charging actions.
- Session-level Usage Reporting Rule (URR) is derived from CHF trigger or local configuration.
- SMF does not associate session-level URR for online and offline method charging description.
- SMF does not associate session-level URR to the configured charging-action URRs.
- Rulebase URR is applicable only for the offline configured URR.
- For the configured online or online-offline charging method, if Ignore Service ID configuration exists, the URR list must contain "rg x urr-id y". Else, the SMF drops the charging actions as malformed.

Important SMF supports multiple charging methods within the same rating group.

Charging Mapping

The N7 interface uses Charging Data from PCC rules or local configuration, N4 interface uses URR or Packet Detection Rule (PDR), and N40 interface uses Used Unit Container (UUC).

SMF charging mapping on N7, N4, and N40 interfaces with various charging methods is described as follows.

Offline Method When Charging Data is Derived from One PCC Rule

- Reporting level: Rating Group level or Service ID level

- N4 interface:
  - First URR is derived from the first Charging Data. Charging data limits from rating group trigger or local configuration.
  - Second URR is derived from Session Limit, which is CHF or local configuration.
  - Second URR is linked to the first URR.
  - First PDR is derived from the first PCC rule.
  - First and second URRs are linked to the first PDR.
- N40 interface:
  - First UUC is derived from the usage report of the first URR.
  - First UUC may or may not have a service identifier.

NOTES:

- Session-level URR is not associated to the configured URRs.
- If configured, rulebase URR replaces session-level URR.
- If configured and rulebase URR exists, it is linked to the first URR.

Online Method When Charging Data is Derived from One PCC Rule

- Reporting level: Service ID level or Rating Group level
- N4 interface:
  - First URR is derived from the first Charging Data, which is threshold or quota from rating group granted-unit.
  - Second URR is derived from Session Limit, which is CHF or local configuration.
  - Second URR is linked to the first URR.
  - First PDR is derived from the first PCC rule.
  - First and second URRs are linked to the first PDR.
- N40 interface:
  - First UUC is derived from usage report of the first URR.
  - First UUC may or may not have a service identifier.

NOTES:

- Session-level URR is not associated to the configured URRs.

Offline Method When Charging Data is Derived from Two PCC Rules

- Reporting level: Service ID level

- N4 interface:
  - First URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
  - Second URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
  - Third URR is derived from rating group level, which limits from Rating-Group trigger or local configuration.
  - Fourth URR is derived from Session Limit, which is CHF or local configuration.
  - The third and fourth URRs are linked to the first and second URRs.
  - First PDR is derived from first PCC rule.
  - Second PDR is derived from second PCC rule.
  - First, third, and fourth URRs are linked to the first PDR.
  - Second, third, and fourth URRs are linked to the second PDR.
- N40 interface:
  - First UUC is derived from the usage report of the first URR.
  - Second UUC is derived from the usage report of the second URR.
  - Both the first and the second UUCs have a service identifier.

NOTES:

- Session-level URR is not associated to the configured URRs.
- If configured, rulebase URR is linked to the first and second URRs.

Online Method When Charging Data is Derived from Two PCC Rules

- Reporting level: Service ID level
- N4 interface:
  - First URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
  - Second URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
  - Third URR is derived from rating group level, which is threshold or quota from the rating group granted unit.
  - Fourth URR is derived from Session Limit, which is CHF or local configuration.
  - Third and fourth URRs are linked to the second and fourth URRs.
  - First PDR is derived from the first PCC rule.
  - Second PDR is derived from the second PCC rule.

- First, third, and fourth URRs are linked to the first PDR.
- Second, third, and fourth URRs are linked to the second PDR.

- N40 interface:
  - First UUC is derived from usage report of the first URR.
  - Second UUC is derived from the usage report of the second URR.
  - Both the first and the second UUCs have a service identifier.

NOTES:

- Session-level URR is not associated to the configured URRs.
- If Ignore Service ID is configured, this method is not valid.

Offline-Online Method When Charging Data is Derived from One PCC Rule

- Reporting level: Service ID level or Rating Group level
- N4 interface:
  - Offline URR is derived from the first Charging Data, which limits rating group trigger or local configuration.
  - Online URR is derived from the first Charging Data, which limits from the granted unit.
  - First PDR is derived from the first PCC rule.
  - Offline and online URRs are linked to the first PDR.

- N40 interface:
  - First UUC is derived from the usage report of the offline URR.
  - Second UUC is derived from the usage report of the online URR.

Offline-Online Method When Charging Data is Derived from Two PCC Rules

- Reporting level: Service ID level
- N4 interface:
  - First offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Off3.
  - Second offline URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Off3.
  - Third offline URR is the rating group level, which limits the rating group trigger or local configuration.
  - First online URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online3.

- Second online URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online3.
- Third online URR is the rating group level, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Second PDR is derived from the second PCC rule.
- First offline URR, first online URR, third offline URR, and third online URR are linked to the first PDR.
- Second offline URR, third online URR, third offline URR, and third online URR are linked to the second PDR.

- N40 interface:
  - First UUC is derived from the usage report of the first offline URR and has a service identifier.
  - Second UUC is derived from the usage report of the second offline URR and has a service identifier.
  - Third UUC is derived from the usage report of the first online URR and has a service identifier.
  - Fourth UUC is derived from the usage report of the second online URR and has a service identifier.

Offline-Online Method When Charging Data is Derived from One PCC Rule with No Service Identifier

- Offline Reporting level: Service ID level
- Online Reporting level: Rating Group level
- Prerequisite: No Reporting Level from PCF
- CLI:
  - Tight interworking mode
  - Ignore Service Identifier
  - Offline Reporting: Service Identifier
  - Online Reporting: Rating Group

NOTES:

- SMF ignores the volume or time limit trigger from CHF at the rating group level.
- Session-level URR is not associated to URRs that are derived from the first Charging Data.
- N4 interface:
  - Offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online.
  - Online URR is derived from the first Charging Data, which limits from the granted unit.
  - First PDR is derived from the first PCC rule.
  - Online URR and offline URR are linked to the first PDR.

- N40 interface:
  - First UUC is derived from the usage report of the offline URR and has a service identifier.
  - Second UUC is derived from the usage report of the online URR and does not have a service identifier.

NOTES:

- Session-level URR is not associated to the configured URRs.
- If URR is configured, URR rulebase is derived from egcdr and is linked to both the offline and the online URRs.

Offline-Online Method When Charging Data is Derived from Two PCC Rules with No Service Identifier

- Offline Reporting level: Service ID level
- Online Reporting level: Rating Group level
- Prerequisite: No Reporting Level from PCF
- CLI:
  - Tight interworking mode
  - Ignore Service Identifier
  - Offline Reporting: Service Identifier
  - Online Reporting: Rating Group

NOTES:

- SMF ignores the volume or time limit trigger from CHF at the rating group level.
- Session-level URR is not associated to URRs that are derived from the first Charging Data.
- N4 interface:
  - First offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online.
  - Second online URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online.
  - URR_Online is derived from the second Charging Data, which limits from the granted unit.
  - First PDR is derived from the first PCC rule.
  - Second PDR is derived from the second PCC rule.
  - First offline URR and URR_Online are linked to the first PDR.
  - Second offline URR and URR_Online are linked to the second PDR.
- N40 interface:
  - First UUC is derived from the usage report of the first offline URR and has a service identifier.

- Second UUC is derived from the usage report of the second offline URR and has a service identifier.
- Third UUC is derived from the usage report of the URR_Online and does not have a service identifier.

NOTES:

- Session-level URR is not associated to the configured URRs.
- If URR is configured, URR rulebase is derived from egcdr and is linked to both the first and second offline URRs along with URR_Online.

Limitations

This feature has the following limitations:

- Same rating group is not supported for multiple Charging-action of rulebase and Dynamic Charg-Desc.
- Tight interworking mode is not supported for the service which is at the rating group level.
- One service at the rating group level and another service at service ID level are not supported.

Standards Compliance

The Different Reporting Level Support for Online and Offline Charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290

Error Handling Scenarios

This section describes the different handling scenarios associated with the errors that are encountered during SMF charging.

Application Error and Result Code Handling

SMF supports the application error codes from CHF at command level as defined in section 6.1.7.3 of specification 3GPP 32.291, v15.3.0. The SMF also supports RG-level result codes as defined in section 6.1.6.3.14 of specification 3GPP 32.291, v15.3.0.

The following labels are defined under "chf_appl_err_stats" counter to indicate the CHF response failures at the application level.

- http2_err_code - The possible values are:
  - 403
  - 400
  - 404
- appl_err_code - The possible values are:

- END_USER_REQUEST_REJECTED
- END_USER_SERVICE_DENIED
- QUOTA_LIMIT_REACHED
- CHARGING_NOT_APPLICABLE

- appl_err_action - The possible values are:
  - drop_traffic
  - disable_charging
  - terminate
- appl_err_exchg_type - The possible values are:
  - initial
  - update

Application Error Codes

The following table provides details of the application error codes with the corresponding SMF action.

Application Error/Session Level	HTTP2 Code	SMF Action	CHF Expected Actions	Limitations
CHARGING_FAILED	400	Terminate	None	None
RE_AUTHORIZATION_FAILED	400	None	Take corrective action	-
CHARGING_NOT_APPLICABLE	403	Continue subscriber session without Charging (no offline charging as well)	None	None
USER_UNKNOWN	404	Terminate	None	None
END_USER REQUEST_DENIED	403	Terminate	None	None
QUOTA_LIMIT_REACHED	403	Drop traffic for the online services. Offline services are not impacted.	CHF sends notify (RAR) after this condition is recovered for the session	

NOTES:

- The error code 403 is not configured in the failure handling template.

- CHARGING_NOT_APPLICABLE (Disable charging) for static and predefined rules is achieved by sending a proprietary IE “Charging Disabled” in subscriber params in N4 modification / establishment request, so that UPF does not generate Start of Traffic for the URRs pending for activation.

RG-level Result Codes

The following table provides details of the result code with the corresponding SMF action.

Result code/RG level	HTTP Status Code	SMF Behaviour	CHF Expected Behaviour	Limitations
RATING_FAILED	200	Drop traffic corresponding to the rating group	None	None
QUOTA_MANAGEMENT_UNAVAILABLE	200	Convert to offline	None	None
USER_UNKNOWN	200	Ignored (supported only at session level)	Not expected from CHF	None
END_USER SERVICE_DENIED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the rating group.	Traffic will be dropped for offline service as well for online/offline services.
QUOTA_LIMIT_REACHED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the session	None
END_USER SERVICE_REJECTED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the session	None

CHF Server Reconciliation

The SMF falls back to the first available offline CHF server when the NF selected by NRF discovery is unreachable. The CHF Reconciliation feature involves deleting the existing subscribers that are associated to a set of offline NFs, and the subscribers that are in offline fallback mode.

The CHF server reconciliation works when any of the following two conditions are met:

1. if the NRF detects that an offline CHF server is now active
2. if the RAR is recieved from the CHF server on an offline converted session

For the condition #2, the session gets deleted directly. With the NRF discovery, this feature involves the following steps:

1. SMF subscribes for the notification of NF instance IDs from NRF through NF_LIB component of Rest-ep.
2. If the NF discovery query determines that all the NFs are down, the NF_LIB component treats these set of NFs as offline. If any one of the NFs is available again, the NRF triggers notification for the same to the SMF.
3. The SMF performs NRF discovery after re-validation timer. If the NRF detects any new NF, the SMF receives the corresponding notification from the NRF.
4. When the SMF learns that an NF is online and it satisfies the NF discovery query parameters, then the SMF initiates the CHF server reconciliation.

The following labels are introduced as part of this feature:

- disc_pdurel_chf_reconciliation: This label is defined under SMF_DISCONNECT_STATS to indicate the disconnect reason.
- chf_reconl_pdu_sess_rel: This label is defined under smf_service_stats metric to display the number of times the PDU session release procedure is initiated.

Dynamic Configuration Change Support

Feature Description

The Failure Handling Profile contains the configurations that are invoked when a failure occurs. Now, the Failure Handling feature supports the N11 and GTPC interface. With the dynamic configuration, you can change the dynamic attributes associated with the Failure Handling Profile while SMF is running.

Similarly, the Dynamic Configuration Change Support feature allows SMF to dynamically handle the configuration changes of the Charging Profile parameters while minimizing the configuration errors. The existing and new SMF Charging parameters can implement dynamic configuration updates. This feature supports the following charging configurations:

- Charging Profile
- Charging Characteristics
- Charging-Action
- Credit-Control-group
- Urr-Id Map
- Rulebase and GTPP Group
- Upf-Apn Configuration Group

Limitations

In this release, the Dynamic Configuration Change Support for Charging Profile has the following limitations:

- For online charging, the URR ID configuration and creation time on SMF and UPF may differ causing a discrepancy in the following configurations:

- Rating Group (RG) and Service ID configuration within the Charging-Action
- URR-ID list that contains the URR IDs created for static or predefined URR
- Ignore-Service in Credit-Control group
- Mapping of Ruledef with the Charging-Action Profile

- Dynamic configuration of changes for the methods within the charging-action configuration are not supported.

How it Works

This section describes how dynamic change in configuration works for the supported Failure Handling Profile and Charging Profile configuration.

Failure Handling Profile

The Failure Handling Profile defines the various parameters for failure handling.

The following table lists the configurations that allow dynamic update.

Table 150: Failure Handling Profile Parameters

Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
profile failure-handling	**profile failure-handling** *name* **interface** *gtpc/n11* **message** *message* **cause-code** *cause_code* **action***action* **timeout** *timeout* **max-retry** *retry_count* **Supported values:** • interface: gtpc or n11 • message: • gtpc-message: • S5S8CreateBearerReq • S5S8CreateBearerReq • S5S8CreateBearerReq • N11-message: n1n2transfer • cause-code: • gtpc-cause-code: temp-fail • N11-cause-code: temp-reject-handover/ temp-reject-register • action: retry/clear/terminate • timeout: Range: [1000-5000] (default: 1000) • max-retry: Range: [0-5] (default: 1) **Note** • The timeout and max-retry parameters are applicable only if the action is set to 'retry'. • The CLI supports only the 'retry' action.	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.

Charging Profile

The Charging Profile supports dynamically updating the configuration based on the values that you pass during the runtime. The refresh operation of the values takes place considering the following scenarios:

- **Configuration reflects in the next encounter to access:** If the values are updated while an operation is in-progress, the SMF ignores the new values and continues to use the old values. For example, Limits in Charg-Profile, CC triggers.
- **Configuration reflects only on a new session:** If the configuration is specific to a session and the session has already ingested the values, then SMF does not consider the new values. For example, PduContext (DB entry). This indicates that any update to the configuration does not impact the sessions that are already created. For instance, Charging Method in Profile or Charg-Profile in Charging Characteristics.
- **Configuration reflects instantly:** Configurations immediately ingest the dynamic values whenever they are updated. If SMF has already used a configuration and it is later updated, then it uses the latest values.

If a session is created using a Charging Profile, which later gets deleted from the Ops Center, the session might attempt to access the configuration structure of the deleted profile. In such cases, the Smf-Service pod maintains a default profile mapped to the sessions whose profiles are missing.

The Charging Profile is responsible for handling the SMF charging parameters.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 151: Charging Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
limit rating-group duration	Allowed	New values are used during the new URR creation or the subsequent URR update for the existing sessions. **Note** The dynamic configuration does not initiate a URR update.
max-charging-condition	Allowed	No impact
max-deferred-urr	Allowed	No impact
metering-method	Allowed	New values are used during the new URR creation for the existing sessions.
method	Allowed	No impact
reporting-level	Allowed	No impact
requested-service-unit time	Allowed	No impact
tight-interworking-mode	Allowed	No impact
triggers session	Allowed	No impact
Request Quota	Allowed	No impact

Charging-Characteristics Profile

The Charging-Characteristics Profile configuration defines the various parameters for a managing a charging characteristics for SMF Charging.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 152: Charging-Characteristics Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
charging-profile	Not Allowed	The configuration is used only once while setting up the session.

Charging-Action Profile

The Charging-Action Profile configuration defines the QoS and charging related parameters associated with the rule definitions.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 153: Charging-Action Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Rating group and Service ID	Allowed	No impact

Usage Reporting Rules ID Profile

The Usage Reporting Rules (URR-ID) specifies the configuration for the rating and service groups.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 154: URR-ID Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
URR ID for rg and ServID*	Allowed	No impact

Credit-Control-Group Profile

The Credit-Control-Group configuration defines the parameters to be used for subscribers who use the mapped rulebase.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 155: Credit-Control-Group Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Ignore Service ID	Allowed	No impact

Rulebase Profile

The Rulebase configuration parameters define the protocol rules to match a flow and associated actions to be taken for matching flow.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 156: Rulebase Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Ruledef association to Charging-action	Allowed	No impact
Credit-Control-Group	Allowed	The configuration is used only once while setting up the session.

GTPP Group Profile

The GTPP Group Profile configuration specifies the parameters for creating the GRPP group.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 157: GTPP Group Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Limits for offline configured urrs	Allowed	New values are used during the new URR creation for the existing sessions.

Upf-Apn Configuration Profile

The Upf-Apn Configuration Profile configuration defines the various parameters for the Upf-Apn parameters.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 158: Upf-Apn Configuration Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Association of gttp Group	Allowed	The configuration is used only once while setting up the session.

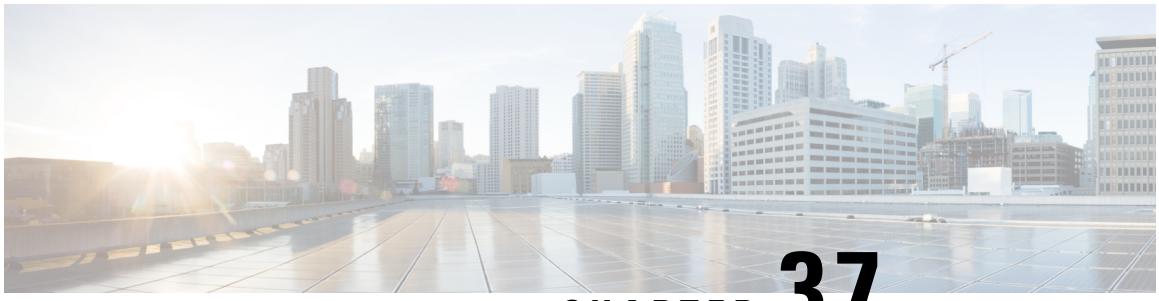
Network Profile for Peer CHF

The network profile for peer CHF configuration defines the various network configurations.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 159: Network Profile for Peer CHF Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Set of CHf's configured	Allowed	No impact



CHAPTER 37

SMF Deregistration with NRF

Feature Summary and Revision History

Summary Data

Table 160: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 161: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the deregistration of Network Function (NF) Repository Function (NRF), wherein the NF deregister service operation of the SMF removes the profile of a network function that is registered in the NRF.

The SMF starts the NF deregister service operation in the following scenarios:

- When the Service Based Interface (SBI) endpoint is not configured and all the rest endpoints stop functioning.
- When all the configured SBI endpoints VIP IP and N11 VIP IPs are offline.

How it Works

The NF deregister service operation deletes the specific resource based on its NF instance ID. The NF deregistration starts when the Uniform Resource Identifier (URI) receives a request to delete a specific NF instance.

The recommended SMF shutdown process involves the following steps:

1. All N11 and SBI VIP IPs are marked as offline. After these endpoints appear offline, the NF deregistration request is sent to the NRF. The NRF notifies the peer NFs, such as AMF, about the SMF shutdown and its unavailability for traffic.
2. Wait for a grace period to allow convergence and perform a "system mode shutdown" to stop all the pods.

When the endpoint SBI is not configured, the system deletes the rest-ep pod immediately and avoids proper convergence. Implementing the system mode shutdown without taking the SBI and N11 VIP IPs offline also avoids convergence.

Call Flows

This section describes the following call flows:

- NRF deregistration call flow
- NRF deregistration trigger events call flow

NF Deregistration Call Flow

This section describes the NF deregistration call flow.

Figure 112: NRF Deregistration Call Flow

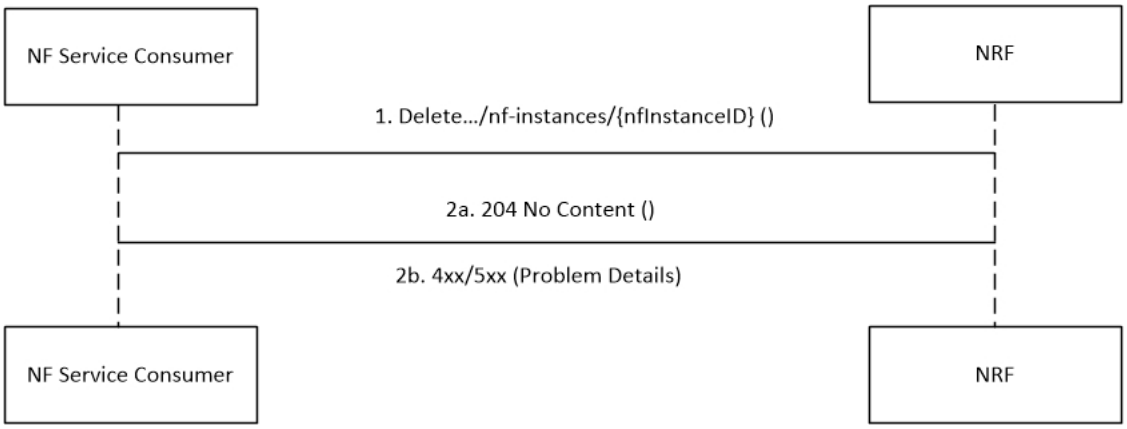


Table 162: NRF Deregistration Call Flow Description

Step	Description
1	The NF Service Consumer sends a Delete request to the resource URI that indicates the NF instance. The request body is empty.
2a	If the deletion of the specified resource is successful, the "204 No Content" message appears. The response body remains empty.
2b	If the NF instance, which is identified with the NF instance ID, does not exist in the list of registered NF instances in the NRF database, the NRF sends the "404 Not Found" status code with the problem details.

NF Deregistration Trigger Events Call Flow

This section describes the NF deregistration trigger events call flow.

Figure 113: NF Deregistration Trigger Events Call Flow

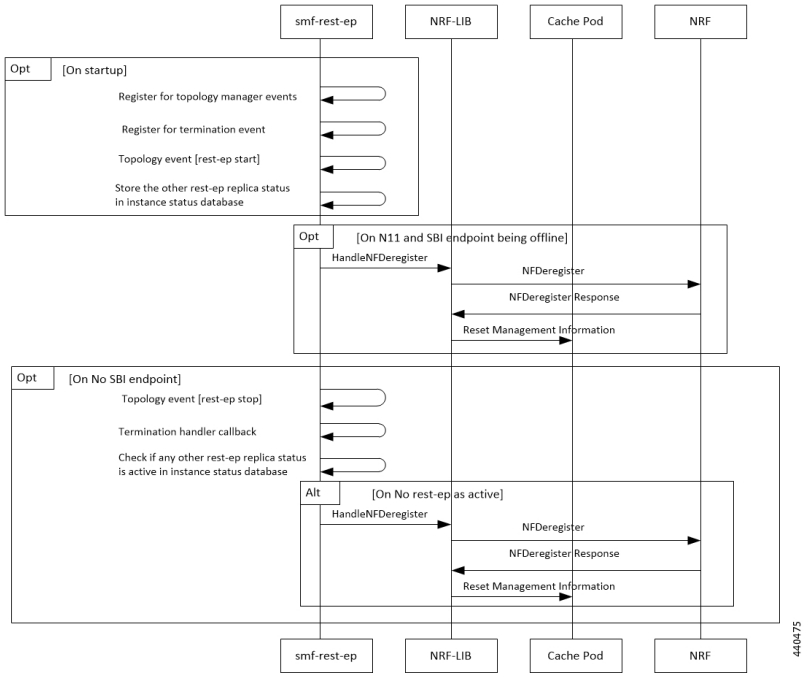


Table 163: NF Deregistration Trigger Events Call Flow Description

Step	Description
On startup	
1	The SMF rest-ep registers for topology manager events to identify the state of other rest-ep instances and keeps a track of these instances in an instance state database.
2	The SMF rest-ep registers for the termination handler with the application infrastructure for receiving notification when the application infrastructure stops functioning. As part of the termination handler, the SMF rest-ep monitors the instance state database for any other working rest-ep.

Step	Description
3	The SMF rest-ep starts the topology event.
4	The SMF rest-ep saves the status of other rest-ep replicas in the instance state database.
When the N11 and SBI endpoints are offline	
5	The SMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
6	When all the SBI and N11 VIP IP endpoints are offline, the SMF rest-ep sends the deregistration request to the NRF.
7	The NRF sends the NF deregister response to the NRF-Lib.
8	The NRF-Lib resets all the management information that is configured in the cache pod.
When no SBI endpoint exists	
9	The SMF rest-ep starts the topology event to stop the other rest-ep.
10	The SMF rest-ep starts the termination handler callback.
11	The SMF rest-ep checks the instance status database for any other working rest-ep.
When no rest-ep is functional	
12	The SMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
13	The SMF rest-ep sends the deregistration request to the NRF.
14	The NRF sends the NF deregistration response to the NRF-Lib.
15	The NRF-Lib resets all the management information that is configured in the cache pod.

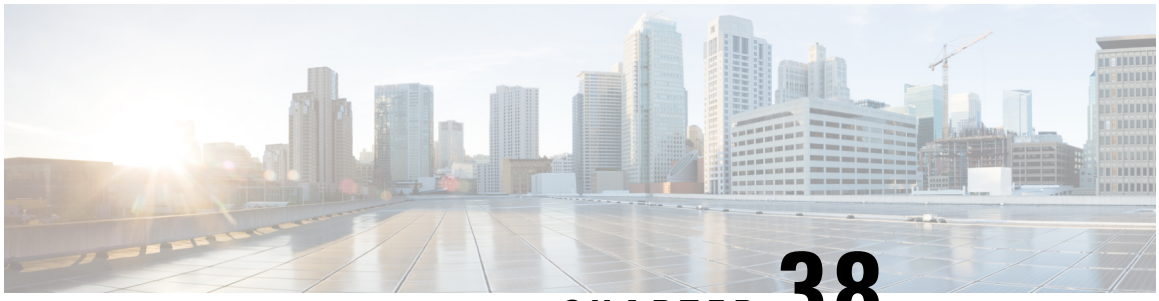
Standards Compliance

The SMF deregistration with NRF feature complies with the 3GPP standard TS 29.510 V15.2.0 (2018-12).

Limitations

The SMF deregistration with NRF feature has the following limitation:

- When N11 and SBI VIP IPs are not marked offline, the NF deregistration is not sent for the system mode shutdown because there is no specific order for pod deletion. Also, no monitoring procedure exists to check if the rest-ep pods are working.



CHAPTER 38

Support for the Unsubscribe-To-Notifications Messages

Feature Summary and Revision History

Summary Data

Table 164: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Product(s) or Functional Area	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 165: Revision History

Revision Details	Release
First introduced.	2020.02.2

Feature Description

The Unified Data Management (UDM) is responsible for primarily storing the subscriber data, which SMF accesses for managing the user sessions on the network. The SMF explicitly subscribes to receive the notifications about the events that occur in the subscriber data such session terminate. When the SMF wants to stop receiving the notifications, it initiates the Unsubscribe-to-Notification messages to UDM. Upon receiving these messages, the UDM cancels the subscription by removing the notification subscription for the subscribed session.

How it Works

This section provides a brief of how the SMF and UDM interact over the Unsubscribe-to-Notifications message:

1. The NF such as SMF sends an Unsubscribe-to-Notifications request to the resource identified by the URI to the UDM. The SMF transacts the request to the UDM over the N10 interface. The Unsubscribe-to-Notifications request lets the SMF unsubscribe from notifications for a specific subscriber session. The SMF receives the URI details during the subscription creation process.

   The Unsubscribe-to-Notifications request contains the ‘SUPI’ and ‘subscriptionId’ in the URI.

2. The UDM processes the request, and based on the response; it sends a response code to the SMF. For example, if the unsubscription is successful, then UDM sends 204 code. If the request is not processed, then the appropriate HTTP status code indicating the error is returned in the response body along with the additional error information.

3. The SMF is equipped to handle the timeout and failure that occurs when sending the Unsubscribe-to-Notifications messages to the UDM. In the event, the Unsubscribe-to-Notifications request fails, the SMF continues to purge the corresponding sessions.

   The Unsubscribe-to-Notification message is required for sessions that are hosted on the EUTRA network. They may not be a requirement for sessions that are released on the NR and WLAN network. For these access types, the SMF sends the UDM registration and deregistration messages that include subscription to notifications through implicit-unsubscribe during the deregistration.

Standards Compliance

The Support for the Unsubscribe-To-Notifications Messages feature complies with the following standards:

- 3GPP TS 29.503 - 5G System; Unified Data Management Services

Call Flows

This section describes the call flow for the Unsubscribe-To-Notifications message support.

Unsubscribe-to-Notifications Call Flow

This section describes the call flow on how the SMF sends a request to the UDM to unsubscribe from notifications of data changes.

Figure 114: Unsubscribe-to-Notifications Interaction with UDM

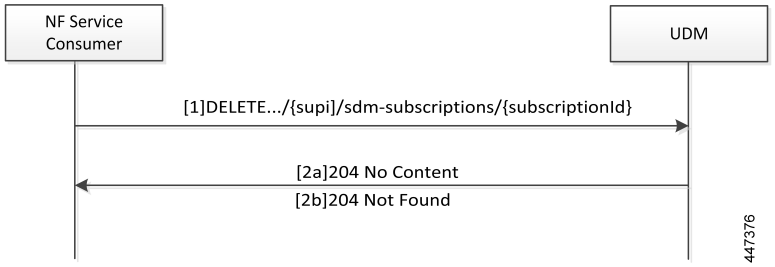


Table 166: Unsubscribe-to-Notifications Interaction Call Flow Description

Step	Description
1	The NF service consumer such as SMF sends a request to the UDM to unsubscribe from notifications. By unsubscribing, the UDM no longer sends notifications to SMF when the data modifications occur in the respective subscriber session. The NF service consumer sends a DELETE request to the resource identified by the URI. The NF service consumer receives the URI when the subscription gets created.
2a	If the deletion of request is successful, the UDM responds with "204 No Content".
2b	If the subscription is invalid, which could be due to an unknown subscriptionId value, then the HTTP status code "404 Not Found" is returned along with the additional error information in the response body (as part of the "ProblemDetails" element). If the request is not processed, then the appropriate HTTP status code indicating the error is returned in the DELETE response body along with the additional error information.

OAM Support for the Unsubscribe-To-Notifications Messages

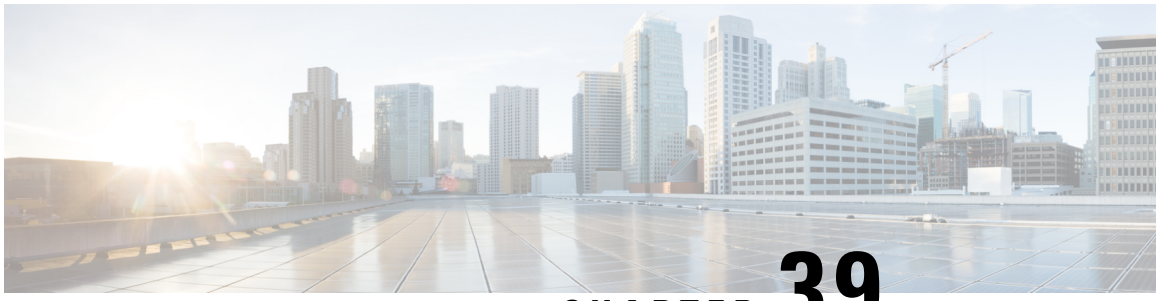
This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF maintains the following labels on the smf-rest-ep pod for monitoring the number of unsubscribe-to-notifications messages that are initiated towards UDM:

- nfType – “udm”
- messageDirection – “outbound”
- apiName – “sdm_unsubscription_req”
- nfUri – “nf_uri”
- respStatus – “response_status”

- rspCause – “response_cause”



CHAPTER 39

SMF Interface for Metrics

Feature Summary and Revision History

Summary Data

Feature Summary

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 167: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

SMF uses Prometheus for gathering statistics/counters from its microservices.

Grafana is used as the user interface to view metrics. It pulls the data from the Prometheus data store. Default graphs for KPI are available using Grafana for rendering a graphical view of the statistics with timelines.

For each microservice, counters and a set of labels are defined. Counters are incremented/decremented with the set of labels depending on the functionality.

The following snapshot is a sample of the Grafana dashboard.

Figure 115: Grafana Dashboard

SMF Rest EP Microservice

This section describes the supported counters and set of labels for the SMF Rest EP microservice.

Counters

The SMF REST EP microservice includes the following counters:

Table 168: SMF REST EP Microservice Counters

Number	Metric	Description
1	smf_restep_http_msg_total	This counter is incremented with every HTTP message received/sent at rest-ep microservice.
2	smf_restep_http_msg	This counter is incremented with every HTTP message received/sent at rest-ep microservice along with the time taken to serve the message.

Labels

The SMF REST EP microservice includes the following labels for the counters:

Table 169: SMF REST EP Microservice Labels for Counters

Number	Label	Description
1	NF TYPE	This label can be any 5G Node that interacts with SMF. For example: AMF, PCF, NRF
2	MESSAGE DIRECTION	Displays the direction of the HTTP message with respect to the REST EP microservice. The possible values are: “inbound” “outbound”
3	API NAME	Displays the service name being served. It can be: "register_ue" "deregister_ue" "subscription_req" "nf_registration" "nf_discovery" "slice_selection" "amf_create_sm_context" "amf_update_sm_context" "amf_release_sm_context" "amf_n1_n2_transfer" "pcf_sm_policy_control_create" "pcf_sm_policy_control_update" "pcf_sm_policy_control_delete" "pcf_sm_policy_control_update_notify" "pcf_sm_policy_control_terminate_notify"
4	NF URI	Displays the rest-ep URI used in the HTTP message (can be FQDN).
5	RESPONSE STATUS	Displays the HTTP Response. It can be any 2xx, 4xx or 5xx response.

SMF Service

This section describes the supported counters and set of labels for the SMF service.

Labels

The SMF service includes the following labels for the counters:

Table 170: SMF Service Labels for Counters

Number	Label	Description
1	PROCEDURE TYPE	This label can take any value depending on the type of procedure queried for: "pdu_sess_create" "ue_req_pdu_sess_mod" "smf_req_pdu_sess_mod" "pcf_req_pdu_sess_mod" "ue_req_pdu_sess_rel" "smf_req_pdu_sess_rel" "pcf_req_pdu_sess_rel" "amf_req_pdu_sess_rel"
2	STATUS	Displays the status type. The possible values are: “attempted” “success” “failure”
3	PDU CONNECTION TYPE	Displays the PDU connection type. The possible values are: “ipv4” “ipv6” “ipv4v6”
4	PDU STATE	Displays the PDU state. The possible values are: “idle” “connected”

SMF Protocol Microservice

This section describes the supported counters and set of labels for the SMF Protocol microservice.

Counters

The SMF service includes the following counters:

Table 171: SMF Service Counters

Number	Metric	Description
1	smf_service_stats	This counter is incremented with every query made to the smf-service.
2	smf_service_counters	This is a gauge counter and can be incremented/decremented based on the functionality with every query made to the smf-service.

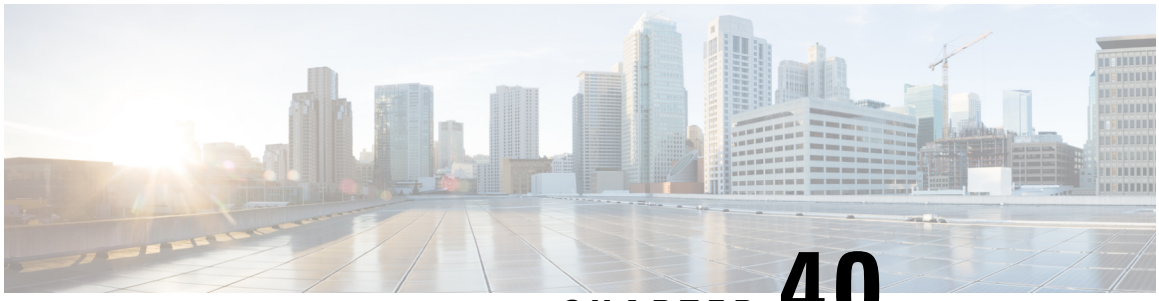
Labels

The SMF Protocol service includes the following labels for the counters:

Table 172: SMF Protocol Service Labels for Counters

Number	Label	Description
1	MESSAGE NAME	This label can take any value depending on the procedure queried for: "n4_session_establishment_req" "n4_session_establishment_res" "n4_session_modification_req" "n4_session_modification_res" "n4_session_report_req" "n4_session_report_res" "n4_session_deletion_req" "n4_session_deletion_res" "n4_association_setup_req" "n4_association_setup_res" "n4_association_update_req" "n4_association_update_res" "n4_association_release_req" "n4_association_release_res" "n4_prime_pfd_management_req" "n4_prime_pfd_management_res" "n4_heartbeat_req" "n4_heartbeat_res" "n4_node_report_req" "n4_node_report_res"

Number	Label	Description
2	MESSAGE DIRECTION	Displays the direction of the HTTP message with respect to the REST EP microservice. The possible values are: “inbound” “outbound”
3	STATUS	Displays the status of the message. The possible values are: “accepted” “denied” “discarded”



CHAPTER 40

SMF Logging

Feature Summary and Revision History

Summary Data

Feature Summary

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 173: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

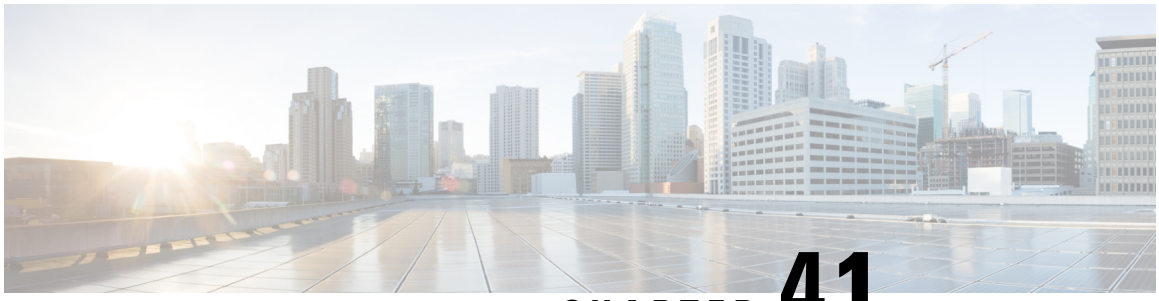
Feature Description

SMF utilizes the common logging framework to generate logs from its micro-services.

The supported logging levels are:

- Error

- Warn
- Info
- Debug
- Trace



CHAPTER 41

Timers Support

Feature Summary and Revision History

Summary Data

Table 174: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 175: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

The SMF supports configurable timers that are either 3GPP compliant or custom-driven.

This chapter provides detailed information about the function, operation and configuration of the timers. This chapter covers the following topics:

- 3GPP-compliant timers
  - GTP timer
  - N11 timer
- Custom-driven timers
  - Absolute timer
  - Control plane inactive timer
  - User plane inactive timer

3GPP-compliant Timers

Feature Description

The SMF supports retransmission through the GTP and N11 timers. With this provision, when the peer does not respond with the timer value, the SMF retransmits the GTP and N11 requests. The SMF lets you configure the maximum number of retransmissions.

Note The SMF provides configuration support for GTP timer and N11 timers.

How it Works

The SMF supports the following 3GPP timers:

- **GTP retransmission timer:**

  The SMF/PGW-C starts the timer denoted in the T3-RESPONSE. The timer is invoked when a signalling message (for which a reply is expected) is sent. A signalling message or the triggered message might get lost if a response is not received before the T3-RESPONSE timer expires.

  Once the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is then retransmitted if the total number of retry attempts is less than N3REQUESTS.

- **5G N1N2 reattempt timer:**

  If AMF rejects the N1N2 MessageTransfer with cause code as "Temporary reject registration ongoing" or "Temporary reject handover ongoing', then the SMF starts the timer for reattempting N1N2 MessageTransfer.

  Once the timer expires, the message corresponding to N1N2 MessageTransfer is reattempted based on the configured retry attempts.

Standards Compliance

The 3GPP timers support feature complies with the following standards:

- 3GPP TS 29.510 V15.2.0 (2018-12)

Configuration Support for the 3GPP Timers Feature

This section describes how to configure the 3GPP timers support feature.

Configuring the N11 Timers

This section describes how to configure the N11 timers.

The N11 timer configuration is invoked when AMF rejects the N1N2 message transfer with the cause code as "Temporary reject registration ongoing" or "Temporary reject handover ongoing", then SMF considers the timer and reattempts the message transfer. When the timer expires, the transfer is reattempted based on the configured retry count.

```
configure
  profile failure-handling failure_handling_name
     interface [ gtpc | N11 ] message message_type
       cause-code [ temp-reject-register | temp-reject-handover ]
         action [ retry { timeout timeout_duration | max-retry retry_count }
|clear | terminate ]
         end
```

NOTES:

- **profile failure-handling** *failure_handling_name*— Enter the name of the profile for failure handling.
- **interface [gtpc | N11]** — Configures the interface over which the message transfer must happen.
- **message** *message_type*— Configures the message type that must be transferred over the interface. The N11 interface supports the message type as n1n2transfer.
- **cause-code [temp-reject-register | temp-reject-handover]** — Configures the HTTP cause code. You can configure multiple cause code values for a message.
- **action [retry | clear | terminate]**— Configures the action that must be performed when the message transfer is not successful.

  Note Clear and terminate are not supported for the N11 interface.

- **action [retry { max-retry** *retry_count* **| timeout** *timeout_duration* **}** — Specifies the number of times the message transfer must be reattempted and the time interval between the consecutive attempts.

Example Configuration

Following is an example of N11 timer configuration.

```
show running-config
profile failure-handling n11-fht
  interface n11 message n1n2transfer
```

```
cause-code temp-reject-register
 action retry
   timeout 1000
     max-retry 2
```

Configuring the GTP Timers

This section describes how to configure the GTP timers.

The GTP timer configuration is implemented when a signaling message or triggered message (for which a reply is expected) is lost as it did not get a response before the T3-RESPONSE timer expired. After the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is retransmitted if the total number of retry attempts is less than the N3-REQUESTS times.

```
configure
  endpoint gtp
     retransmission { max-retry retry_count | timeout timeout_duration }
     end
```

NOTES:

- **endpoint gtp**— Enters the GTP retransmission configuration.
- **max-retry** *retry_count*— Specifies the number of times the signalling message request to SMF must be reattempted. The accepted range is 0–5. Default range is 3. When the *retry_count* is set to "0", the retransmission feature is disabled.
- **timeout** *timeout_duration*— Configures the interval of time (in milliseconds) after which the GTP retransmission request is reattempted. The accepted range is 0–10. Default range is 2. When the *timeout_duration* is set to "0", the retransmission feature is disabled.

Example Configuration

Following is an example of GTP timer configuration.

```
show running-config
  endpoint gtp
   retransmission max-retry 2 timeout 5
```

Custom-driven Timers

Absolute Timer Support

Feature Description

The SMF supports Absolute Session Timeout for each PDU session. With this support, the SMF can retain the PDU session resources until the Absolute Session Timer expires.

You can configure *Absolute Session Timeout* value under the DNN-Profile. If you have not configured the timeout value, the session timeout feature appears disabled and no timer is initiated.

Based on the configured value under the DNN-Profile, the Absolute Session Timer is triggered during the session creation. You cannot modify the timer value during interim of handling any access and mobility

procedures for that session. After the timer expires, the SMF performs SMF-initiated release by informing all SBI interfaces and N4 Interfaces, that is, toward UE, UDM, PCF, CHF, and UPF interfaces.

Configuring Absolute Session Timeout

To configure Absolute Session Timeout parameter under the DNN profile:

```
configure
  profile dnn dnnprofile_name
     timeout absolute absolutetimer_value
     end
```

NOTES:

- *absolutetimer_value*: Specifies the maximum duration of the session (in seconds), before the system automatically terminates the session. The default value is 0, which indicates the function is disabled.

  absolutetimer_value must be an integer in the range of 0-2147483647.

The following is a sample configuration.

```
smf(config)# profile dnn intershat timeout absolute 900
```

Inactivity Timer Support

Feature Description

The SMF supports the following timers to handle the user plane (UP) and control plane (CP) inactive requests:

- UP inactivity timer
- UP idle timer
- CP idle timer

Configuring UP Inactivity Timer

To configure the UP inactivity timer under DNN profile, use the following commands:

```
configure
   profile dnn dnnprofile_name
      userplane-inactivity-timer timer_value
      end
```

NOTES:

- **userplane-inactivity-timer** *timer_value*: Specifies the timer value in seconds. *timer_value* must be an integer in the range of 0-86400. The default value of the timer is 0, which means the function is disabled.
- The SMF sends the configured inactivity timer to the UPF through the N4 PDU Session Establishment request. After the session establishment, if the configured value changes, the SMF reports the changes to the UPF through N4 modification request.
- The UPF starts the inactivity timer when there is no uplink or downlink data transmission over the N3 tunnel. The UPF stops the timer when the data transmission over N3 tunnel is resumed. On expiry of the timer, the UPF sends session report to the SMF with the user plane inactivity request (UPIR) flag set.

After receiving the report indication for a session, the SMF clears the session if it is a 4G session and initiates idle mode entry if it is a 5G session.

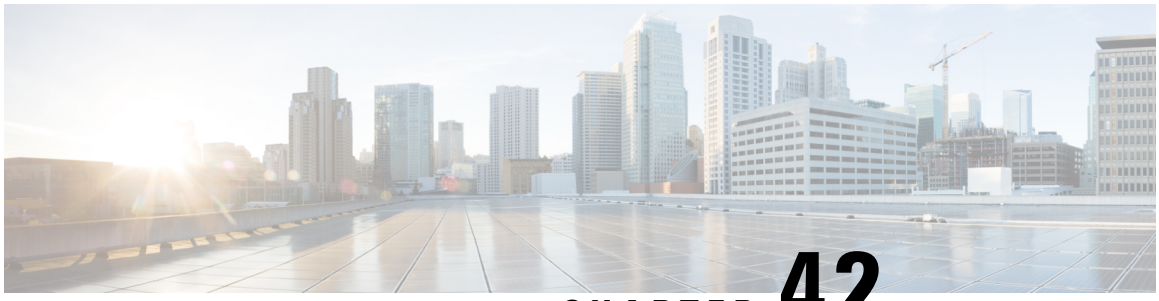
Configuring CP and UP Session Idle Timer

To configure the CP and UP idle timers under DNN profile, use the following commands:

```
configure
   profile dnn dnnprofile_name
      timeout { cp-idle timer_value | up-idle timer_value }
      end
```

NOTES:

- **cp-idle** *timer_value*: Specifies the maximum duration of the 5G session after the migration to CP idle state and before the automatic termination. The default value is 0, which indicates the function is disabled. *timer_value* must be an integer in the range of 0-2147483647.
- **up-idle** *timer_value*: Specifies the maximum duration of the 5G session after the migration to UP idle state and before the automatic termination. The default value is 0, which indicates the function is disabled. *timer_value* must be an integer in the range of 0-2147483647.
- The up-idle timer starts when an AN-initiated or Network-initiated 5G session enters the idle mode. This timer stops when the session exits the idle mode. On expiry of the timer, the SMF clears the 5G sessions.
- The cp-idle timer starts when any 4G or 5G procedure ends, and stops when any new procedure starts. If the timer expires, the SMF clears the session.



CHAPTER 42

UDP Proxy for SMF

Feature Summary and Revision History

Summary Data

Table 176: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 177: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF has UDP interfaces toward the UPF (N3) and SGW (s5/s8 for EPS interworking). With the help of the protocol layer pods (smf-protocol and gtp-ep), the messages are encoded and decoded and exchanged on these UDP interfaces. For achieving the functionalities mentioned on the 3GPP specifications:

- It is mandatory for the protocol layer pods to receive the original source and destination IP address and port number. But the original IP and UDP header is not preserved when the incoming packets arrive at the UDP service in the Kubernetes (K8s) cluster.
- Similarly, for the outgoing messages, the source IP set to the external IP address of the UDP service (published to the peer node) is mandatory. But the source IP is selected as per the egress interface, when different instances of protocol layer pods send outgoing messages from different nodes of the K8s cluster.

The protocol layer POD spawns on the node, which has the physical interface configured with the external IP address to achieve the conditions mentioned earlier. However, spawning the protocol layer pods has the following consequences:

- It is not possible to achieve the node level HA (High Availability) because the protocol pods are spawned on the same node of the K8s cluster. Any failure to that node may result in loss of service.
- The protocol pods (smf-protocol, gtp-ep, and radius-ep) must include their own UDP client and server functionalities. In addition, each protocol layer pod may require labeling of the K8s nodes with the affinity rules. This restricts the scaling requirements of the protocol layer pods.

The SMF addresses these issues with the introduction of a new K8s POD called "smf-udp-proxy." The primary objectives of this POD are:

- The "smf-udp-proxy" POD acts as a proxy for all kinds of UDP messages. It also owns the UDP client and server functionalities.
- The protocol pods perform the individual protocol (PFCP, GTP, Radius) encoding and decoding and provide the UDP payload to the "smf-udp-proxy" POD. The "smf-udp-proxy" POD sends the UDP payload out after it receives the payload from the protocol pods.
- The "smf-udp-proxy" POD opens the UDP sockets on a virtual IP (VIP) instead of a physical IP. This ensures that the "smf-udp-proxy" POD does not have any strict affinity to a specific K8s node (VM). Thus, enabling node level HA for the UDP proxy.

NOTE: One instance of the "smf-udp-proxy" POD is spawned by default in all the worker nodes in the K8s cluster. There are no changes to the configurations in this release.

Relationships

The UDP proxy for SMF feature has functional relationship with the following feature:

- Virtual IP Address.

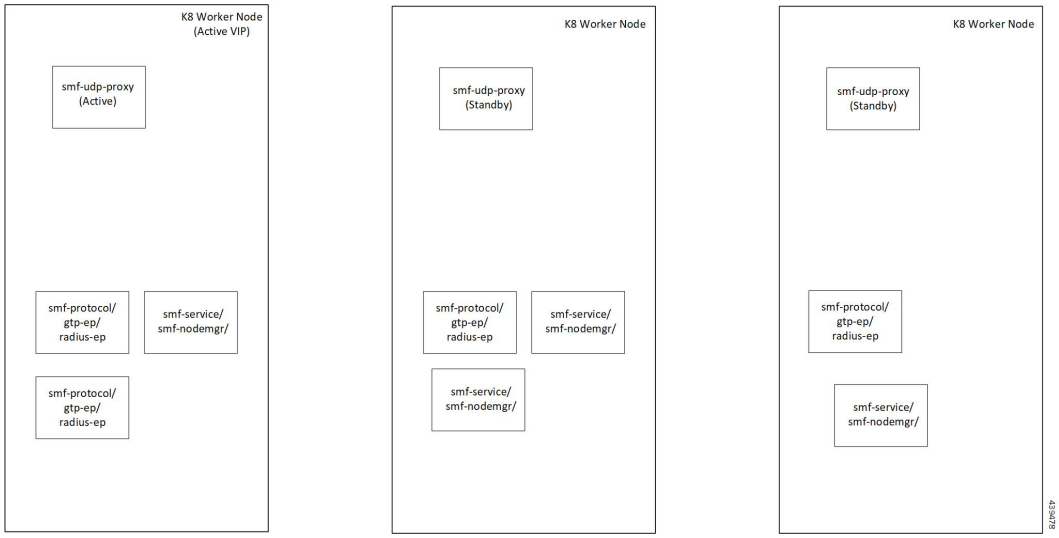
Architecture

The "smf-udp-proxy" POD is placed in the worker nodes in the K8s cluster.

1. Each of the K8s worker node contains one instance of the "smf-udp-proxy" POD. However, only one of the K8s worker node owns the virtual IP at any time. The worker node that owns the virtual IP remains in the active mode while all the other worker nodes remain in the standby mode.
2. The active "smf-udp-proxy" POD binds to the virtual IP and the designated ports for listening to the UDP messages from the peer nodes (UPF and SGW).

3. The UDP payload received from the peer nodes are forwarded to one instance of the smf-protocol, gtp-ep, or radius-ep pods. The payload is forwarded either on the same node or different node for further processing.
4. The response message from the smf-protocol, gtp-ep, or radius-ep pods is forwarded back to the active instance of the "smf-udp-proxy" POD. The "smf-udp-proxy" POD sends the response message back to the corresponding peer nodes.
5. The SMF-initiated messages are encoded at the smf-protocol, gtp-ep, or radius-ep pods. In addition, the UDP payload is sent to the "smf-udp-proxy" POD. Eventually, the "smf-udp-proxy" POD comprises of the complete IP payload and sends the message to the peer. When the response from the peer is received, the UDP payload is sent back to the same smf-protocol, gtp-ep, or radius-ep POD from which the message originated.

Figure 116: UDP Proxy Architecture



How it Works

The following sections describe the UDP proxy working principles.

Port and Sequence Number Selection

The duplicate messages are detected based on the source IP, source address, and sequence number for all UDP-based protocols. Each message from the peer includes a unique combination of these three parameters (source IP, source address, and sequence number).

In this release, only the sequence number changes for each new SMF initiated message. The SMF initiated messages use the same source IP (Virtual IP) and same port (fixed to 8809) number.

The sequence number (PFCP) is a 24-bit value. The 8 MSBs (Most Significant Bit) specify the smf-protocol pod's instance number. The 16 LSBs (Least Significant Bit) are incrementing counters, which generate a unique number for each instance of the smf-protocol POD.

NOTE: The UDP proxy uses the smf-protocol POD instance sequence number to determine the smf-protocol instance to which the response message must be forwarded to.

NOTE: Message retransmission and duplicate detection are not supported in this release.

Protocol POD Selection for Peer Initiated Messages

When the "smf-udp-proxy" POD receives the peer node (for instance UPF) initiated messages, it is load balanced across the smf-protocol instances to select any instance of the smf-protocol POD. An entry of this instance number is stored along with the source IP and source port number of the peer node. This ensures that the messages form the same source IP and source port are sent to the same instance that was selected earlier.

NOTE: This release does not support the landing of retransmitted messages (from the peer nodes) on the same instance of the smf-protocol where duplicate messages are detected.

High Availability for the UDP Proxy

The UDP proxy's HA model is based on the keepalived virtual IP concepts. A VIP is designated to the N4 interface during deployment. Also, a keepalived instance manages the VIP and ensures that the IP address of the VIP is created as the secondary address of an interface in one of the worker nodes of the K8s cluster.

The "smf-udp-proxy" instance on this worker node binds to the VIP and assumes the role of the active "smf-udp-proxy" POD. All "smf-udp-proxy" instances in other worker nodes remain in the standby mode.

When the worker node hosting the VIP fails, the keepalived instance moves the VIP to another worker node in the K8s cluster. The "smf-udp-proxy" instance in that worker node assumes the active role now.

NOTE: In this release, the VIP support for the "smf-udp-proxy" is enabled with single instance of "smf-udp-proxy." The failover scenario is not supported in this release.

Call Flows

This section describes the call flow defined for the UDP proxy feature.

UDP Proxy for SMF Call Flow

The following call flow describes the flow of messages for the SMF initiated messages (applicable to messages initiated by peer nodes as well).

Figure 117: UDP Proxy for SMF Call Flow

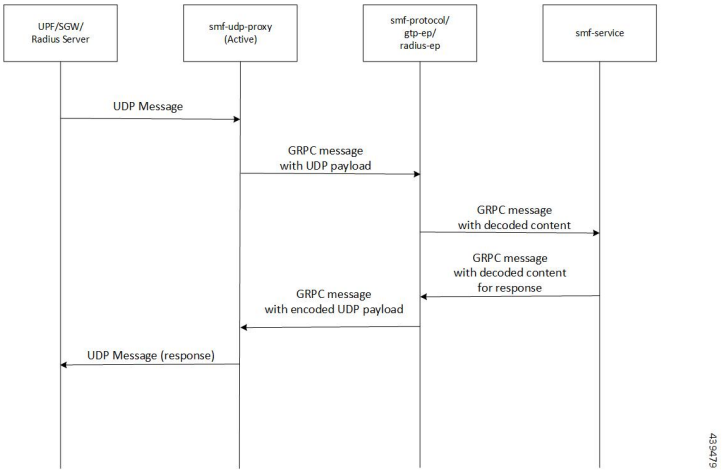
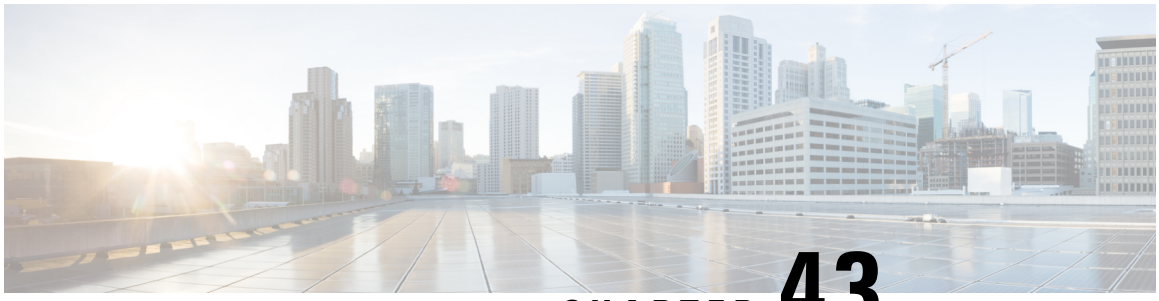


Table 178: UDP Proxy for SMF Call Flow

Step	Description
1	The peer nodes send the UDP messages to the VIP address. The active instance of "smf-udp-proxy" receives the UDP messages.
2	The UDP message's IP and the UDP header is stripped and the UDP payload is sent to the selected smf-protocol, gtp-ep, or radius-ep POD. The meta-data contains the source IP and source port number. With the help of the internal GRPC based IPC, the message is forwarded to the smf-protocol, gtp-ep, or radius-ep POD.
3	Based on the protocol, the smf-protocol, gtp-ep, or radius-ep POD decodes the message and loads the contents in proto-encoded buffer. The smf-protocol, gtp-ep, or radius-ep POD forwards the message to the smf-service POD for further processing over GRPC.
4	The smf-service POD generates the response message and sends it back to the smf-protocol, gtp-ep, or radius-ep POD in proto-encoded buffer.
5	The smf-protocol, gtp-ep, or radius-ep POD encodes the message and creates the UDP payload. The UDP payload is sent to the active "smf-udp-proxy" in a GRPC message.
6	The active "smf-udp-proxy" sends the message to the peer nodes on the UDP socket.



CHAPTER 43

UPF Path Management and Restoration

Feature Summary and Revision History

Summary Data

Table 179: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 180: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

A heartbeat is used to monitor the status of a UPF node in terms of its responsiveness. The heartbeat initiates a bilateral flow of request and response between the SMF and UPF.

The SMF periodically sends a signal in the form of a heartbeat request to the registered UPF node to determine if it is active. If the SMF does not receive a response from UPF after the retransmission attempts are exhausted, then SMF recognizes that a failure has occurred and purges the subscribers that are mapped to that UPF node.

You can control the number of heartbeat requests that SMF sends to UPF, the interval between the consecutive requests, and the duration until which SMF waits for a response.

Standards Compliance

The heartbeat transmission between SMF and UPF complies with the following standards:

- *3GPP TS 23.527*
- *3GPP TS 23.007*

How it Works

You can configure the heartbeat capability at the interface-level, UPF profile group-level, or both. The interface-level configuration is mandatory. If the interface-level configuration is unavailable, then the heartbeat parameters get configured with the default values. The profile-level configuration overrides the interface-level configuration.

The heartbeat feature is also extended to achieve high-availability for the Node Manager.

Interface and profile-level heartbeat

The SMF-UPF interaction to detect the UPF path failure using the heartbeat messages involves the following steps:

1. The SMF sends a heartbeat request message to the discovered UPF instances or profile groups based on the configured schedule.
2. If the UPF instance or profile is alive, it sends a heartbeat response to the SMF indicating that it is operational. In case the UPF does not send a heartbeat response, then SMF retransmits the heartbeat request based on the configured interval and the number of permitted attempts.
3. After the configured count of heartbeat message reattempts is exhausted and the SMF does not receive a response from UPF, then SMF starts 'Network requested PDU Session Release' procedure for the subscribers that are associated with that UPF.

Heartbeat and high-availability in Node Manager

Each UPF instance is associated with a primary and secondary Node Manager. The secondary Node Manager acts as a standby system on which the primary manager fails over. The primary Node Manager is responsible for the IP allocation and managing the association-specific messages such as association create, update, or delete request. To achieve uninterrupted access to the UPF and ensure a high-availability environment, the following interactions occur:

- When the Node Manager goes down or reinstated, it updates its status to all the mapped UPFs.
- In case the primary Node Manager is down, the secondary manager is notified. The secondary manager sends a heartbeat request to the UPF node to determine if the node is alive.
- When the secondary Node Manager is informed that the primary Node Manager is available, the secondary manager suspends the heartbeat timers and retransmission for the UPF node that is managed by the primary Node Manager.

Configuration Support for UPF Path Management and Restoration

This section describes how to configure the support for monitoring the UPF status.

Configuring the support for detecting the UPF status using the heartbeat feature involves the following steps:

- Configuring the Heartbeat Parameters for UPF
- Configuring the Heartbeat Parameters for UPF Profile
- Associating UPF Group to Individual UPF Network Configuration

Configuring the Heartbeat Parameters for UPF

This section describes how to configure the heartbeat feature for the UPF.

To configure the heartbeat feature for UPF at the interface-level, use the following configuration:

```
configure
  endpoint pfcp
  interface n4
  heartbeat
     interval interval
     max-retransmissions max_retry
     retransmission-timeout retry_count
     end
```

NOTES:

- **endpoint pfcp**— Enters the endpoint configuration mode.
- **interface**— Configures the N4 interface over which the heartbeat messages are exchanged between SMF and UPF.
- **heartbeat** — Enters the heartbeat configuration.
- **interval** *interval*— Specifies the heartbeat interval in seconds. The accepted range is 60–360. The default value is 60 seconds.

  Setting the *interval* to "0", disables the heartbeat feature.
- **max-retransmissions** *max_retry*— Specifies the maximum retries for the Packet Forwarding Control Protocol (PFCP) heartbeat request. The accepted range is 0–10. The default value is 3.

- **retransmission-timeout** *retry_count*— Specifies the heartbeat retransmission timeout in seconds. The accepted range is 1–20. The default value is 5.

Verifying the Heartbeat Configuration for UPF

This section describes how to verify the heartbeat configuration for UPF.

To view the configuration, use the **show running-config endpoint pfcp** command.

The following is a sample output of the **show running-config endpoint pfcp** command.

```
show running-config endpoint pfcp
endpoint pfcp
interface n4
  heartbeat
   interval               61
   retransmission-timeout 3
   max-retransmissions    5
  exit
exit
exit
```

Configuring the Heartbeat Parameters for the UPF Profile

This section describes how to configure the heartbeat feature for the UPF profile.

To configure the heartbeat parameters for the UPF profile, use the following configuration:

```
configure
   profile upf-group group_name
     heartbeat
       interval interval
       retransmission-timeout max_retry
       max-retransmissions retry_count
       end
```

NOTES:

- **profile upf-group** *group_name*— Specifies the UPF group for which the heartbeat feature must be enabled.
- **interface**— Configures the N4 interface over which the heartbeat messages are exchanged between SMF and UPF.
- **heartbeat** — Enters the heartbeat configuration.
- **interval** *interval*— Specifies the heartbeat interval in seconds. The accepted range is 60–360. The default value is 60 seconds.

  Setting the *interval* to "0", disables the heartbeat feature.
- **max-retransmissions** *max_retry*— Specifies the maximum retries for the Packet Forwarding Control Protocol (PFCP) heartbeat request. The accepted range is 0–10. The default value is 3.
- **retransmission-timeout** *retry_count*— Specifies the heartbeat retransmission timeout in seconds. The accepted range is 1–20. The default value is 5.

Verifying the Heartbeat Configuration for UPF Group

This section describes how to verify the heartbeat configuration for the UPF group.

To view the configuration, use the **show running-config profile upf-group** command.

The following is a sample output of the **show running-config profile upf-group** command.

```
show running-config profile upf-group
profile upf-group upfGroup1
heartbeat
  interval              62
  retransmission-timeout 3
  max-retransmissions    2
exit
exit
```

Associating UPF Group to Individual UPF Network Configuration

This section describes how to associate a UPF group with a UPF configuration.

Each UPF network configuration includes the UPF profile that associates each UPF instance with a UPF profile.

To associate an UPF group profile with a network configuration, use the following configuration:

```
configure
  profile network-element upf upf1
   upf-group-profile upf_group
   end
```

NOTES:

- **profile network-element upf**— Configures the UPF network configuration.
- **upf-group-profile** *upf_group*— Configures the UPF group name that must be associated to the specified UPF network configuration.

Verifying the Association of the UPF Group with the Individual UPF

This section describes how to verify the association of the UPF group with the individual UPF.

To view the association, use the **show running-config profile network-element upf** command.

The following is a sample output of the **show running-config profile network-element upf** command.

```
profile network-element upf upf1
n4-peer-address ipv4 10.80.70.229
n4-peer-port      8805
upf-group-profile upfGroup1
dnn-list          [ intershat intershat1 intershat2 ]
capacity          65535
priority          65535
```

OAM Support

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

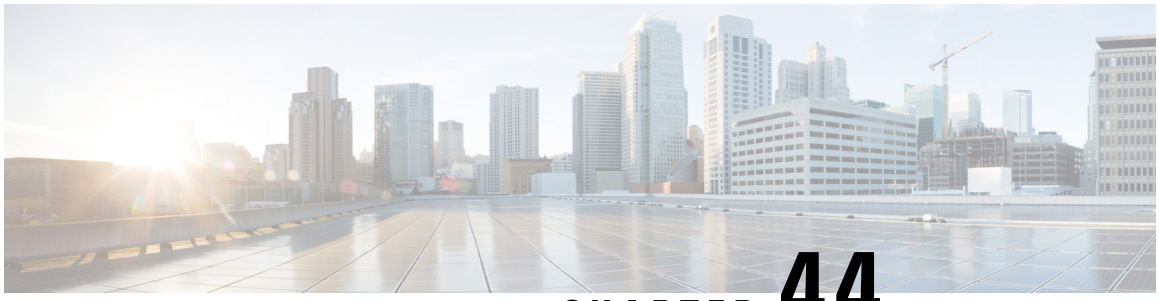
Bulk Statistics

The SMF maintains the following bulk statistics triggered during the heartbeat request and response procedure.

- nodemgr_upf_heartbeat_fail_stats— Counter that gets updated per UPF when it fails to respond to a heartbeat request.
- nodemgr_upf_hb_msg_stats— Counter for all the heartbeat messages for the specified UPF.

  The nodemgr_upf_heartbeat_fail_stats counter supports the following labels:

  - upf_heartbeat_req_tx— Label for the heartbeat request that the SMF sends.
  - upf_heartbeat_req_retx— Label for the retransmitted heartbeat request.
  - upf_heartbeat_rsp_rx— Label for the heartbeat response that the SMF receives.



CHAPTER 44

Voice over New Radio

Feature Summary and Revision History

Summary Data

Table 181: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 182: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

New Radio (NR) is the 5G radio access technology, and Voice over NR (VoNR) is the voice or video over the 5G network. VoNR is the target voice or video communication solution for 5G networks.

Voice services in 5GS over NG-RAN continue to be based on IP Multimedia Subsystem (IMS), such as Voice over LTE (VoLTE). VoNR is supported only when 5GS is connected to the IMS core.

Standards Compliance

The VoNR feature complies with the following standards:

- 3GPP TS 23.228, Release 15.3.0
- 3GPP TS 23.501, Release 15.4.0
- 3GPP TS 23.502, Release 15.4.0

VoNR P-CSCF Address Support

Feature Description

The SMF supports IMS Protocol Data Unit (PDU) Session Creation and fetches the P-CSCF addresses to be sent to the UE during initial attach over NR.

How it Works

The serving PLMN AMF sends an indication toward the UE during the registration procedure to indicate whether an IMS voice over PS session is supported in the 3GPP access network. A UE with "IMS voice over PS" voice capability over 3GPP access takes this indication into account when performing voice domain selection. The UE includes extended Protocol Configuration Options (ePCO) IE in "PDU Session Establishment Request" by setting P-CSCF container options in the AMF. Further, the AMF forwards these ePCO IE options in smContextCreate Request towards the SMF. The SMF fetches the P-CSCF addresses based on DNN profile, which maintains IMS-related data. The SMF includes P-CSCF IPv4 and IPv6 address in N1N2Message Transfer towards the AMF as per PDN-Types and requested P-CSCF container values.

Important The SMF does not include the P-CSCF address if the UE does not set the P-CSCF container options in the ePCO IE.

Call Flows

This section describes the call flow that is associated with this feature.

VoNR PDU Session Creation Call Flow

This section describes the VoNR PDU Session Creation call flow.

Figure 118: VoNR PDU Session Creation Call Flow

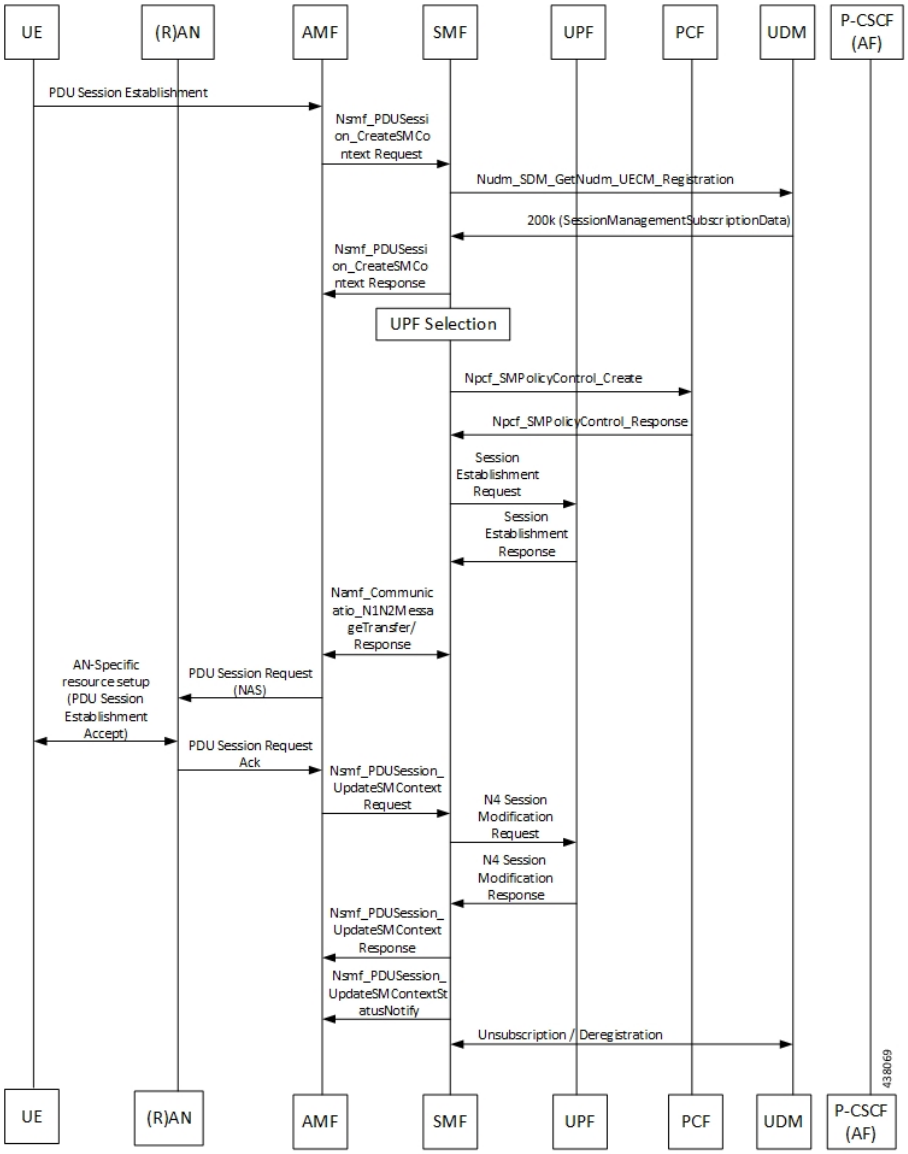


Table 183: VoNR PDU Session Creation Call Flow Description

Step	Description
1	Based on the UE registration with the RAN and the AMF, the UE set to "voice centric" for 5GS ensures that the voice service is always available. The UE selects the respective DNN for IMS. The UE initiates N1-Message with “PDU Session Establishment Request” by including container identifier “P-CSCF IPv4/IPv6 Request” in ePCO IE. NOTE: The DNN can be common for both the “voice” and “data” centric services.
2	The AMF performs the SMF selection as described in 3GPP TS 23.501.

Step	Description
3	The AMF sends Nsmf_PDUSession_CreateSMContext Request to the SMF by including N1 and N2 Message as Multipart along with ePCO IE if it is received from the UE in "PDU Session Establishment Request".
4	The SMF fetches the session management subscription data for the corresponding SUPI, DNN, and S-NSSAI. If it is not available locally, the SMF retrieves the subscription data using Nudm_SDM_Get and subscribes for the subscription data change notification using Nudm_SDM_Subscribe. The UDM retrieves this information from UDR using Nudr_DM_Query and subscribes to the notifications from the UDR for the same data by Nudr_DM_subscribe. The S-NSSAI used with the UDM is the S-NSSAI with value for the HPLMN. The SMF uses the DNN Selection Mode to decide the retrieval of session management subscription data. If the SMF is not subscribed for subscription data (DNN, S-NSSAI), then the SMF uses local configuration instead of session management subscription data.
5	The UDM provides the subscription details to the SMF. Based on the local configuration or session management subscription data from UDM for the respective DNN, the "IMS Voice over PS" is supported.
6	The SMF sends Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID, or N1 SM container (PDU Session Reject (Cause))) by processing the PDU Session Establishment Request. The SMF creates an SM context and responds to the AMF by providing an SM Context Identifier.
7	The SMF also selects one or more UPFs based on SSC mode, PDU Session-Type, and voice or data-centric services based on DNN capabilities.
8	The SMF initiates "Npcf_SMPolicyControl_Create" Request by including "SmPolicyContextData", which contains Supi, pduSessionId, ratType, servingNetwork, userLocationInfo, ueTimeZone, Pei, Online/Offline charging, chargingcharacteristics, PDU Session-Type, allocated UE IP address/prefix(es), subsDefQos, and information.
9	The PCF responds back with "Npcf_SMPolicyControl_CreateResponse (200 OK)" by including "SmPolicyDecision" in the message to the SMF. "SmPolicyDecision" contains the sessionRules, pccRules, qosDecs, chgDecs, chargingInfo, traffConDecs, umDecs, qosChars, and so on as defined in the 3GPP TS 29.512, Section 5.6.2.4. All these parameters are only applicable for "IMS Voice over PS session". This section does not cover Data and Voice PDU sessions. **Note** When a UE initiates a Resource Modification Request, and if the SMF includes the "qosFlowUsage" attribute containing "IMS_SIG" within SmPolicyUpdateContextDatadata structure and the PCF accepts that a QoS flow dedicated to IMS signaling can be used, the PCF returns the "qosFlowUsage" containing "IMS_SIG" value within the SmPolicyDecision data structure. The PCC rules provided have the 5QI applicable for IMS signaling.
10	The SMF initiates "N4 Session Establishment Request" to the UPF and provides packet detection, enforcement, and reporting rules to be installed on the UPF for this PDU session.

Step	Description
11	The UPF acknowledges by sending an N4 Session Establishment Response. If CN Tunnel Info is allocated by the UPF, the CN Tunnel Info is provided to SMF in this step.
12	The SMF sends Namf_Communication_N1N2MessageTransfer to the SMF. This transfer message includes the PDU Session ID, N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), CN Tunnel Info, S-NSSAI from the Allowed NSSAI, Session-AMBR, PDU Session Type, User Plane Security Enforcement information, UE Integrity Protection Maximum Data Rate), N1 SM container (PDU Session Establishment Accept (QoS Rule(s) and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s), selected SSC mode, S-NSSAI(s), DNN, allocated IPv4 address, interface identifier, Session-AMBR, selected PDU Session Type, Reflective QoS Timer (if available), P-CSCF address(es), and [Always-on PDU Session])). The N1 SM container contains the PDU Session Establishment Accept that the AMF provides to the UE. If the UE requested P-CSCF discovery, then the message also includes the P-CSCF IP addresses as determined by the SMF. The SMF fetches these P-CSCF addresses from DNN configuration, which are locally provisioned under DNN with IMS-Support and list of P-CSCF addresses or P-CSCF FQDN.
13	The AMF sends N2 PDU Session Request (N2 SM information, NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept))) to (R)AN.
14	The (R)AN issues AN-specific signaling exchange to the UE that is related with the information received from the SMF. The (R)AN also allocates (R)AN N3 Tunnel Info for the PDU session. The (R)AN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) that was provided in Step 12 to the UE. The (R)AN provides the NAS message only if the necessary (R)AN resources are established and the allocation of (R)AN Tunnel Info is successful.
15	The (R)AN sends N2 PDU Session Response (PDU Session ID, Cause, N2 SM information (PDU Session ID, AN Tunnel Info, List of accepted/rejected QFI(s), User Plane Enforcement Policy Notification)) to the AMF. The AN Tunnel Info corresponds to the Access Network address of the N3 tunnel corresponding to the PDU session. If the (R)AN rejects QFI(s) the SMF is responsible of updating the QoS rules and QoS flow-level QoS parameters if needed for the QoS flow associated with the QoS rule(s) in the UE accordingly. The NG-RAN rejects the establishment of UP resources for the PDU session when it cannot fulfill User Plane Security Enforcement information with a value of Required. The SMF releases the PDU session and the NG-RAN sends notification to the SMF when it cannot fulfill a User Plane Security Enforcement with a value of Preferred.

Step	Description
16	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type) to the SMF. The AMF forwards the N2 SM information received from (R)AN to the SMF. If the list of rejected QFI(s) is included in N2 SM information, the SMF releases the rejected QFI(s) associated QoS profiles. If the User Plane Enforcement Policy Notification in the N2 SM information indicates that no user plane resources can be established, and the User Plane Enforcement Policy indicated "required" as described in 3GPP TS 23.501, Section 5.10.3, the SMF releases the PDU session.
17	The SMF initiates an N4 Session Modification procedure with the UPF. The SMF provides AN Tunnel Info to the UPF and the corresponding forwarding rules.
18	The UPF provides an N4 Session Modification Response to the SMF.
19	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (Cause) to the AMF.
20	(Conditional) The SMF sends Nsmf_PDUSession_SMContextStatusNotify (Release) to the AMF.
21	If during the procedure, any time after Step 5, the PDU Session Establishment is not successful, the SMF informs the AMF by invoking Nsmf_PDUSession_SMContextStatusNotify (Release). The SMF also releases any N4 session(s) created, any PDU session address if allocated (for example, IP address) and releases the association with PCF, if any.

Limitations

Currently, only up to 64 address lists can be configured for both P-CSCF IPv4 and IPv6 addresses.

Configuring the VoNR P-CSCF Address Support

This section describes how to configure VoNR P-CSCF Address Support.

Configuring VoNR P-CSCF Address Support involves the following steps:

1. Creating P-CSCF Profile
2. Configuring P-CSCF Server Selection Method
3. Configuring P-CSCF Server Parameters
4. Defining P-CSCF Profile in DNN Profile Configuration

Creating P-CSCF Profile

Use the following configuration to create a P-CSCF profile instance:

```
configure
   profile pcscf pcscf_profile_name
   end
```

NOTES:

- **pcscf** *pcscf_profile_name*: Specifies the P-CSCF profile. This command creates a P-CSCF profile and provides access to the P-CSCF Profile Configuration mode. For details on the commands supported in this mode, see the *pcscf-profile* section in this document. *pcscf_profile_name* must be an alphanumeric string.

Configuring P-CSCF Server Selection

Use the following configuration to configure the P-CSCF server selection method:

```
configure
   profile pcscf pcscf_profile_name
      pcscf-selection round-robin
      end
```

NOTES:

- **pcscf-selection round-robin**: Configures the P-CSCF server selection method. Currently, round-robin is the only supported algorithm for the server selection.
- This command performs the round-robin selection of P-CSCF server based on the configured precedence value.

Configuring P-CSCF IPv4 Server

Use the following configuration to configure the P-CSCF IPv4 server:

```
configure
   profile pcscf pcscf_profile_name
      v4-list
      end
```

NOTES:

- **v4-list**: Prompts you to configure the P-CSCF IPv4 server details.
- Entering the **v4-list** command takes you to the P-CSCF IPv4 Server Configuration mode. For details on the commands supported in this mode, see the *CLI Reference Content*.

Configuring P-CSCF Primary and Secondary Server IPv4 Address

Use the following configuration to configure the IPv4 address of the primary and secondary P-CSCF servers.

```
configure
   profile pcscf pcscf_profile_name
      v4-list
         precedence value
            primary ipv4_address
            secondary ipv4_address
            end
```

NOTES:

- **precedence** *value*: Specifies the precedence value. *value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary** *ipv4_address*: Specifies the IPv4 address of the primary P-CSCF server in dotted-decimal notation.
- **secondary** *ipv4_address*: Specifies the IPv4 address of the secondary P-CSCF server in dotted-decimal notation.

Configuring P-CSCF IPv6 Server

Use the following configuration to configure the P-CSCF IPv6 server:

```
configure
   profile pcscf pcscf_profile_name
      v6-list
      end
```

NOTES:

- **v6-list**: Prompts you to configure the P-CSCF IPv6 server details.
- Entering the **v6-list** command prompts you to the P-CSCF IPv6 Server Configuration mode. For details on the commands supported in this mode, see the *CLI Reference* section.

Configuring P-CSCF Primary and Secondary Server IPv6 Address

Use the following configuration to configure the IPv6 address of the primary and secondary P-CSCF servers:

```
configure
   profile pcscf pcscf_profile_name
      v6-list
         precedence value
            primary ipv6_address
            secondary ipv6_address
            end
```

NOTES:

- **precedence** *value*: Specifies the precedence value. *value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary** *ipv6_address*: Specifies the IPv6 address of the primary P-CSCF server in colon-separated hexadecimal notation.
- **secondary** *ipv6_address*: Specifies the IPv6 address of the secondary P-CSCF server in colon-separated hexadecimal notation.

Configuring P-CSCF IPv4v6 Server

Use the following configuration to configure the P-CSCF IPv4v6 server:

```
configure
   profile pcscf pcscf_profile_name
      v4v6-list
      end
```

NOTES:

- **v4v6-list**: Prompts you to configure the P-CSCF IPv4v6 server details.
- Entering the **v4v6-list** command takes you to the P-CSCF IPv4v6 Server Configuration mode. For details on the commands supported in this mode, see the *CLI Reference* section.

Configuring P-CSCF Primary and Secondary Server IPv4v6 Address

This section describes how to configure the IPv4v6 address of the primary and secondary P-CSCF servers.

```
configure
   profile pcscf pcscf_profile_name
      v4v6-list
         precedence value
            primary ipv4 ipv4_address ipv6 ipv6_address
            secondary { [ ipv4 ipv4_address ] [ ipv6 ipv6_address ] }
            end
```

NOTES:

- **precedence** *value*: Specifies the precedence value. *value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary ipv4** *ipv4_address* **ipv6** *ipv6_address*: Specifies the IPv4 and IPv6 address of the primary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.
- **secondary { [ipv4** *ipv4_address* **] [ipv6** *ipv6_address* **] }**: Specifies the IPv4 and IPv6 address of the secondary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.

Defining P-CSCF Profile in DNN Profile Configuration

Use the following configuration to configure the P-CSCF profile in the existing DNN profile configuration:

```
configure
   profile dnn dnn_profile_name
      pcscf-profile pcscf_profile_name
      end
```

NOTES:

- **pcscf-profile** *pcscf_profile_name*: This command defines the P-CSCF profile to be associated with the DNN profile. *pcscf_profile_name* must be the name of the configured P-CSCF profile.

Verifying the Feature Configuration

Use the following show command to verify the P-CSCF FQDN feature configuration.

show running-config

The following is an example of the output of this show command:

```
profile pcscf pcscf1
fqdn cisco.com
v4-list
precedence 3
primrary 3.3.3.1
secondary 3.3.3.2
exit
precedence 5
primary 5.5.5.1
secondary 5.5.5.2
exit
```

VoNR MO and MT Call Support

Feature Description

The SMF supports Mobile Originated (MO) and Mobile Terminated (MT) VoNR with 5G QoS Identifier (5QI) as Guaranteed Bit Rate (GBR) flow for UE after the IMS PDU Session Creation. The SMF further supports VoNR calls for the following mobility (inter gNB, inter AMF) scenarios:

- MO and MT calls for idle mode UE
- MO and MT calls when the UE is handing over

During the mobility scenario of VoNR MO and MT calls, make sure to consider the following points:

- VoNR GBR flows are supported during UE and network service request procedures, Xn and N2 based handover.
- QoS failures at N1 and N2 interface, which are rejected by UE and gNB, are not handled by SMF.
- Charging features are not integrated with VoNR MO and MT, and mobility features.

Call Flows

This section describes the call flows associated with this feature.

VoNR MO Call Handling Procedure

This section describes the VoNR MO call handling procedure.

Figure 119: VoNR MO Call Handling Flow

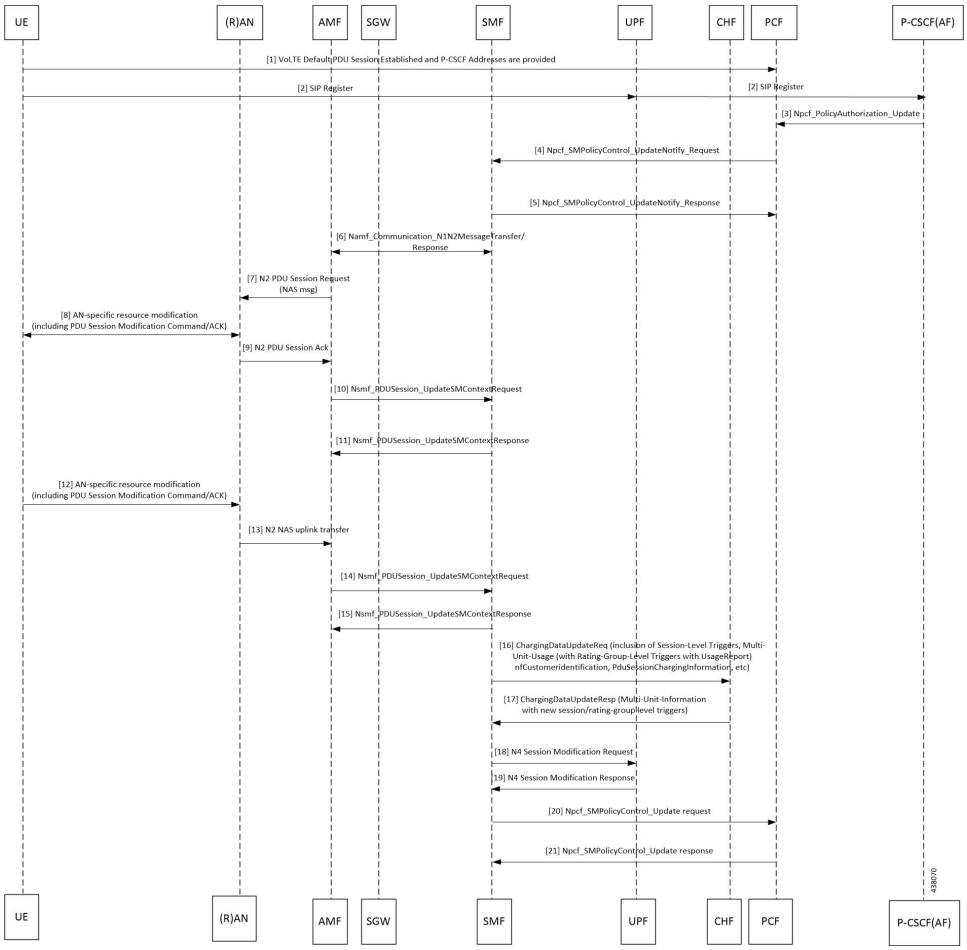


Table 184: VoNR MO Call Handling Flow Description

Step	Description
1	The SMF performs the PDU Session Establishment as described in the VoNR PDU Session Creation Call Flow, on page 600 section.
2	The UE initiates SIP Registration towards the called-party via UPF, P-CSCF through the backed IMS core network.
3	P-CSCF sends “Npcf_PolicyAuthorization_Update” to PCF to enforce policies, modify service information, gate control, modify subscription to SDF notification/deactivation, updating of traffic routing information, and so on (as defined in 3GPP TS 29.514). This service allows the NF consumer to subscribe and unsubscribe the notification of events (for example, change of Access Type, RAT type, or changes of the PLMN identifier).
4	The PCF sends Npcf_SMPolicyControl_UpdateNotify request to update and/or delete the PCC rule(s) PDU session-related policy context at the SMF and Policy Control Request Trigger information. This enforces PCC rules, policy control request triggers, SDF, and charging related information.

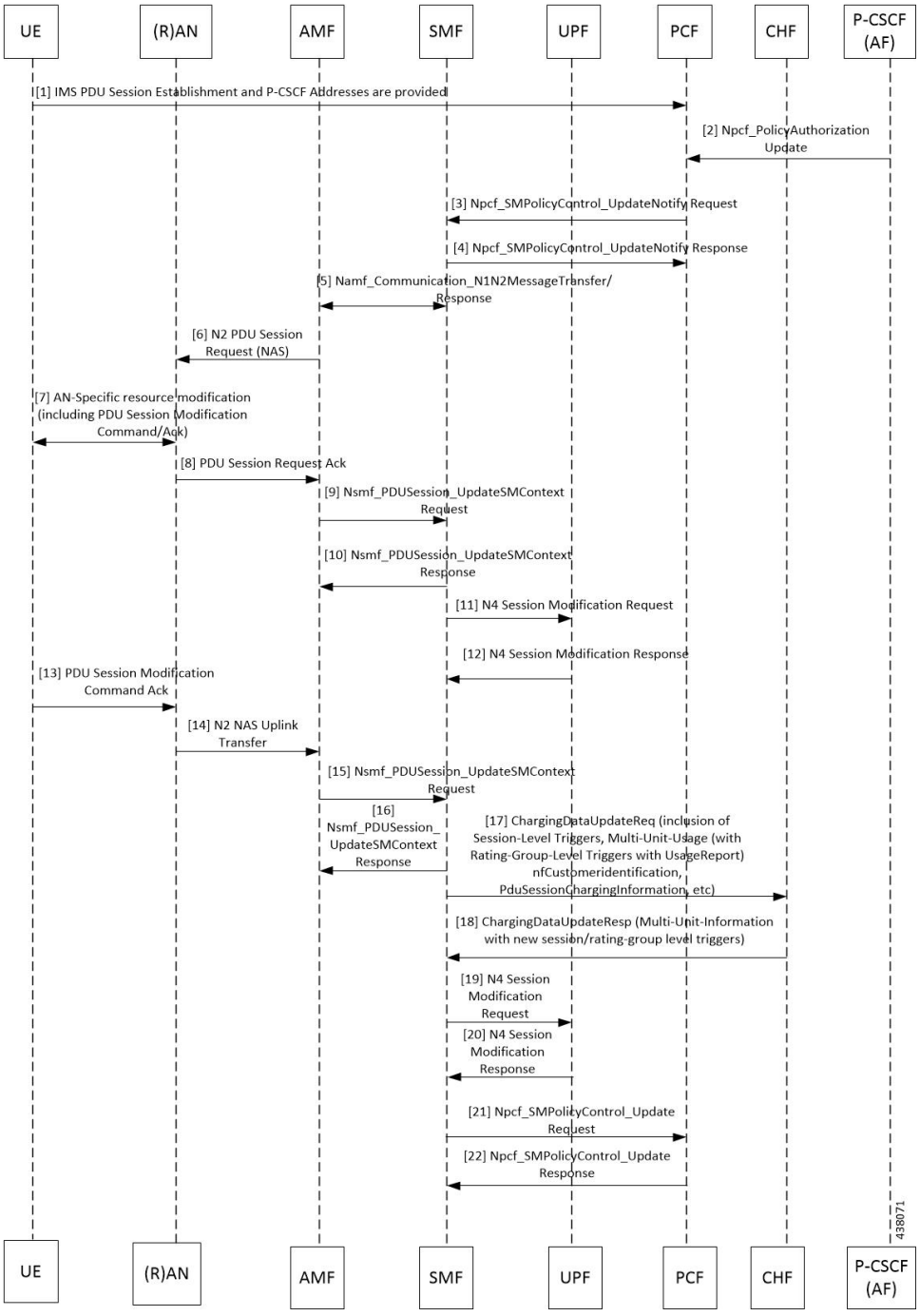
Step	Description
5	The SMF processes the received PCC rules and sends 200 OK message for a successful scenario. When the processing of any content fails, the SMF includes "400 Bad Request" in “Npcf_SMPolicyControl_UpdateNotify request” and sends it along with appropriate cause value as defined in 3GPP TS 29.512.
6	The SMF sends Namf_Communication_\nN1N2MessageTransfer/Response (PDU Session ID, QFIs, QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS rule(s), QoS Flow level parameters if needed for the QoS Flow(s) associated with the QoS rule(s), QoS rule operation, and QoS Flow level QoS parameters operation, Session-AMBR))). If the UE is in CM-IDLE state or Mobility handover (HO) state, see the procedure in VoNR MO Call Flow for UE in Idle Mode, on page 612.
7	The AMF sends N2 PDU Session Request (N2 SM information received from SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) message to the (R)AN.
8	The (R)AN issues AN specific signalling exchange with the UE that is related with the information received from SMF. For example, in an NG-RAN, an RRC Connection Reconfiguration takes place with the UE modifying the necessary (R)AN resources related to the PDU session.
9	The (R)AN acknowledges N2 PDU Session Request by sending a N2 PDU Session ACK (N2 SM information (List of accepted/rejected QFIs, AN Tunnel Info, PDU Session ID, Secondary RAT usage data), User Location Information) message to the AMF. In case of Dual Connectivity, if one or more QFIs were added to the PDU session, the master RAN node assigns one or more of these QFIs to an NG-RAN node which was not involved in the PDU session earlier. In this case, the AN Tunnel Info includes a new N3 tunnel endpoint for QFIs assigned to the new NG-RAN node. Correspondingly, if one or more QFIs were removed from the PDU session, a (R)AN node may no longer be involved in the PDU session anymore, and the corresponding tunnel endpoint is removed from the AN Tunnel Info. The NG-RAN rejects QFIs if it cannot fulfill the User Plane Security Enforcement information for a corresponding QoS Profile, for example, due to the UE Integrity Protection Maximum Data Rate being exceeded.
10	The AMF forwards the N2 SM information and the User Location Information received from the (R)AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. If the (R)AN rejects QFIs, the SMF updates the QoS rules and QoS parameters if needed for the QoS flow(s) associated with the QoS rule(s) in the UE accordingly.
11	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response. N2 SM information includes Secondary RAT Usage Data.
12	The UE acknowledges the PDU Session Modification Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command ACK)) message.
13	The (R)AN forwards the NAS message to the AMF.

Step	Description
14	The AMF forwards the N1 SM container (PDU Session Modification Command ACK) and User Location Information received from the (R)AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation.
15	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response. If the SMF-initiated modification is to delete QoS Flows (for example, triggered by PCF) which do not include QoS Flow associated with the default QoS rule and the SMF does not receive response from the UE, the SMF marks that the status of those QoS Flows is to be synchronized with the UE.
16	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
17	CHF provides ChargingDataUpdtaeResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides parameter changes for Session-Level and Rating-Group values.
18	The SMF updates N4 session of the UPF(s) that are involved in the PDU Session Modification by sending N4 Session Modification Request (N4 Session ID) message to the PCF. For a PDU Session of Ethernet PDU Session Type, the SMF notifies the PCF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s). The UPFs that are impacted in the PDU Session Modification procedure depend on the modified QoS parameters and the deployment. For example, in case of the session AMBR of a PDU Session with UL flow classifier (CL) changes, only the UL CL is involved.
19	The PCF sends an N4 session modification response message containing any information that the PCF has to provide to the SMF in response to the control information received.
20	For PCF-initiated policy modification case, the SMF notifies the PCF whether the PCC decision could be enforced or not by performing an SMF-initiated SM Policy Association Modification procedure as defined in 3GPP TS 23.502, Section 4.16.5.1. The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change.
21	The PCF sends an Npcf_SMPolicyControl_Update response with updated policy information about the PDU session.

VoNR MT Call Handling Procedure

This section describes the VoNR MT call handling procedure.

Figure 120: VoNR MT Call Handling Flow

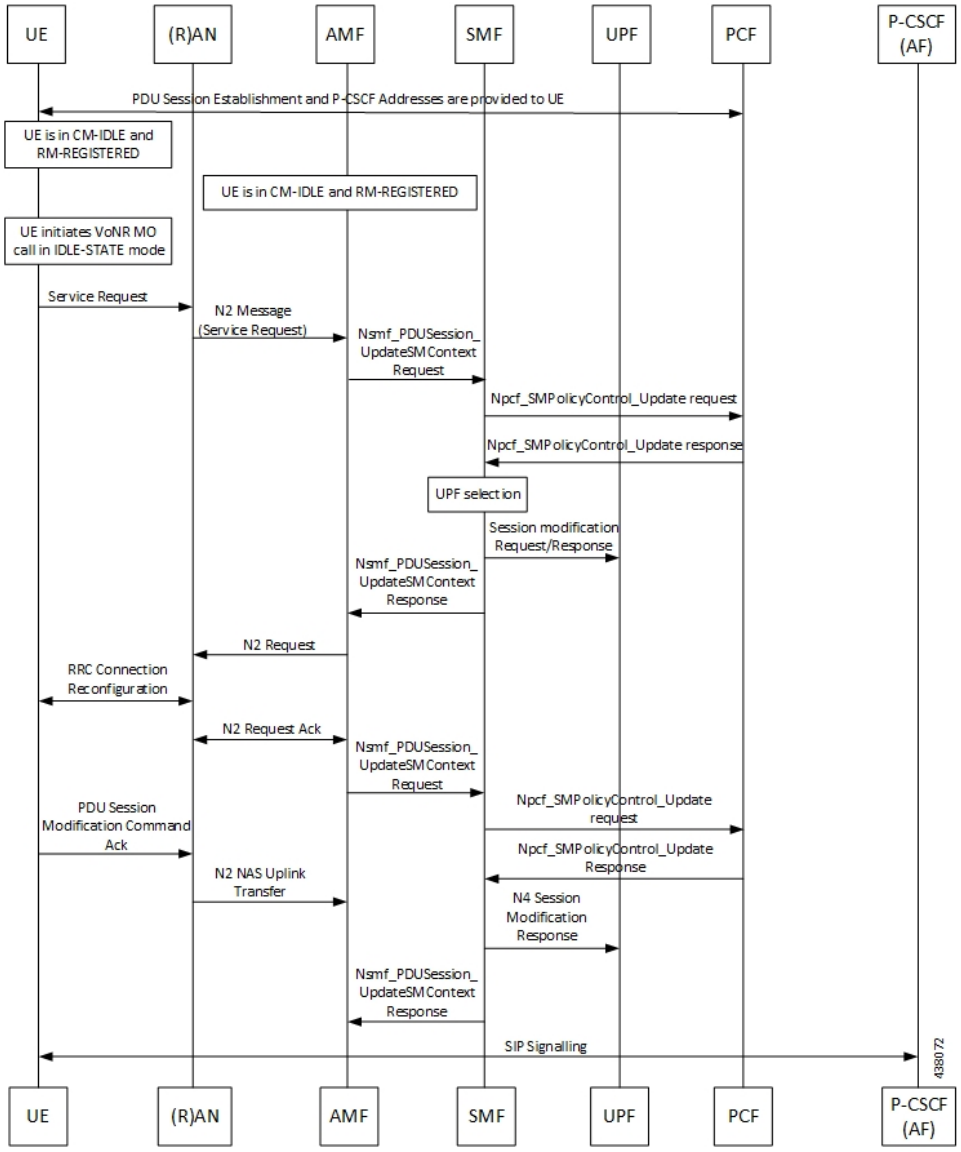


The VoNR MT call handling procedure remains the same as the VoNR MO call handling procedure except for the SIP Registration Request initiated from UE to P-CSCF(AF) through the UPF.

VoNR MO Call Flow for UE in Idle Mode

This section describes the VoNR MO call handling procedure when the UE is in idle mode.

Figure 121: VoNR MO Call Handling Flow for UE in Idle Mode



Step	Description
1	The SMF performs the PDU session establishment as described in VoNR PDU Session Creation Call Flow, on page 600 section, and fetches the P-CSCF addresses for sending it to the UE. The SMF programs UPF with Paging Policy Differentiation (PPD) for the respective PDU session as part of N4 interface by provisioning flows, and traffic detection information for every PDR.
2	The UE maintains its state in CM-IDLE and RM-REGISTERED.
3	The UPF maintains the UE in CM-IDLE and RM-REGISTERED state.
4	The UE initiates the VoNR call in CM-IDLE state.

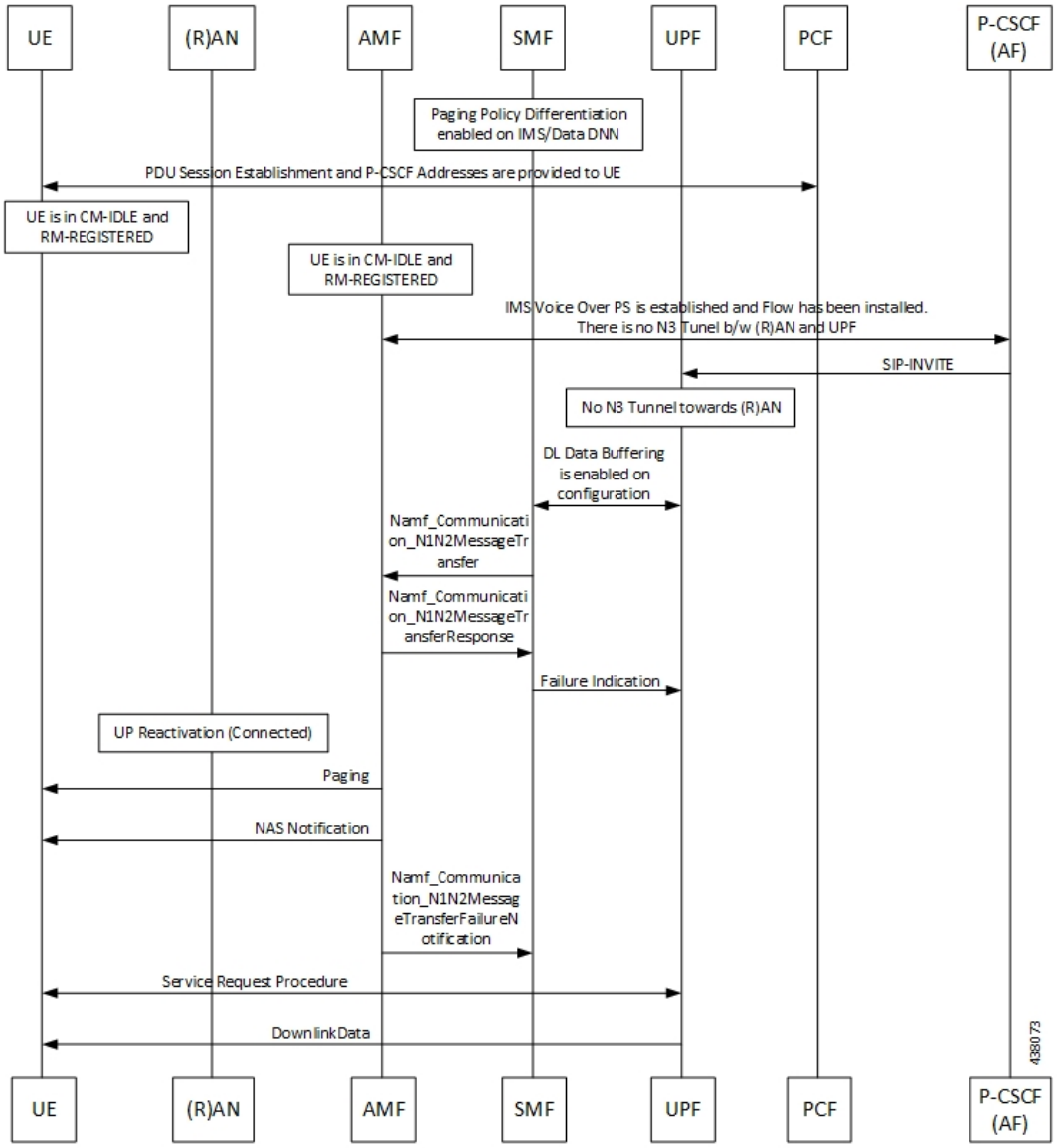
Step	Description
5	The UE performs Service-Request procedures as defined in 3GPP TS 23.502.
6	The RAN sends N2 message (service request) to the AMF.
7	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID(s), Operation Type, UE Location information, Access Type, RAT Type, UE presence in LADN service area, Indication of Access Type can be changed) to the SMF.
8	If the AMF notifies the SMF that the access type of the PDU session can be changed, and if the PCC is deployed, the SMF performs an SMF-initiated SM Policy Association Modification procedure as defined in 3GPP TS 23.502, Section 4.16.5.1.
9	The PCF provides the updated PCC Rule(s) to the SMF.
10	The SMF performs the UPF selection. **NOTE**: Selection of multiple or other UPFs is currently not supported.
11	The SMF initiates an N4 Session Modification request to the UPF. The SMF provides (R)AN Tunnel Info and the corresponding forwarding rules to the UPF. The UPF provides an N4 Session Modification Response to the SMF.
12	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (N2 SM information (PDU Session ID, QFI(s), QoS profile(s), CN N3 Tunnel Info, S-NSSAI, User Plane Security Enforcement, UE Integrity Protection Maximum Data Rate), N1 SM Container, Cause) to the AMF. The SMF sends N1 SM Container and/or N2 SM Information to the AMF when applicable.
13	The AMF sends N2 Request (N2 SM information received from SMF, security context, Mobility Restriction List, Subscribed UE-AMBR, MM NAS Service Accept, list of recommended cells, TAs, NG-RAN node identifiers, UE Radio Capability, Core Network Assistance Information, Tracing Requirements) to the (R)AN.
14	The NG-RAN performs RRC Connection Reconfiguration with the UE depending on the QoS Information for all the QoS Flows of the PDU sessions whose UP connections are activated, and Data Radio Bearers.
15	The (R)AN sends N2 Request Acknowledgement message (N2 SM information (AN Tunnel Info, List of accepted QoS Flows for the PDU Sessions whose UP connections are activated, List of rejected QoS Flows for the PDU Sessions whose UP connections are activated), PDU Session ID) to the AMF. The N2 Request ACK message includes N2 SM information, for example, AN Tunnel Info. NG-RAN responds N2 SM information with separate N2 message (for example, N2 tunnel setup response) if the AMF sends separate N2 message.

Step	Description
16	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, RAT Type, Access Type) per PDU Session to the SMF. The AMF determines Access Type and RAT Type based on the Global RAN Node ID associated with the N2 interface. If the AMF received N2 SM information (one or multiple), then the AMF forwards the N2 SM information to the relevant SMF per PDU Session ID. If the UE Time Zone has changed compared to the last reported UE Time Zone, then the AMF includes the UE Time Zone IE in this message.
17	The SMF notifies the PCF whether the PCC decision could be enforced or not by performing an SMF-initiated SM Policy Association Modification procedure as defined in 3GPP TS 23.502, Section 4.16.5.1. The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change.
18	The PCF sends an Npcf_SMPolicyControl_Update response with updated policy information about the PDU session.
19	The SMF updates N4 session of the UPF(s) that are involved in the PDU session modification by sending N4 Session Modification Request (N4 Session ID) message to the UPF. For a PDU session of Ethernet PDU Session Type, the SMF notifies the UPF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s). The UPFs that are impacted in the PDU Session Modification procedure depend on the modified QoS parameters and the deployment. For example, in case of the session AMBR of a PDU session with UL CL changes, only the UL CL is involved. The UPF sends an N4 session modification response message containing any information that the UPF has to provide to the SMF in response to the control information received.
20	The SMF sends a Nsmf_PDUSession_UpdateSMContext Response. The N2 SM information includes Secondary RAT Usage Data.

VoNR MT Call Flow for UE in Idle Mode

This section describes the VoNR MT call handling procedure when the UE is in idle mode.

Figure 122: VoNR MT Call Flow for UE in Idle Mode



The VoNR MT call flow remains the same as the VoNR MO call flow for service request when the UE is in CM-IDLE state except the following:

- The SIP-INVITE received by P-CSCF
- The PCC rule enforcements triggered from PCF towards SMF.

NOTE: The PCC rules, QoS, PDR, and traffic detection rule enforcements remain the same as the VoNR MT Call Handling procedure as defined in VoNR MT Call Handling Procedure, on page 611VoNR MT Call Handling Procedure.

When the AMF receives Namf_Communication_N1N2MessageTransfer Request (N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS rule(s), QoS Flow level parameters if needed for the QoS Flow(s) associated with the

QoS rule(s), QoS rule operation, and QoS Flow level parameters operation, Session-AMBR))) when the UE is in CM-IDLE state. If the UE is in CM-IDLE state and an Asynchronous type communication (ATC) is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer.

The AMF performs paging operations to the UE, and the UE triggers service request procedure. Once the paging is established, the AMF decides QoS Flows, QoS rules, and Session-AMBR that need to be accepted, which are received in Namf_Communication_N1N2MessageTransfer Request and the AMF performs Nsmf_PDUSession_UpdateSMContext operation with SMF to notify on accepting the QoS Flows, QoS rules, session-AMBR, and so on.

Paging Policy Differentiation Support

Feature Description

The SMF supports Paging Policy Differentiation feature by providing a configuration at PLMN, DNN, and 5QI level for data and IMS DNN sessions of the UE. The SMF provides Paging Policy Indicator based on UPF data. The SMF also supports QoS flow (PPI, ARP, and 5QI) towards the AMF over N11 interface.

Call Flows

This section describes the call flows associated with this feature.

VoNR Paging Policy Differentiation Procedure

This section describes the VoNR Paging Policy Differentiation procedure.

Figure 123: VoNR Paging Policy Differentiation Call Flow

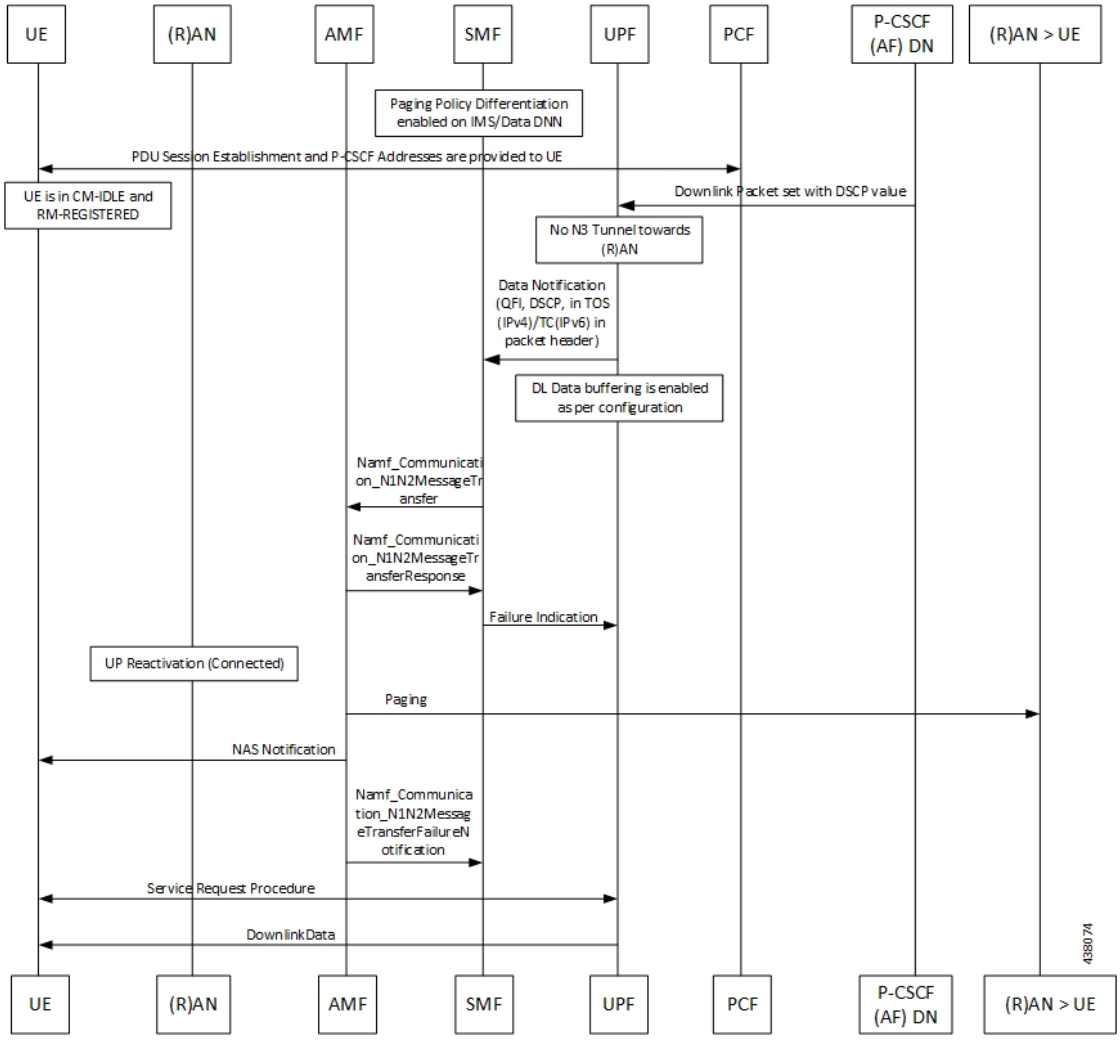


Table 185: VoNR Paging Policy Differentiation Call Flow Description

Step	Description
1	The SMF enables Paging Policy Differentiation (PPD) under DNN profile based on DNN, 5QI, and PLMN.
2	The SMF performs the PDU session establishment as described in VoNR PDU Session Creation Call Flow section, and fetches the P-CSCF addresses for sending it to the UE. The SMF programs UPF with PPD for the respective PDU session as part of N4 interface by provisioning flows, and traffic detection information for every PDR.
3	The UPF detects if any Downlink (DL) Packet is set with \nDSCP value (TOS in IPv4 / TC in IPv6) when PPD is enabled for the PDU session.
4	The UPF detects that there is no forwarding path as there is no N3 Tunnel for the DSP marked DL packets.

Step	Description
5	The UPF sends Data-Notification (QFI, DSCP in TOS (IPv4) / TC (IPv6) in packet header).
6	The UPF enables DL Data buffering based on the buffering configuration. The UPF sends Data Notification (N4 Session ID, Information to identify the QoS Flow for the DL data packet, DSCP) message to the SMF. **1.** On arrival of the first DL data packet for any QoS Flow, the UPF sends Data Notification message to the SMF, if the SMF has not previously notified the UPF (in which case the next steps are skipped). **2.** If the UPF receives DL data packets for another QoS Flow in the same PDU session, the UPF sends another Data Notification message to the SMF. **3.** If the Paging Policy Differentiation feature (as specified in TS 23.501, section 5.4.3) is supported by the UPF and if the PDU Session type is IP, the UPF includes the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the DL data packet and the information to identify the QoS Flow for the DL data packet. **4.** The SMF sends the Data Notification Acknowledgement message to the UPF. **5.** The UPF forwards the DL data packets towards the SMF on request. The SMF buffers the data packets.
7	The SMF determines the AMF and invokes the Namf_Communication_N1N2MessageTransfer to the AMF including the PDU Session ID based on N4 Session ID. The SMF, while waiting for the User Plane Connection to be activated, receives additional Data Notification message. The SMF derives a different Paging Policy Indicator according to the additional Data Notification or the DSCP of the data packet. The SMF invokes a new Namf_Communication_N1N2MessageTransfer indicating the higher priority or different Paging Policy Indicator to the AMF. When supporting Paging Policy Differentiation, the SMF determines the Paging Policy Indicator related to the downlink data that has been received from the UPF or triggered the Data Notification message, based on the DSCP as described in 3GPP TS 23.501, section 5.4.3. The SMF indicates the Paging Policy Indicator in the Namf_Communication_N1N2MessageTransfer.
8	The AMF sends Namf_Communication_N1N2MessageTransfer response to the SMF with a cause “Attempting to reach UE" if the UE is in CM_IDLE State. If the UE is in CM-CONNECTED state, then the AMF sends a Namf_Communication_N1N2MessageTransfer response to the SMF immediately with a cause "N1/N2 transfer success".
9	The SMF sends Failure Indication to the UPF on receiving a negative response from AMF.
10	The AMF initiates paging towards the UE through the (R)AN.
11	The AMF initiates NAS Notification towards the UE.

Step	Description
12	The AMF notifies the SMF by sending Namf_Communications_N1N2MessageTransfer Failure Notification to the Notification Target Address provided by the SMF if the UE does not respond to paging. The AMF is unaware of an ongoing Mobility Management (MM) procedure that prevents the UE from responding. The AMF receives an N14 Context Request message indicating that the UE performs Registration procedure with another AMF.
13	If the UE is in CM-IDLE state, upon receiving a paging request for a PDU session associated to 3GPP access, the UE initiates the UE Triggered Service Request procedure as defined in 3GPP TS 23.502, Section 4.2.3.2.

Configuring the VoNR Paging Profile Differentiation

This section describes how to configure VoNR Paging Profile Differentiation feature.

Configuring VoNR Paging Profile Differentiation feature involves the following steps:

1. Creating PPD Profile
2. Configuring PPD Profile Parameters
3. Enabling PPD in DNN Profile Configuration

Creating PPD Profile

Use the following configuration to create an instance of PPD profile:

```
configure
   profile ppd ppd_profile_name
   end
```

NOTES:

- **ppd** *ppd_profile_name*: Specifies the PPD profile. This command creates a PPD profile and provides access to the PPD Profile Configuration mode. For details on the commands supported in this mode, see the *ppd-profile* section in this document. *ppd_profile_name* must be an alphanumeric string.

Configuring PPD Profile Parameters

Use the following configuration to define the PPD profile parameters:

```
configure
   profile ppd ppd_profile_name
      5qi 5qi_value
      dscp dscp_value { ppi ppi_value }
      end
```

NOTES:

- **5qi**: Specifies the list of 5QI Priority Level. *5qi_value* must be an integer in the range of 0-127. To list the different priority levels, use comma and hyphen as needed. For example, 5QI 3,10-15,65.

- **dscp** *dscp_value*: Specifies the DSCP value. *dscp_value* must be an integer in the range of 0-63.
- **ppi** *ppi_value:* Specifies the paging policy indicator value. *ppi_value* must be an integer in the range of 0-7.

Enabling PPD in DNN Profile Configuration

Use the following configuration to enable the PPD feature in the existing DNN profile configuration:

```
configure
   profile dnn dnn_profile_name
      ppd-profile ppd_profile_name
      end
```

NOTES:

- **ppd-profile** *ppd_profile_name*: This command defines the PPD profile to be associated with the DNN profile. *pdd_profile_name* must be the name of the configured PPD profile.
- This command enables the PPD feature in the DNN profile based on the configured values of DNN, 5QI, and PLMN.

Verifying the Feature Configuration

Use the following show command to verify the feature configuration details.

show running-config

The following is an example of the output of this show command:

```
product smf# show running-config
profile dnn dnntst1
pcscf-profile pcscf1
!
```

P-CSCF FQDN

Feature Description

The SMF sends the DNS queries to the DNS server through the DNS proxy server to fetch a maximum of two P-CSCF IP addresses. This operation helps in resolving the Fully Qualified Domain Name (FQDN) of the P-CSCF. This release provides the configuration support for the P-CSCF FQDN within the SMF profile.

For more information on the configuration commands, see the Configuring the P-CSCF FQDN, on page 622 section.

Relationships

The P-CSCF FQDN feature works only when the DNS proxy is configured. For more information on the DNS proxy configuration, see the *DNS Proxy Integration in SMF* chapter.

Configuring the P-CSCF FQDN

Use the following configuration to define the FQDN of the P-CSCF.

```
configure
   profile pcscf pcscf_profile_name
      fqdn domain_name
      end
```

NOTES:

- **pcscf-profile** *pcscf_profile_name*: Specifies the P-CSCF profile name, and enters into the P-CSCF Profile Configuration mode. *pcscf_profile_name* must be an alphanumeric string.
- **fqdn** *domain_name*: Specifies the FQDN of the P-CSCF server. *domain_name* must be an alphanumeric string.

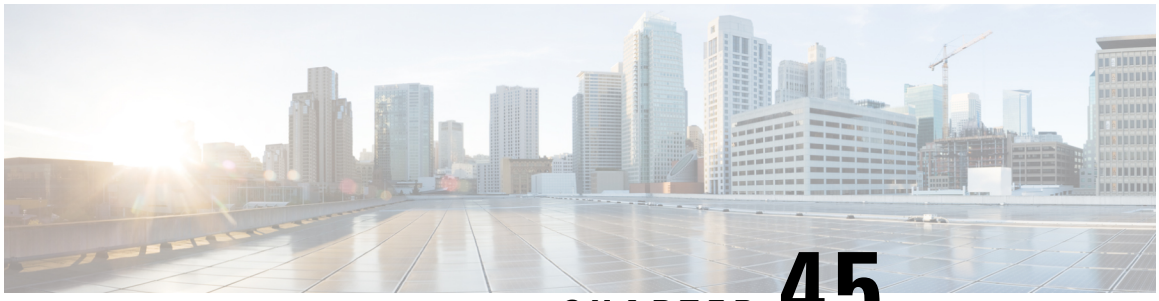
Verifying the Feature Configuration

Use the following show command to verify the feature configuration details.

show running-config

The following is an example of the output of this show command:

```
profile ppd ppdtemp
5QI 3,10-15,65
dscp 15 ppi 2
dscp 20 ppi 3
!
profile dnn ims
ppd-profile ppdtemp
!
```



CHAPTER 45

VoLTE Support

Feature Summary and Revision History

Summary Data

Table 186: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 187: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports Voice over Long-Term Evolution or LTE (VoLTE). The VoLTE technology utilizes IP Multimedia Subsystem (IMS) to allow you to make cellular calls over the LTE access network.

How it Works

A 5G mobile device with LTE access requests voice services to communicate with PGW-C over S-GW and MME resulting in the establishment of a PDU session. The P-GW supports a non-GBR bearer with QCI flows as 5 for VoLTE sessions. This support allows IMS signaling along with P-CSCF, DNS IPv4, or DNS IPv6 addresses for end users. For mobile-originated (MO) or mobile-terminated (MT) calls, the Application Function (AF) provides policy authorization details to the PCF. The PCF then converts these details to GBR flows and PCC rules and sends them to PGW-C. The PGW-C then converts the GBR-flows to dedicated bearers by establishing the dedicated bearer creation procedure with UE. The PGW-C provisions the GBR with the QCI flow as 1 to UPF. By this provisioning, the UPF supports voice communication between the calling and called devices over IMS network elements.

As per the E-UTRAN Attach procedure, the MME triggers the GTPv2 Create Session Request to PGW-C over S-GW. This request includes the EPS Bearer Identity (EBI) value, ePCO options for P-CSCF and DNS IPv4 or DNS IPv6 containers, PDN-Type, and PAA options for IPv4 or IPv6 allocated address for end users. The P-GW then processes the received Create Session Request and communicates with various SBI interfaces to receive the following information:

- Subscription data from UDM by including PGW-C FQDN in the subscription request.
- Policy information from PCF by sending SM policy create request. Policy information includes details, such as PCC rules and Session-AMBR.
- Online and offline charging information from CHF by sending the charging create data request.

After communication with SBI interfaces, which are based on the local SMF profile configuration, the P-GW sends the GTPv2 Create Session Response to the end user over S-GW and MME. This response includes:

- PAA with IPv4 or IPv6 addresses that PGW-C IPAM module allocates
- ePCO option with P-CSCF
- DNS IPv4 or DNS IPv6 address based on DNN-Profile configuration
- Non-GRB with the QCI flow as 5 for IMS signaling

For an MO or MT call, if the PCF is provisioned for GBR with the QCI flow as 1 for end users, the P-GW converts these GBR flows to the dedicated bearer creation. The GBR flows include the flow information and the PCC rules in the SM Policy Update Notify Request. The dedicated bearer is created by sending GTPv2 Create Bearer Request to UE over S-GW or MME. Another S5-U tunnel is created between S-GW and P-GW to allow GBE flow packets for the voice communication between the calling and called devices.

Call Flows

This section describes the following call flows:

- VoLTE PDU Session Creation Call Flow
- VoLTE Mobile-Originated (MO) Call Creation Call Flow
- VoLTE Mobile-Terminated (MT) Call Creation Call Flow

VoLTE PDU Session Creation Call Flow

To enable the connectivity through a 5G core, the initial attach on the E-UTRAN or EPS deviates from the defined 3GPP procedures in the following ways:

- An SMF+P-GW replaces the P-GW in the procedure.
- The SM Policy Association Establishment procedure replaces the IP-CAN Session Establishment and modification.
- The integrated charging over the NCHF interface with CHF replaces the online and offline charging functionality by using the Gy and Gz interfaces.
- Communication with the User Plane node happens over the N4 interface instead of the Sxb interface.

Note Depending on the mapped PCC rules, the SMF+PGW-C can initiate the dedicated bearer creation.

The following call flow depicts the creation of a VoLTE PDU session.

Figure 124: VoLTE PDU Session Creation Call Flow

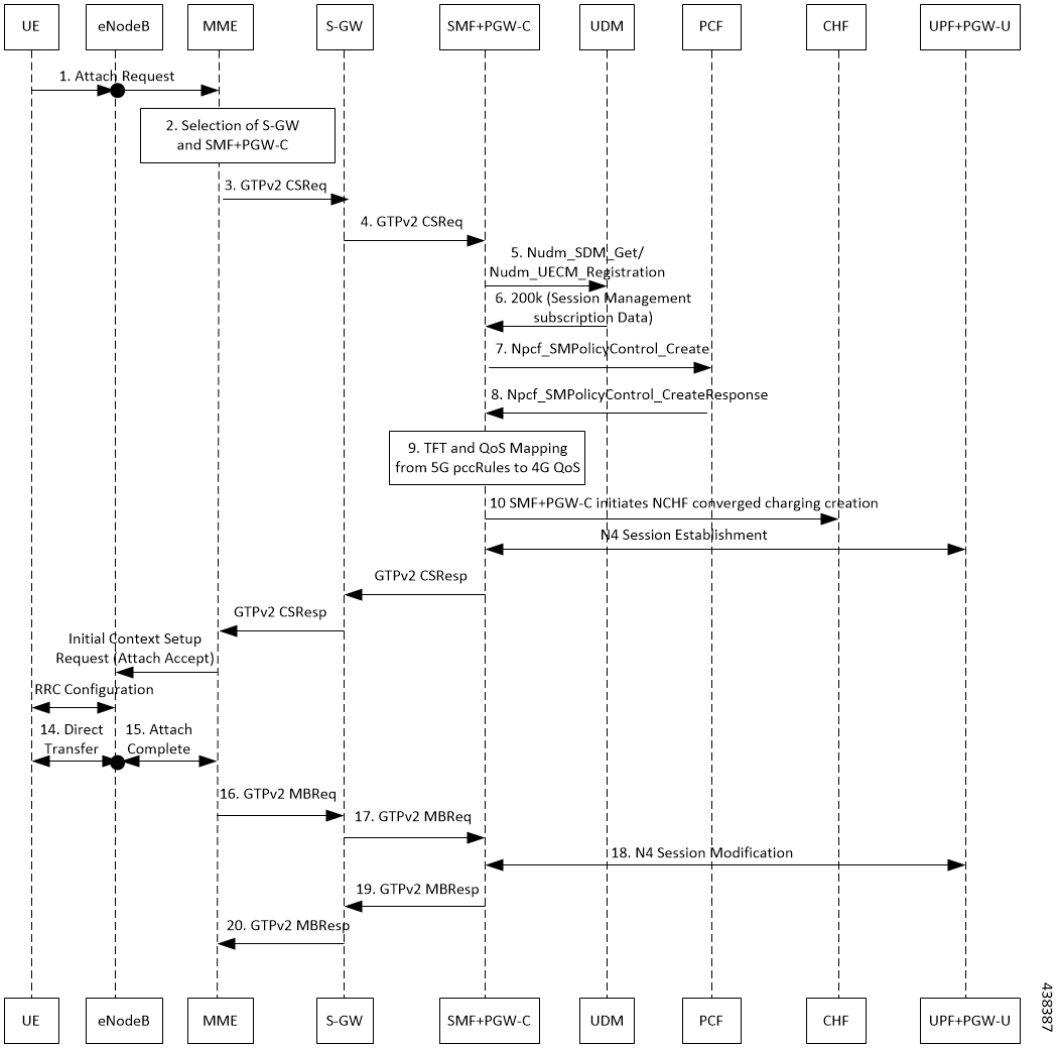


Table 188: VoLTE PDU Session Creation Call Flow Description

Step	Description
1	UE sends the attach request to MME through eNodeB.
2	MME determines if the UE is active and subscribed for the handoff to NR. Then, MME selects a SMF+PGW-C node as the P-GW for the PDU session.
3	MME sends the create session request to the selected S-GW and includes the selected SMF+PGW-C address in the request.
4	S-GW initiates the create session request toward SMF+PGW-C by including the "P-CSCF IPv4 or IPv6 request" container identifier in the extended PCO IE options. SMF+PGW-C extracts and saves the PDU session ID that UE sends in the PCO option. Then, SMF+PGW-C performs a UDM registration and sends both the N11 and S5 or S8 interface ID to UDM. Based on the local configuration or the session management subscription data, which is received from UDM for respective DNN, SMF+PGW-C determines to support "IMS Voice over PS".
5	SMF+PGW-C sends the NPCF SM policy control creation request to PCF to initiate the SM policy association establishment procedure. In this procedure, PGW-C+SMF includes the information elements that are received in the create session request message into the Npcf_SMPolicyControl_Create service. These elements comprise the following information: • SUPI contains the IMSI. • DNN contains the APN. • PEI contains the IMEI-SV. • Session AMBR contains the APN-AMBR. • Default QoS information that contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.
6	PGW-C+SMF receives the PCC rules, PDU session policy information, and 5G QoS information. The PCC rules are mapped into EPS QoS information. The SMF+PGW-C creates TFT from the SDF filters that are received in the PCC rules. Then, SMF+PGW-C associates them with the corresponding default and dedicated bearers.
7	Based on the charging policies received from the PCF, the SMF+PGW-C initiates the NCHF converged charging creation procedure toward CHF. This procedure is based on the charging rules that are received from the PCF.
8	The SMF+PGW-C starts the UPF+PGW-U selection and N4 session establishment procedure. As this session is a 4G session that connects to the SMF+PGW-C, a separate CN tunnel is created for each bearer. Also, the QoS Flow Identifier (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
9	The SMF+PGW-C sends create session response to the S-GW. This response includes the bearer information and the TEID for the default bearer. The SMF+PGW-C also includes the 5G QoS parameters in PCO options 001CH (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime), and 001FH (QoS flow descriptions) to the UE.

Step	Description
10	Based on the charging policies received from PCF, the SMF+PGW-C initiates NCHF converged charging creation procedure toward CHF. This procedure is based on the charging rules that are received from PCF.
11	S-GW sends create session response to MME.
12	MME sends the Initial Context Setup Request to eNodeB with the N1 Attach Accept message.
13	eNodeB and UE perform the RRC configuration.
14	UE sends the direct transfer message to eNodeB.
15	eNodeB sends the attach completion message in the Initial Context Setup Response and the TEID of eNodeB to MME.
16	MME sends a modify bearer request to S-GW with eNodeB TEID.
17	S-GW sends the modify bearer request to SMF+PGW-C with eNodeB TEID.
18	SMF+PGW-C performs the N4 session modification to update the eNodeB TEID on the data path to the UPF+PGW-U.
19	SMF+PGW-C sends the modify bearer response to the S-GW.
20	S-GW sends the modify bearer response to MME.

VoLTE Mobile-Originated (MO) Call Creation Call Flow

This section describes the VoLTE MO call creation call flow.

Figure 125: VoLTE MO Call Creation Call Flow

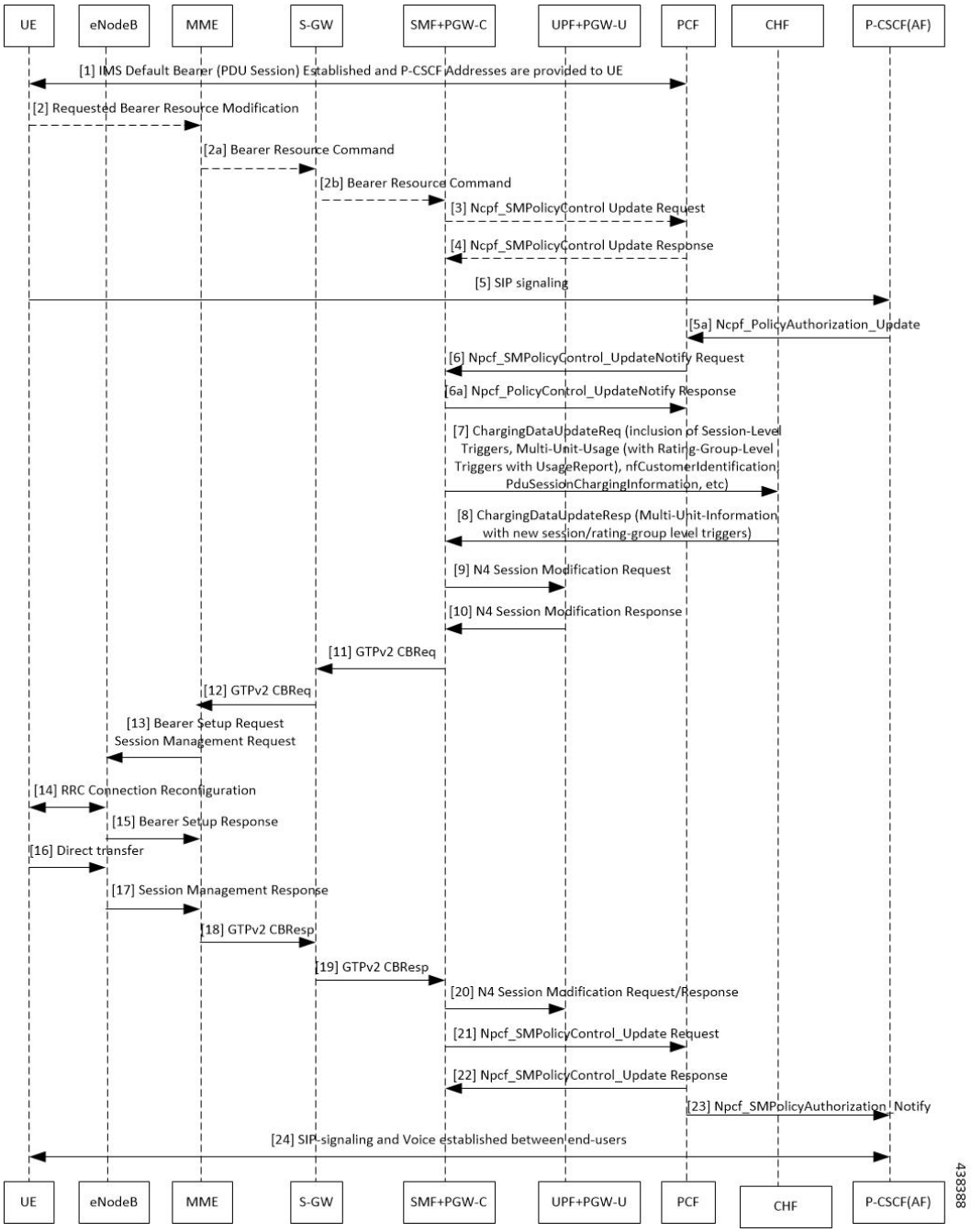


Table 189: VoLTE MO Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	UE sends the requested bearer resource modification information to MME.

Step	Description
2a	MME sends the bearer resource command to S-GW.
2b	S-GW sends the bearer resource command to SMF+PGW-C.
3	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
4	PCF sends the NPCF SM Policy control update response back to SMF+PGW-C.
5	UE initiates SIP signaling toward P-CSCF (AF).
5a	P-CSCF sends NPCF Policy Authorization Update message to PCF through CHF.
6	PCF sends the NPCF SM policy control update notify request to SMF+PGW-C.
6a	SMF+PGW-C sends the NPCF SM Policy control update notify response back to PCF.
7	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
8	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
9	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
10	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
11	SMF+PGW-C sends the GTPv2 create bearer request to S-GW.
12	S-GW sends the GTPv2 create bearer request to MME.
13	MME sends the bearer setup request and session management request to eNodeB.
14	RRC connection reconfiguration starts between UE and eNodeB.
15	The eNodeB sends the bearer setup response to MME.
16	UE initiates a direct transfer toward eNodeB.
17	eNodeB sends the session management response to MME.
18	MME sends the GTPv2 create bearer response to S-GW.
19	S-GW sends the GTPv2 create bearer response to SMF+PGW-C.
20	SMF+PGW-C sends the N4 session modification request or response to UPF+PGW-U.
21	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
22	PCF sends the NPCF SM policy control update response back to SMF+PGW-C.
23	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
24	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

NOTES:

- The PCC rules that the PCF provides are mapped to TFTs for the new dedicated bearer. The associated QoS is mapped to 4G QoS.
- The NCHF Converged Charging Update service procedures replace all the Gy and Gz interface messages.
- The User Plane resources for dedicated bearers are added through the N4 Session Modification procedure towards the UPF. PDRs, QERs, and FARs are added for the SDF filters for the new dedicated bearer.
- SMF+PGW-C saves the EBI for the dedicated bearer that is received in the create bearer response.

VoLTE Mobile-Terminated (MT) Call Creation Call Flow

This section describes the VoLTE MT call creation call flow.

Figure 126: VoLTE MT Call Creation Call Flow

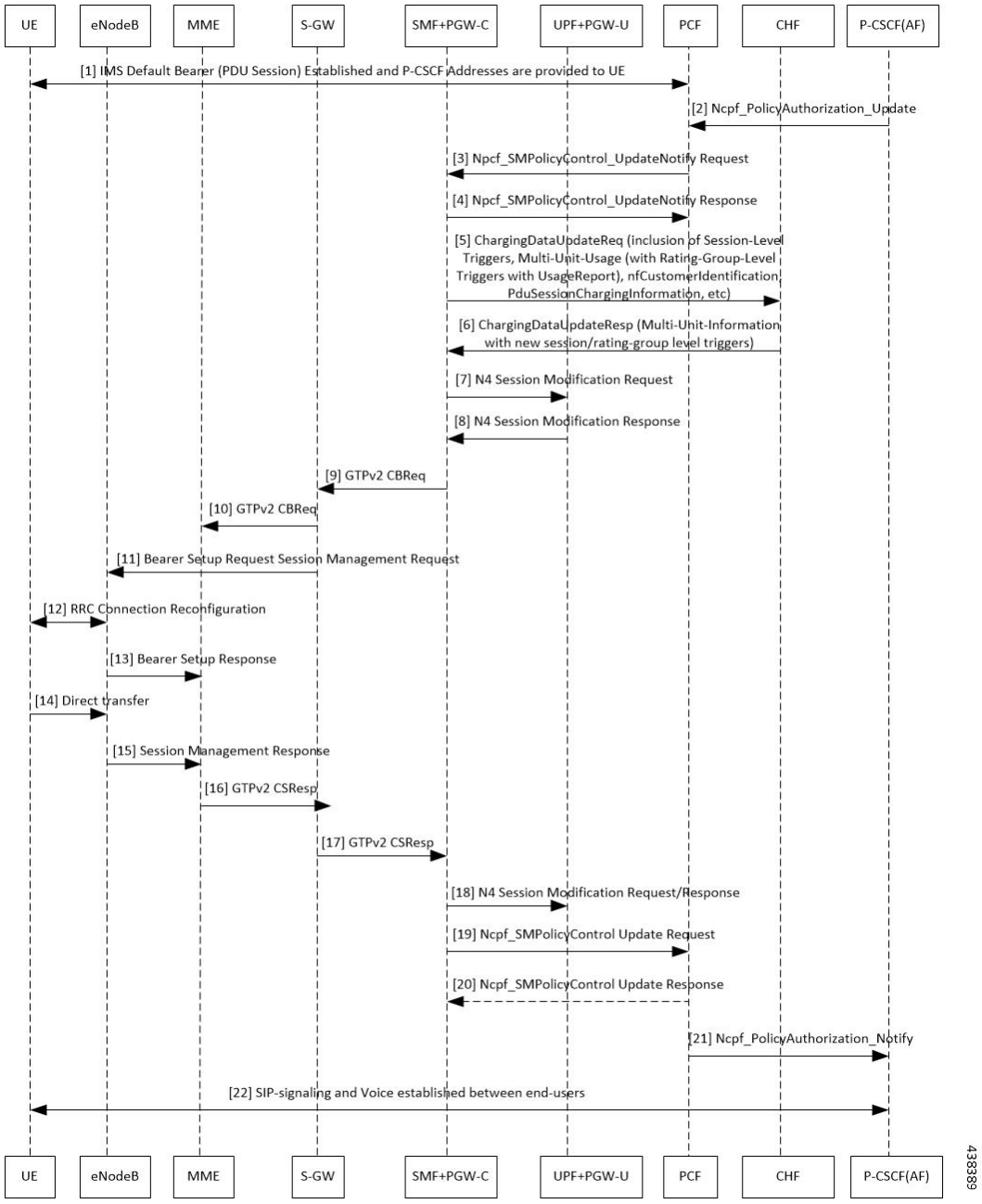


Table 190: VoLTE MT Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	P-CSCF (AF) sends the NPCF policy authorization update to PCF.

Step	Description
3	PCF sends the NPCF SM Policy control update notify request to SMF+PGW-C.
4	SMF+PGW-C sends the NPCF SM Policy control update notify response to PCF.
5	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
6	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
7	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
8	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
9	SMF+PGW-C sends the GTPv2 create bearer request to S-GW.
10	S-GW sends the GTPv2 create bearer request to MME.
11	MME sends the bearer setup request and session management request to eNodeB.
12	RRC connection reconfiguration starts between UE and eNodeB.
13	eNodeB sends the bearer setup response to MME.
14	UE initiates a direct transfer toward eNodeB.
15	eNodeB sends the session management response to MME.
16	MME sends the GTPv2 create bearer response to S-GW.
17	S-GW sends the GTPv2 create bearer response to SMF+PGW-C.
18	SMF+PGW-C sends the N4 session modification request or response to UPF+PGW-U.
19	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
20	PCF sends the NPCF SM policy control update response back to SMF+PGW-C.
21	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
22	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

Standards Compliance

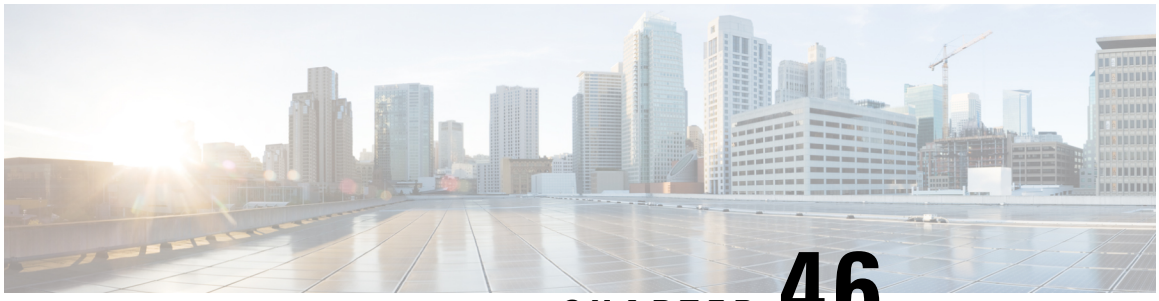
The VoLTE support feature complies with the following standard:

- 3GPP TS 23.502 V15.2.0 (2018-09)

Limitations

The VoLTE support feature has the following limitations:

- The UE-initiated dedicated bearer creation is not supported.
- VoLTE is not integrated with charging.
- PCF-initiated modification is not supported to change the GBR flows and PCC rules. However, the addition and deletion of GBR flows are supported.



CHAPTER 46

VoWiFi Support

Feature Summary and Revision History

Summary Data

Table 191: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 192: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

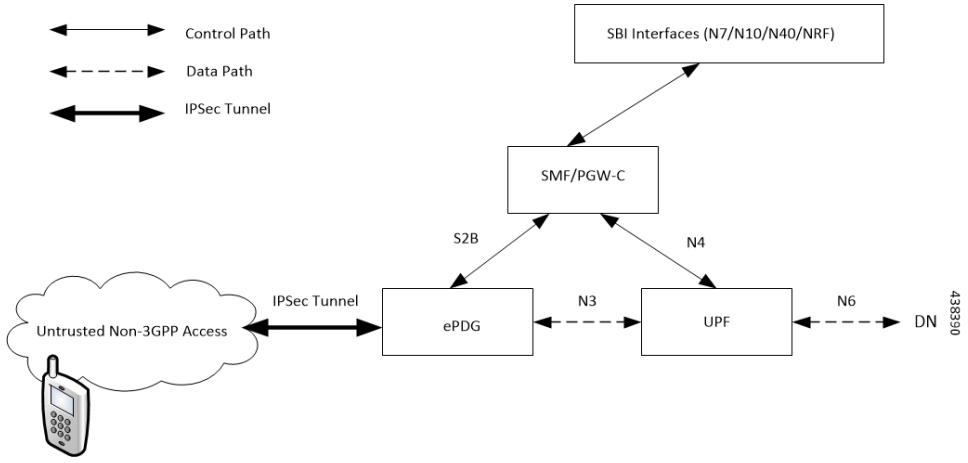
Feature Description

The SMF supports Voice over Wi-Fi (VoWiFi). The VoWiFi technology provides the telephony services using Voice over IP (VoIP) from the mobile devices that are connected across a Wi-Fi network.

Architecture

This section describes the VoWiFi architecture.

Figure 127: VoWiFi Architecture



How it Works

A 5G mobile device connects through an untrusted Wi-Fi network for voice services to establish a PDN connection with PGW-C. This connection is established through Internet Key Exchange Protocol version 2 (IKEv2) protocol between the UE and enhanced Packet Data Gateway (ePDG). The P-GW receives the GTPv2 Create Session Request from an untrusted Wi-Fi ePDG over the S2b interface. The PGW-C then communicates with the SBI interfaces for creating the default and dedicated bearers. The SBI interfaces can be an N7, N10, N40, or an NRF interface.

Call Flows

This section describes the following call flows:

- VoWiFi PDU Session Creation Call Flow
- VoWiFi Mobile-Originated (MO) Call Creation Call Flow
- VoWifi Mobile-Terminated (MT) Call Creation Call Flow

VoWiFi PDU Session Creation Call Flow

To enable connectivity through a 5G core, the initial attach on the ePDG or EPS deviates from the defined 3GPP procedures in the following ways:

- An SMF+P-GW replaces the P-GW in the procedure.
- The SM Policy Association Establishment procedure replaces the IP-CAN Session Establishment and modification.
- The integrated charging over the NCHF interface with CHF replaces the online and offline charging functionality by using the Gy and Gz interfaces.
- Communication with the User Plane node happens over the N4 interface instead of the Sxb interface.

The following call flow depicts the creation of a VoWifi PDU session.

Figure 128: VoWiFi PDU Session Creation Call Flow

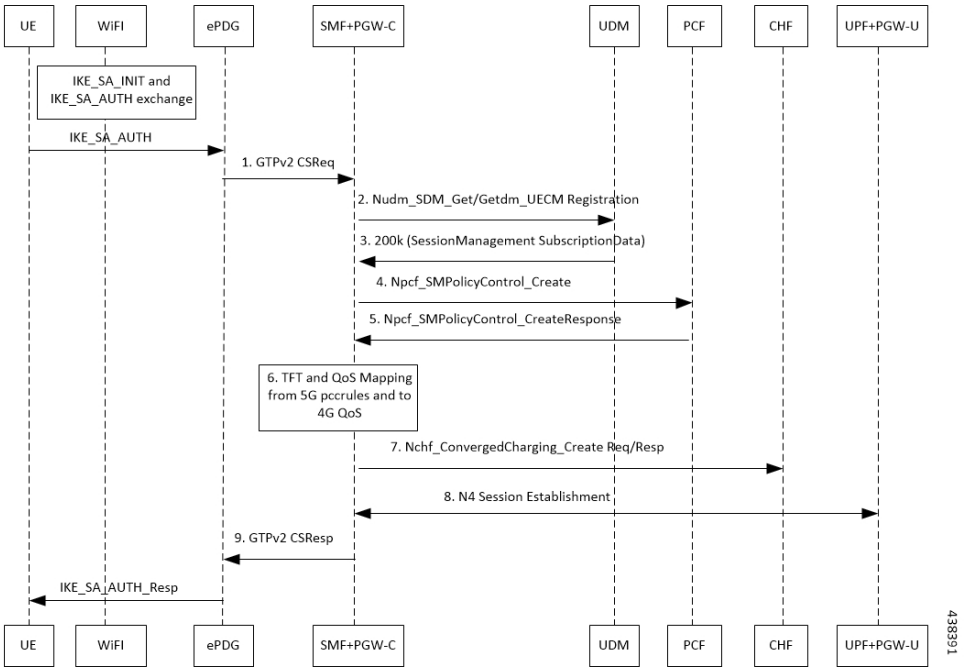


Table 193: VoWiFi PDU Session Creation Call Flow Description

Step	Description
1	The UE initiates the IKE_SA_INIT and IKE_SA_AUTH exchange. The UE then sends the IKE_SA_AUTH exchange message to ePDG to create the IPSec tunnel.
2	The UE sends the IKE_SA_AUTH exchange message to the SMF+PGW-C as a GTP Create Session Request by including the “P-CSCF IPv4 or IPv6 request and DNS IPv4 or IPv6” container identifier in APCO IE Options.
3	The SMF+PGW-C extracts and saves the PDU Session ID that the UE sent in the APCO IE option. The SMF+PGW-C then performs a UDM registration and sends both the N11 and S2b interface IDs to UDM. Based on the local configuration or session management subscription data that is received from UDM for respective DNN, SMF+PGW-C determines to support “IMS Voice over PS”.

Step	Description
4	The SMF+PGW-C sends the NPCF SM Policy Control Creation Request to the PCF to initiate the SM Policy Association Establishment procedure. In this procedure, the PGW-C+SMF includes the information elements that are received in the Create Session Request message into the Npcf_SMPolicyControl_Create service. These elements comprise the following information: • SUPI contains the IMSI. • DNN contains the APN. • PEI contains the IMEI-SV. • Session AMBR contains the APN-AMBR. • Default QoS information that contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.
5	The PGW-C+SMF receives the PCC rules, PDU session policy information, and 5G QoS information. The PCC rules are mapped into EPS QoS information. The SMF+PGW-C creates TFT from the SDF filters that are received in the PCC rules. The SMF+PGW-C then associates them with the corresponding default and dedicated bearers.
6	Based on the charging policies received from the PCF, the SMF+PGW-C initiates Nchf_ConvergedCharging_Create procedure toward CHF. This procedure is based on the charging rules that are received from the PCF.
7	The SMF+PGW-C starts the UPF+PGW-U selection and N4 Session Establishment procedure. As this session is a 4G session that connects to the SMF+PGW-C, a separate CN tunnel is created for each bearer. Also, the QoS Flow Identifier (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
8	Th eSMF+PGW-C sends Create Session Response to the ePDG. This response includes the bearer information and the TEID for the default bearer. The SMF+PGW-C also includes the 5G QoS parameters in APCO options 001CH (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime), and 001FH (QoS flow descriptions) to the UE.
9	The ePDG sends IKE_SA_AUTH Response to the UE. Then, depending on the mapped PCC rules, the SMF+PGW-C initiates the dedicated bearer creation.

VoWiFi Mobile-Originated (MO) Call Creation Call Flow

This section describes the VoWiFi MO call creation call flow.

Figure 129: VoWiFi MO Call Creation Call Flow

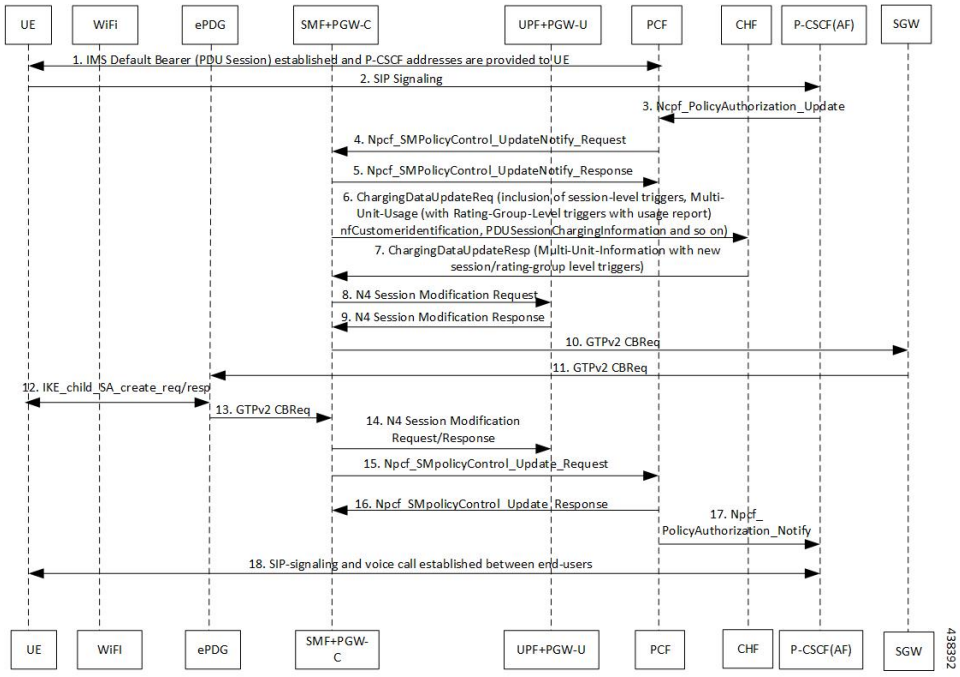


Table 194: VoWiFi MO Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	The UE initiates the SIP signaling toward P-CSCF (AF).
3	The P-CSCF (AF) sends the NPCF Policy Authorization Update message to the PCF.
4	The PCF sends the NPCF SM Policy Control Update Notify Request to the SMF+PGW-C.
5	The SMF+PGW-C sends the NPCF SM Policy Control Update Notify Response back to the PCF.
6	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
7	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
8	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
9	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.

Step	Description
10	The SMF+PGW-C sends the GTPv2 Create Bearer Request to the S-GW.
11	The S-GW sends the GTPv2 Create Bearer Request to the ePDG.
12	IKE_CHILD_SA exchange happens between the UE and ePDG.
13	The ePDG sends the GTPv2 Create Bearer Response back to the SMF+PGW-C.
14	The established N4 session is modified between SMF+PGW-C and UPF+PGW-C.
15	The SMF+PGW-C sends the NPCF SM Policy Control Update Request to the PCF.
16	The PCF sends the NPCF SM Policy Control Update Response back to the SMF+PGW-C.
17	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
18	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

NOTE:

- The PCC rules that the PCF provides are mapped to TFTs for the new dedicated bearer. The associated QoS is mapped to 4G QoS.
- The NCHF Converged Charging Update Service procedures replace all the Gy and Gz interface messages.
- The User Plane resources for dedicated bearers are added through the N4 Session Modification procedure towards the UPF. PDRs, QERs, and FARs are added for the SDF filters for the new dedicated bearer.
- The SMF+PGW-C saves the EBI for the dedicated bearer that is received in the Create Bearer Response.

VoWifi Mobile-Terminated (MT) Call Creation Call Flow

This section describes the Mobile-Terminated (MT) call flow.

Figure 130: VoWifi MT Call Creation Call Flow

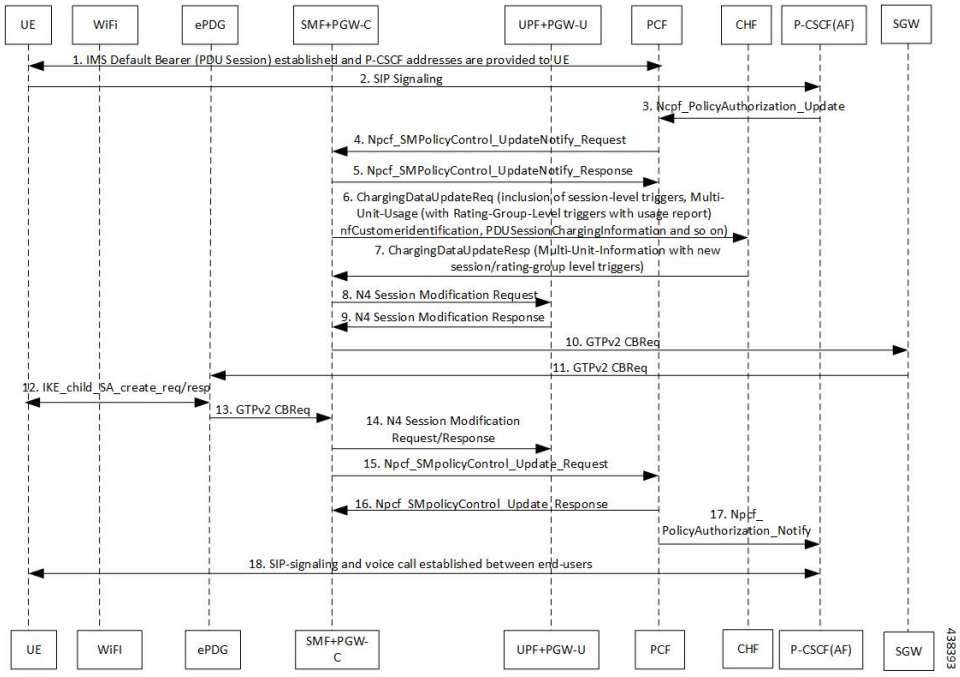


Table 195: VoWifi MT Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	The UE-initiates the SIP signaling towards the P-CSCF (AF).
3	The P-CSCF (AF) sends the NPCF Policy Authorization Update message to the PCF.
4	The PCF sends the NPCF SM Policy Control Update Notify Request to the SMF+PGW-C.
5	The SMF+PGW-C sends the NPCF SM Policy Control Update Notify Response back to the PCF.
6	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
7	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
8	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
9	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.

Step	Description
10	The SMF+PGW-C sends the GTPv2 Create Bearer Request to the S-GW.
11	The S-GW sends the GTPv2 Create Bearer Request to the ePDG.
12	IKE_CHILD_SA exchange happens between the UE and ePDG.
13	The ePDG sends the GTPv2 Create Bearer Response back to the SMF+PGW-C.
14	The established N4 session is modified between SMF+PGW-C and UPF+PGW-C.
15	The SMF+PGW-C sends the NPCF SM Policy Control Update Request to the PCF.
16	The PCF sends the NPCF SM Policy Control Update Response back to the SMF+PGW-C.
17	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
18	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

Standards Compliance

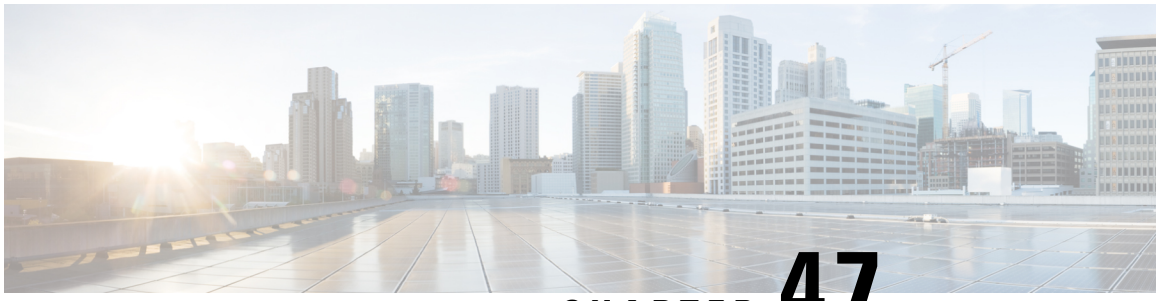
The VoWiFi support feature complies with the following standard:

- 3GPP TS 23.502 V15.2.0 (2018-09)

Limitations

In this release, the VoWiFi support feature has the following limitations:

- UE-initiated Dedicated Bearer Creation is not supported.
- VoWiFi is not integrated with charging.
- PCF-initiated modification is not supported to change the GBR flows and PCC rules. However, the addition and deletion of GBR flows are supported.
- Integration of charging is not supported.



CHAPTER 47

Wi-Fi Handovers

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 196: Revision History

Revision Details	Release
The Wi-Fi to 5GS Handover with EPS Fallback feature is fully qualified in this release.	2020.02.2
The Wi-Fi to 5GS Handover with EPS Fallback feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.1
First introduced.	Pre-2020.02.0

Feature Description

The Cloud Native based SMF+PGW-C product supports the Wi-Fi handover. The cloud-based architecture supports the following Wi-Fi handovers in 5GS or EPS and non-3GPP untrusted access.

- EPC to non-3GPP untrusted Wi-Fi handover
- Non-3GPP untrusted Wi-Fi to EPC handover
- Non-3GPP untrusted Wi-Fi to 5GS handover with EPS fallback
- Non-3GPP untrusted Wi-Fi to 5GS handover
- 5GS to non-3GPP untrusted Wi-Fi handover

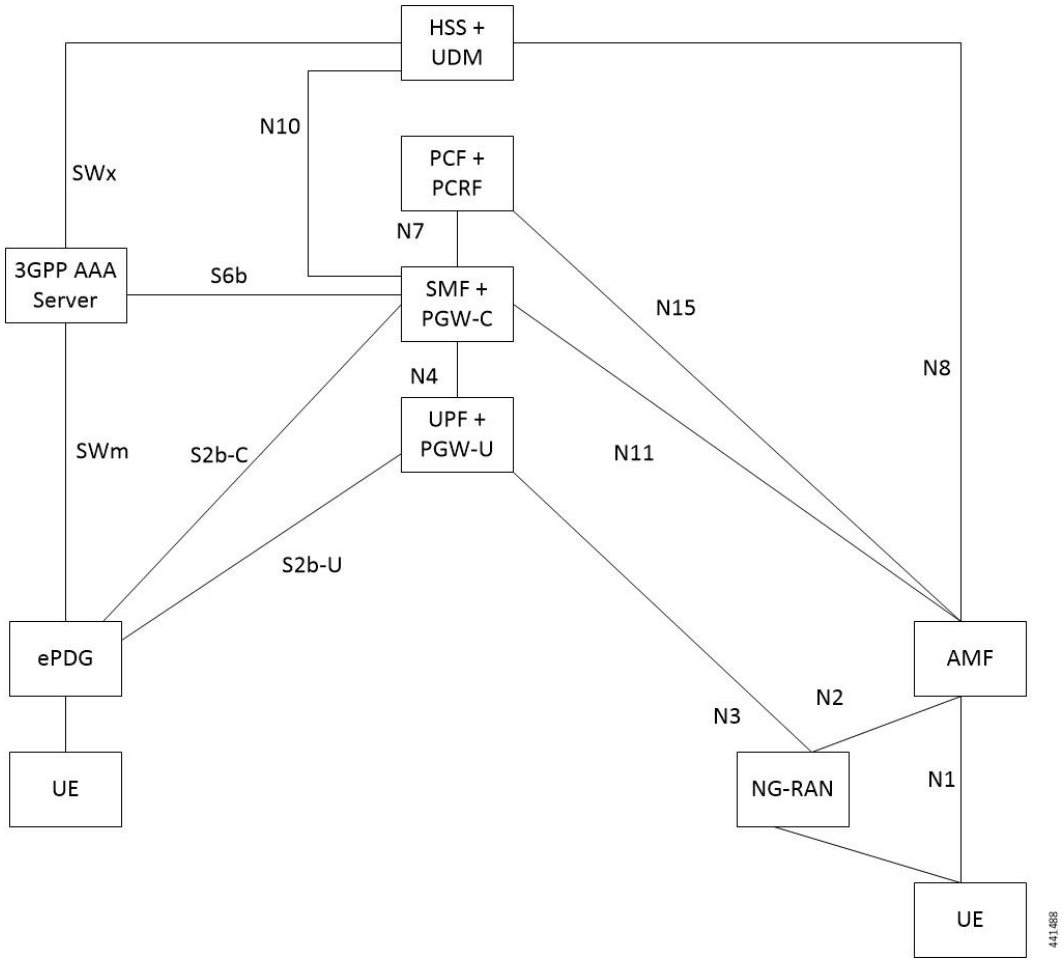
Architecture

The following sections describe the architecture for interworking between the ePDG or EPC and 5GS and the non-roaming architecture within the EPS using S5 and S2b interfaces.

ePDG and 5GS Interworking for Handover

The following figure illustrates the non-roaming architecture for interworking between the ePDG or EPC and 5GS.

Figure 131: Non-Roaming Architecture for Interworking between ePDG or EPC and 5GS



The interworking between the ePDG and 5GS is similar to the interworking between EPC and 5GS without the N26 interface. In this interworking, the IP address preservation occurs on the UEs on inter-system mobility. Saving and fetching PGW-C+SMF and the corresponding APN and DNN information through the HSS+UDM makes interworking possible. In such networks, AMF also supports interworking with UEs without the N26 interface during the initial registration in 5GC. The AMF may support interworking with UEs without N26 in the Attach procedure in 5GS. In case of a non-3GPP untrusted Wi-Fi access, the ePDG does not communicate with the AMF because the N26 interface does not exist.

A 5GS supports network slicing and can interwork with the EPS in its PLMN or in other PLMNs. SMF+PGW-C performs UDM registration for each UE with PGW-C FQDN + NSSAI values. With this registration, the AMF or ePDG identify the PGW-C IP-address from the UDM or HSS as part of the subscription information after the UE authorization is completed.

The mobility between 5GC to EPC does not ensure that all the active PDU sessions can be transferred to the EPC. During PDN connection establishment in the EPC, the UE allocates the PDU session ID and sends it to the PGW-C+SMF through the PCO.

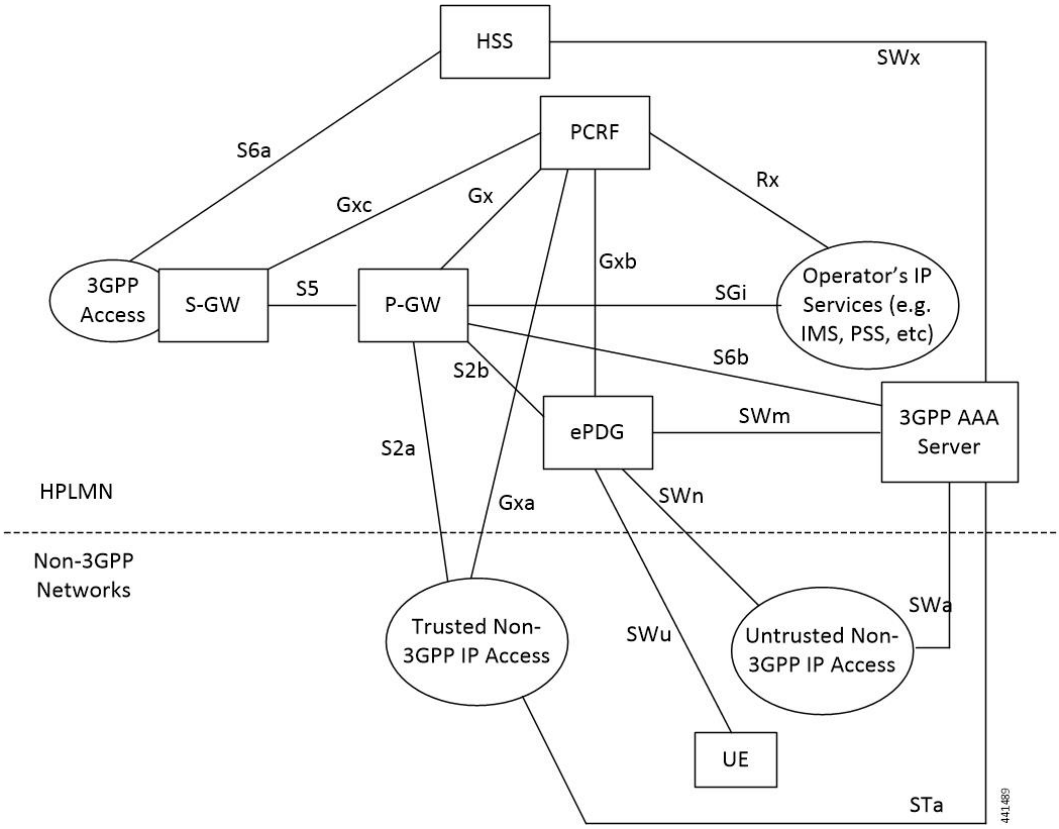
An S-NSSAI that is associated with the PDN connection is determined based on the operator policy by the PGW-C+SMF. For example, the combination of PGW-C+SMF address and APN is sent to the UE in PCO along with a PLMN ID to which the S-NSSAI relates. If the PGW-C+SMF supports multiple S-NSSAI and the APN is valid for multiple S-NSSAIs, the PGW-C+SMF selects only the S-NSSAI that is mapped to the

subscribed S-NSSAIs of the UE. The UE saves this S-NSSAI and the PLMN ID that is associated with the PDN connection. The UE derives the requested NSSAI through the received PLMN ID. The requested NSSAI is included in the NAS registration request message and RRC that is carrying the registration request when the UE registers in 5GC. This scenario is applicable if the UE is non-roaming or the UE has configured NSSAI for the VPLMN in roaming case.

EPS and ePDG Interworking for Handover

The following figure illustrates the non-roaming architecture within the EPS using S5 and S2b interfaces.

Figure 132: Non-Roaming Architecture Within EPS using S5, S2a, and S2b Interfaces



For 3GPP access to non-3GPP access untrusted Wi-Fi handover and for non-3GPP access untrusted Wi-Fi to 3GPP access handover, if a UE has multiple PDN connections to different APNs in the source access and the UE can route different simultaneously active PDN connections through different access networks, the UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them. This transfer can have the restriction that multiple PDN connections to the same APN have one access.

The transfer process can occur in the following scenarios:

- 3GPP access to non-3GPP access untrusted Wi-Fi handover
- Non-3GPP access untrusted Wi-Fi to 3GPP access handover

The UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them if the following conditions are met:

- The UE has multiple PDN connections to different APNs in the source access
- The UE can route different, but simultaneously active, PDN connections through different access networks."

The SMF supports untrusted Wi-Fi access for end-users over S2b interface with ePDG after establishment of IPSec connection between the end-user and ePDG.

For untrusted Wi-Fi to EPC handover, the SMF provides a PGW-C FQDN during UDM registration and fetches the subscription information.

During UE handover, the MME fetches PGW-C FQDN from HSS. After authentication, MME initiates GTPv2 create session request indicating handover. SMF+PGW-C does not perform the UDM registration and subscription procedures while processing handover request. SMF+PGW-C ensures that GTPv2 MB request indicating handover is sent to perform data path switching from untrusted Wi-Fi to EPC.

For EPC to untrusted Wi-Fi handover, for the subscribers who are initially connected to EPC Access, HSS provides SMF+PGW-C FQDN after authentication. When UE performs handover, after authentication HSS provides SMF+PGW-C FQDN. The ePDG initiates GTPv2 create session request indicating handover toward PGW after IPSec tunnel establishment. SMF+PGW-C performs the UDM registration and no subscription procedures exist while processing the handover request.

How it Works

This section describes the Wi-Fi to LTE handover, Wi-Fi handover with EPS fallback, and Wi-Fi to 5GS handover.

EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the EPC to non-3GPP untrusted Wi-Fi handover call flow.

Figure 133: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow

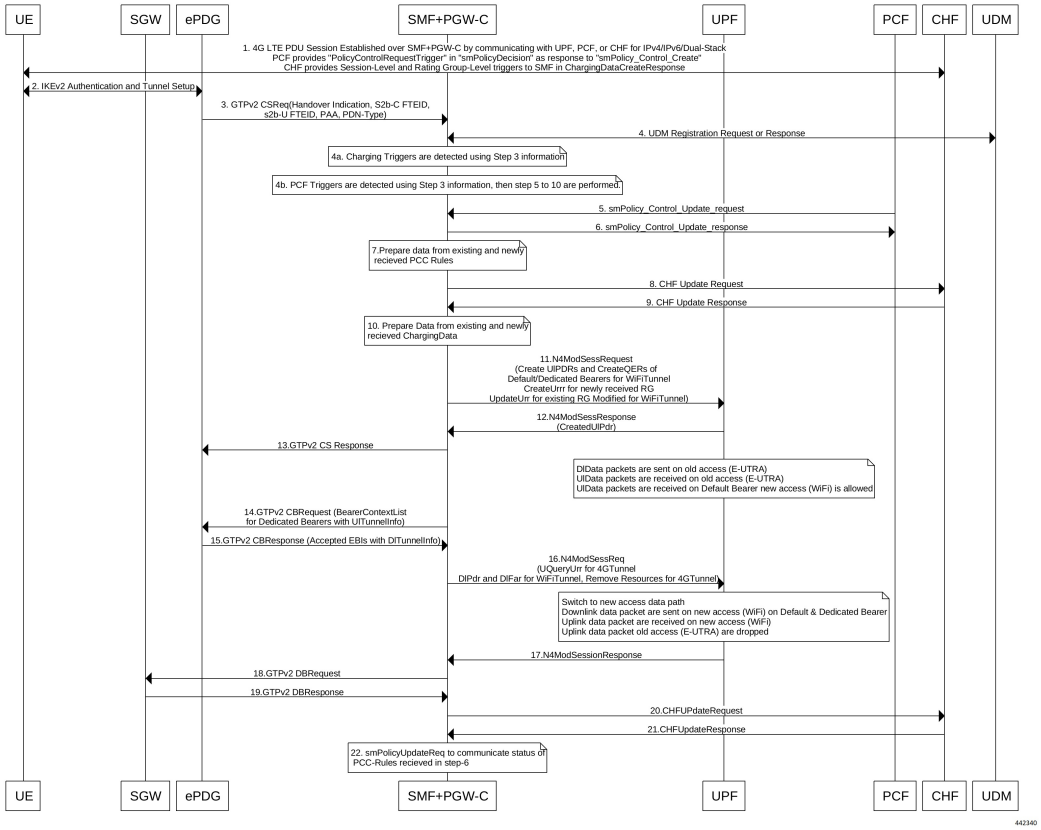


Table 197: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	UE is attached to the 3GPP access network. The 4G LTE PDU session is established over SMF+PGW-C by communicating with UPF, PCF, and CHF for IPv4, IPv6, or dual-stack. PCF sends the Policy Control Request trigger, which is the SM Policy Decision, in response to SM Policy Control Create. CHF provides session-level or rating-group-level triggers to SMF in Charging Data Create response.
2	UE connects to an untrusted non-3GPP access and an ePDG is selected through the ePDG selection process. Then, UE initiates the handover attach procedure, as defined in 3GPP TS 23.402, section 8.6.2.1. After the IKE tunnel is established between UE and ePDG and after UE is authenticated over SWM interface with AAA server, UE initiates IKE_AUH. The IKE_AUH includes cfg_params of the earlier assigned IPv4 or IPv6 addresses in EPC and P-CSCF and DNS options.

Step	Description
3	ePDG sends a Create Session Request to the PDN gateway. This request includes details, such as IMSI, APN, handover indication, RAT type, ePDG TEID of the control plane, ePDG address for the user plane, ePDG TEID of the user plane, EPS bearer identity, and user location. The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and is included in the port analyzer adapter (PAA), then ePDG configures the handover indication in the Create Session Request to allow the PDN gateway to re-allocate the same IP address or the prefix assigned to the UE. This IP address or prefix is assigned while UE is connected to the 3GPP IP access and initiates the policy modification procedure with PCF.
4	SMF performs UDM registration by updating the PGW-C FQDN with UDM. The UDM registration does not happen during the session establishment with EPC.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.
4b	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
6	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.
8	If new PCC rules are received in Step 6 with new Rating Group that requires quota information, SMF sends the Charging Update request to CHF. SMF also includes new access parameters for the PDU session information.
9	CHF sends the Charging Update Response with multi-unit information that contains quota information for the requested rating-group in Step 8 to SMF. CHF may also send the new quota information for the existing rating-group of EPC session.
10	SMF processes the information that is received as Charging Update response from CHF.
11	SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, and update on URR for modified quota information.
12	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, P-GW S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SMF sends the GTPv2 Create Bearer request to S-GW. This request includes information on bearer context list, which contains DL tunnel information to end-user, to be created.

Step	Description
15	S-GW sends the GTPv2 Create Bearer response to SMF. The response includes details on request accepted or request accepted partially and bearer contexts.
16	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to create the DL PDR and DL FAR with DL tunnel information for each bearer, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
17	UPF sends the usage report as N4 Session Modification response to SMF.
18	SMF+PGW-C sends the GTPv2 DB request to S-GW. This request includes EBI or list of EBIs.
19	S-GW sends the GTPv2 DB response to SMF+PGW-C.
20	SMF sends the Charging Update request to CHF. This request includes the PDU session information with the new access params and multi-usage report containing details on the access params and usage report that is received in Step 8
21	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information may include new quota information for the existing rating-groups.
22	SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response. PCF sends the SM policy decision as SM Policy Control Update response. SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to EPC handover call flow.

Figure 134: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow

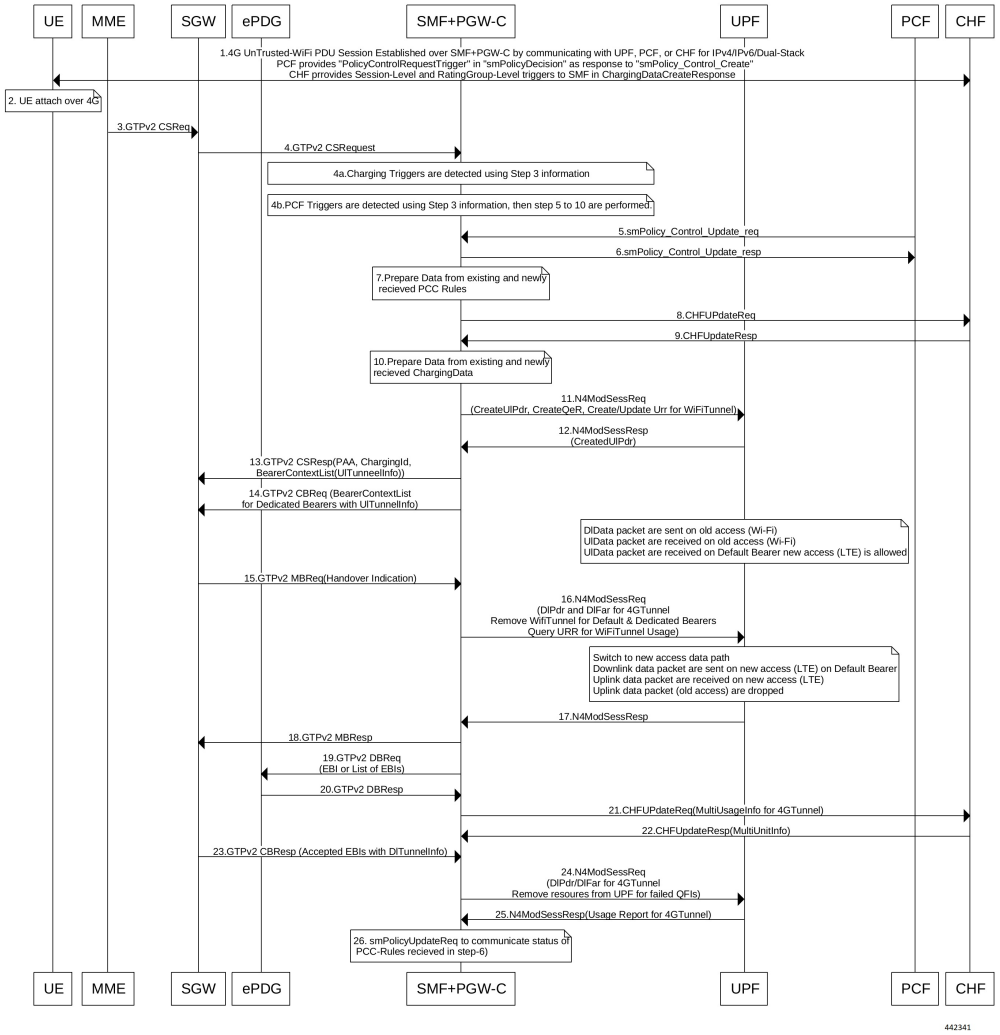


Table 198: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	UE discovers the E-UTRAN access and hands over the sessions from the currently used non-3GPP access system to E-UTRAN. For details on UE discovery of the 3GPP access system, see 3GPP TS 23.401, section 4.8. UE sends an Attach request to MME for the Handover Attach request type. E-UTRAN routes the messages received from UE to MME as defined in 3GPP TS 23.401. UE includes the one of the APNs which are corresponding to the PDN connections in the source non-3GPP access. The APN is provided as defined in 3GPP TS 23.401.

Step	Description
3	MME and HSS perform authentication, which is followed by location update procedure and subscriber data retrieval to receive the APN information. The MME selects an APN, an SGW and PDN gateway as defined in 3GPP TS 23.401. MME sends a Create Session Request message to SGW. This request includes information on IMSI, MME context ID, PDN-GW address, handover indication for the “handover” request type, and APN.
4	SGW sends a Create Session Request, which is handover indication, message to PDN-GW in the HPLMN as described in TS 23.401. As the MME includes the handover indication information in the Create Session Request message, the SGW sends the GTPv2 Create Session Request message to PDN GW. This message includes details on IMSI, APN, handover indication, RAT type, S5-C TEID, S5-U TEID of the user plane, EBI, and user location information. The RAT type indicates the 3GPP IP access E-UTRAN technology type. If the UE supports IP address preservation and is included in PAA, the SGW configures the handover indication in the Creation Session Request. With this configuration, the PDN GW re-allocates the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access. With this configuration, SGW initiates the Policy Modification Procedure to the PCF. As the handover indication is includes, the PDN GW does not switch the tunnel from non-3GPP IP access to 3GPP access system at this point. SMF does not perform the UDM Registration as the registration happens during the Wi-Fi session establishment.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.
4b	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
6	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.
8	If SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request, with the new rating-group having quota information, to CHF. This request includes the PDU session information with the new access params.
9	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the rating-group and the existing rating-group of EPC session, if any.
10	SMF prepares the charging data of the received Charging Update Response that CHF sent.

Step	Description
11	SMF sends the N4 Session Modification Request to UPF. This request includes the details on creation of UL and DL PDR, creation of QER, creation of URR for received new rating-group quota information, updated URR for modified quota information, and creation of FAR.
12	UPF sends the UL tunnel information in the created PDR as N4 Session Modification response to SMF.
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, P-GW S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SGW sends the Modification Bearer request with handover indication to PGW for data path switching from Wi-Fi tunnel to 4G tunnel.
15	PGW sends the N4 Session Modification request to delete the Wi-Fi tunnel and to configure DL tunnel information that is received in GTPv2 Create Session request for 4G tunnel in Step 4.
16	UPF sends the N4 Session Modification response to SMF.
17	SMF sends the GTPv2 Create Session request, which includes the bearer context list, to SGW. This list includes the DL Tunnel information for the end-user.
18	SGW sends the GTPv2 Create Session response to SMF. This response includes details on request accepted or request accepted partially and bearer contexts.
19	ePDG sends the GTPv2 Create Bearer resp (accepted EBIs with DL tunnel info to SMF
20	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to update the DL FAR with the DL tunnel information, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
21	UPF sends the N4 Session Modification Response with usage report to SMF.
22	SMF sends the Charging Update request to CHF. This request includes the PDU session information with new access params and multi-usage report consisting of access-params and usage report that is received in Step 8.
23	CHF sends the Charging Update Response with multi-unit information that contains quota information for the existing rating-groups to SMF.
24	SMF+PGW-C initiates the GTPv2 DB Request toward SGW by including EBI or EBI list.
25	SGW sends the GTPv2 DB Response toward SMF+PGW-C.

Step	Description
26	SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response. PCF sends the SM policy decision as SM Policy Control Update response. SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to 5GS handover call flow.

Figure 135: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow

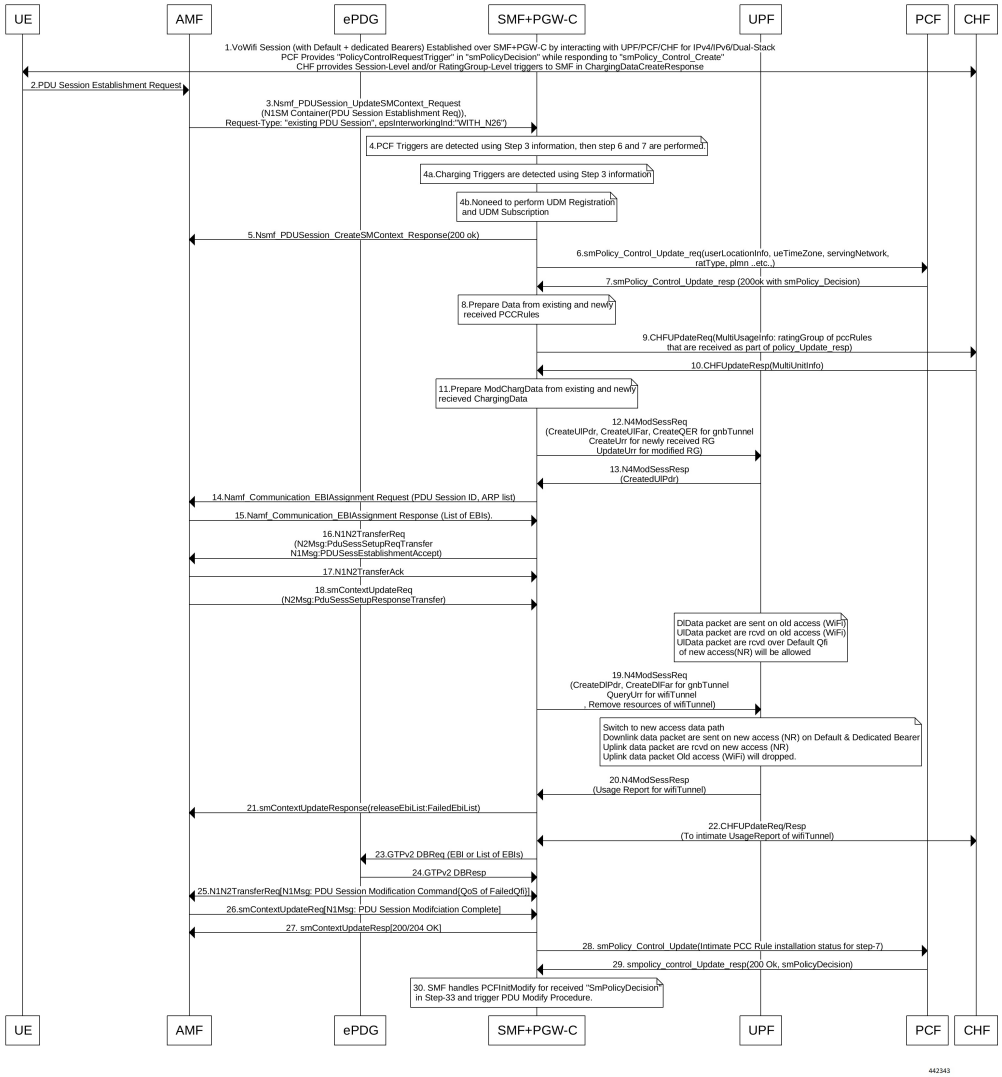


Table 199: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	UE sends the PDU Session Establishment request through 3GPP access to AMF. This request includes details on PDU session ID, requested PDU session type, requested SSC mode, 5GSM capability PCO, SM PDU DN request container, number of packet filters, and an optional requested always-on PDU session. The request type with an existing PDU session indicates switching between 3GPP access and non-3GPP access or to a PDU session handover from an existing PDN connection in EPC.
3	If the request type is “Existing PDU Session”, the AMF selects the SMF based on SMF-ID that is received from UDM. For this request type, if AMF does not identify the PDU Session ID or the subscription context that the AMF received from UDM during the Registration or if the subscription profile update notification procedure contains no SMF ID corresponding to the PDU Session ID, an error occurs. Then, AMF updates the Access Type stored for the PDU session. If the request type with an existing PDU session refers to a PDU session that moved between 3GPP access and non-3GPP access and if the S-NSSAI of the PDU session is available in the Allowed NSSAI of the target access type, the PDU Session Establishment procedure is performed when the SMF ID corresponding to the PDU Session ID and the AMF are part of the same PLMN. AMF sends the NSMF PDU Session Create SM Context Request with the request type “Existing PDU Session” to SMF. This request includes information on SUPI, DNN, S-NSSAIs, PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container including the PDU Session Establishment Request, User location information, Access Type, PEI, GPSI, Subscription For PDU Session Status Notification, DNN Selection Mode. SMF analyzes the existing PDU session from the PDU Session Establishment request using SUPI+PDU-Session-ID. SMF also compare the IPv4 or IPv6 addresses of the received UE against the retrieved PDU session IPv4 or IPv6 addresses. SMF reject the request if the session is not retrieved or IPv4 or IPv6 addresses do not match.
4	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the earlier communication with PCF during Wi-Fi session.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during Wi-Fi session.
4b	SMF does not perform the UDM registration as happens during Wi-Fi Session Establishment.
5	SMF sends the NSMF PDU Session Create SM Context response to AMF. This response includes the cause, SM Context ID or N1 SM container with PDU session rejection cause.

Step	Description
6	Based on the detected armed Policy Control Triggers that are received in Step 4a, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
7	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.
8	Based on the information received in Step 7 and existing policy data of Wi-Fi session, SMF prepares the information.
9	If SMF receives new PCC rules in Step 7, the SMF sends the Charging Update request to CHF with new rating-group for quota information. This request includes the PDU session information with the new access params.
10	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes quota information for the rating-groups received in Step 9 and for the existing rating-group of Wi-Fi session.
11	SMF processes the data that is received Charging Update response from CHF.
12	SMF sends the N4 session modification request to UPF for gnb tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, update on URR for modified quota information, and creation of FAR.
13	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
14	SMF sends the EBI assignment request to AMF. This request includes the ARP list for the PDU session ID.
15	AMF sends the list of EBIs as response to SMF.
16	SMF sends the N1 N2 Transfer Request toward AMF. This request includes the N2 message as “PDU Session Resource Setup Request Transfer” with supported QFI list and UL Tunnel Information of gnb Tunnel. This request also includes the N1 message as “PDU Session Establishment Accept” with authorized QoS rule, authorized QoS flow description, EPCO, PDN addresses, and session AMBR values.
17	AMF sends the N1 N2 Transfer acknowledgement to SMF.
18	AMF sends the SM Context Update request to SMF with “PDU Session Resource Setup Response Transfer” containing the failed QFI list and the DL tunnel information.
19	SMF sends the N4 session modification request to UPF for the gnb tunnel resources. This request is to create the DL PDR, to create DL FAR with DL tunnel information, include details on RAT-change and delete resources for Wi-Fi tunnel. SMF also deletes the N4 resources of gnb tunnel for received failed QFI list.
20	UPF sends the N4 Session Modification Response with the usage report to SMF.
21	SMF sends the SM Context Update response to AMF.

Step	Description
22	SMF sends the Charging Update request to PCF. This request includes the PDU session information with new access params and multi-usage report with old access-params and usage report that is received in Step 18. SMF receives the Charging Update response that includes new quota information for existing rating-groups.
23	SMF+PGW-C initiates the GTPv2 DB request, which includes EBIs, to ePDG.
24	ePDG sends the GTPv2 DB response to SMF+PGW-C.
25	SMF receives the SM Context Update request with N1 message for PDU session modification completion from AMF.
26	SMF sends 200/204 OK as SM Context Update response to AMF.
27	SMF sends the SM policy decision as SM Policy Control Update response to AMF.
28	SMF sends the SM Policy Control Update request to PCF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of N2 message.
29	PCF sends the SM policy decision as SM Policy Control Update response to SMF.
30	SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the 5GS to non-3GPP untrusted Wi-Fi handover call flow.

Figure 136: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow

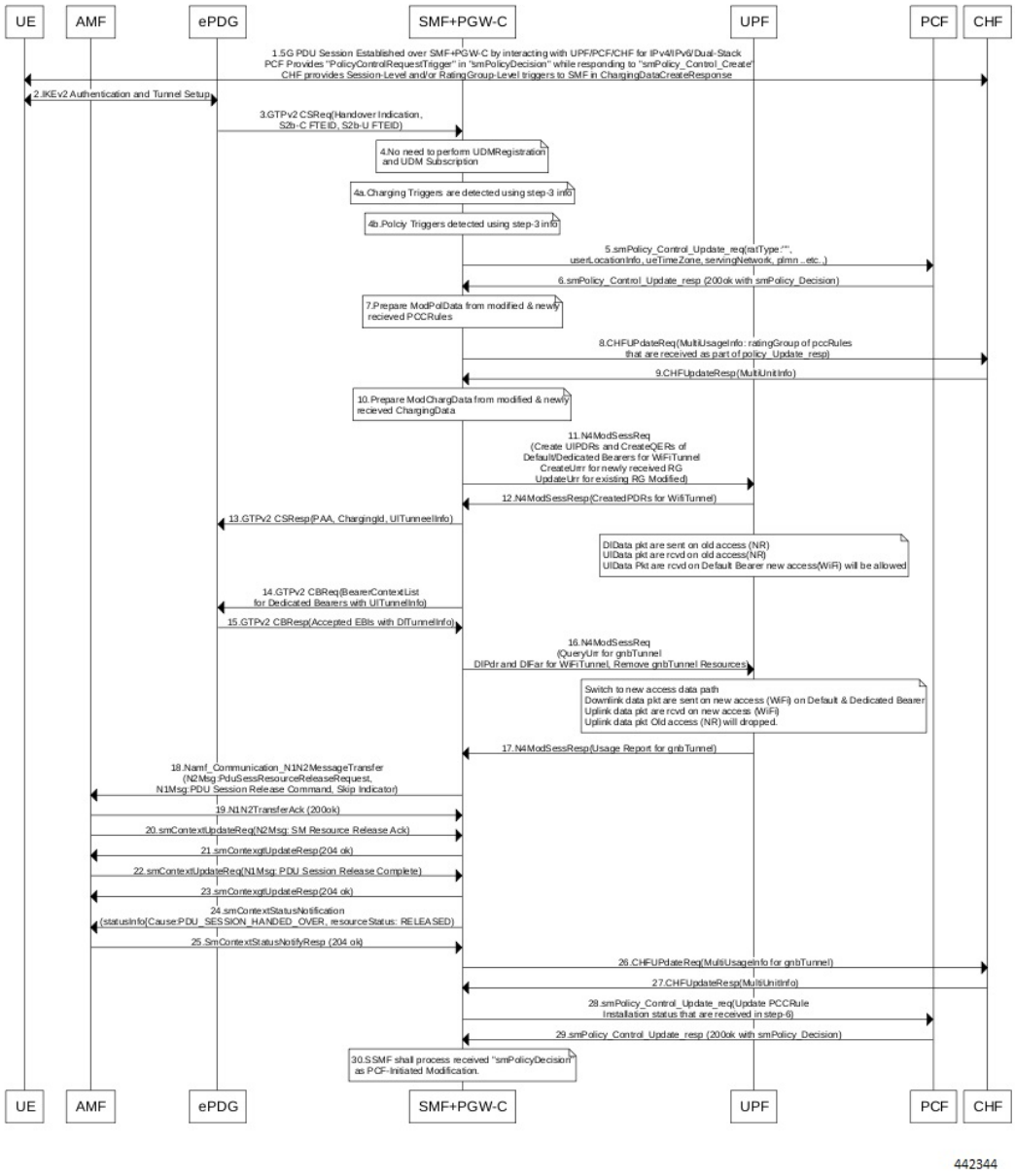


Table 200: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	The UE and the SMF or the UPF interact through the NG-RAN to establish one or more PDU sessions.

Step	Description
2	The UE connects to an untrusted non-3GPP access and selects an ePDG. Then, the UE initiates the handover attach procedure, as defined in 3GPP TS 23.402, section 8.6.2.1. After establishing the IKE tunnel between the UE and the ePDG, and authenticating the UE over SWm interface with the AAA server, the UE initiates IKE_AUH. The IKE_AUH includes cfg_params of the earlier assigned IPv4 or IPv6 addresses in 5GS and P-CSCF and DNS options.
3	The ePDG sends a Create Session request to the P-GW. This request includes the following details: • IMSI • APN • handover indication • RAT type • ePDG TEID of the control plane • ePDG address for the user plane • ePDG TEID of the user plane • EPS bearer identity • user location The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and includes it in the port analyzer adapter (PAA), then the ePDG configures the handover indication in the Create Session request. This configuration allows the P-GW to reallocate the same IP address or the prefix assigned to the UE. The IP address or prefix assignment occurs while the UE is connected to the 3GPP IP access. The policy modification procedure begins with the PCF.
4	The SMF does not perform the UDM registration as it has already been registered with UDM during the 5GS session establishment.
4a	The SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during the Wi-Fi session.
4b	The SMF detects the policy triggers with the information available in Step 3 against the requested policy control triggers that are received while communicating with PCF during the Wi-Fi session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, the SMF sends the SM Policy Control Update request with the detected access parameters to the PCF.
6	The PCF sends the SM policy decision in the SM Policy Control Update response by including new or updated PCC rules.
7	Based on the information received in Step 6 and the existing policy data of 5GS session, the SMF prepares the “ModPolData” information.

Step	Description
8	If the SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request to the CHF with new rating-group for quota information. This request includes the PDU session information with the new access parameters.
9	The CHF sends the multi-unit information as Charging Update response to the SMF. The multi-unit information includes quota information for the rating-groups received in Step 8 and for the existing rating-group of 5GS session.
10	The SMF processes the ModChargingData in the Charging Update response received from the CHF.
11	The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnels. This request includes details on creation of uplink FAR, creation of QER, creation of URR for the received new rating-group quota information, and update on URR for the modified quota information.
12	The UPF sends the N4 session modification response to the SMF with the UL tunnel information in the created PDR.
13	The SMF sends the GTPv2 Create Session response to the S-GW. The response includes details on accepted request or partially accepted request, P-GW S2b F-TEID, PAA, APN-AMBR, creation of bearer context, charging gateway address, and APCO.
14	The SMF sends the GTPv2 Create Bearer request to the S-GW. This request includes information on bearer context list, which contains UL tunnel information for each dedicated bearer to end-user.
15	The S-GW sends the GTPv2 Create Bearer response to the SMF. The response includes details on accepted request or partially accepted request and bearer contexts.
16	The SMF processes the Create Bearer response and derives the DL tunnel information for the established bearer and the failed EBI list, if any. The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnel. This request is to create DL PDR and DL FAR with the DL tunnel information or list of charging description IDs for the detected charging triggers. The SMF deletes the gnb tunnel resources and the N4 resources of the Wi-Fi tunnel for the failed bearer context list.
17	The UPF sends the usage report in the N4 Session Modification response to the SMF.
18	The SMF initiates the NAMF communication N1 N2 message transfer, to the S-GW. This transfer message includes the PDU Session Resource Release Request N2 message.
19	The AMF sends N1 N2 Transfer Acknowledgement to the SMF.
20	The AMF sends the SM Context Update request to the SMF. This request includes the SM Resource Release Acknowledgement N2 message.
21	The SMF sends the 200/204 OK as SM Context Update response to the AMF.
22	The AMF sends the SM Context Update request to the SMF. This request includes the PDU Session Release Complete N1 message.

Step	Description
23	The SMF sends the 200/204 OK as SM Context Update response to the AMF.
24	If the SMF supports the June 2019 compliance version of 3GPP specification 23.502, the SMF indicates the release details to the AMF. The SMF achieves this functionality by sending the SM Context Status Notification message (statusInfo {Cause: PDU_SESSION_HANDED_OVER, resourceStatus: RELEASED). The SMF sends this notification after a successful handover of 5GS to Non-3GPP Untrusted WiFi session. The SMF processes the message as per the compliance profile configured for the corresponding service. For information on the compliance profile configuration, see the Configuring Compliance Profile, on page 662 section. **Important** If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.
25	The AMF sends the 204 OK as SM Context Status Notify response to the SMF. **Important** If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.
26	The SMF sends the Charging Update request to the CHF. This request includes the PDU session information with the new access parameters and multi-usage report containing details on the old access parameters and the usage report that is received in Step 17.
27	The CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the existing rating-groups.
28	The SMF sends the SM Policy Control Update to PCF. This update includes the new access parameters and rule report for failed QFI list that are received from the AMF as part of Create Bearer response.
29	The PCF sends the SM policy decision through the SM Policy Control Update response to the SMF.
30	The SMF processes the SM policy decision and handles it as PCF-initiated modification procedure as defined in 3GPP TS 23.502, section 4.3.3.2.

Standards Compliance

The Wi-Fi handovers feature complies with the following standards:

- 3GPP TS 23.502 V15.2.0 (2018-09)
- 3GPP TS 23.402 V15.3.0 (2018-03)
- 3GPP TS 29.214 V15.5.0 (2018-03)

Configuring Compliance Profile

The SMF provides the compliance profile support for the 3GPP specification 23.502 through the CLI configuration. This compliance profile is in use during the 5GS to non-3GPP untrusted WiFi handover procedure.

Use the following configuration to configure the SMF in compliance with the 3GPP specification.

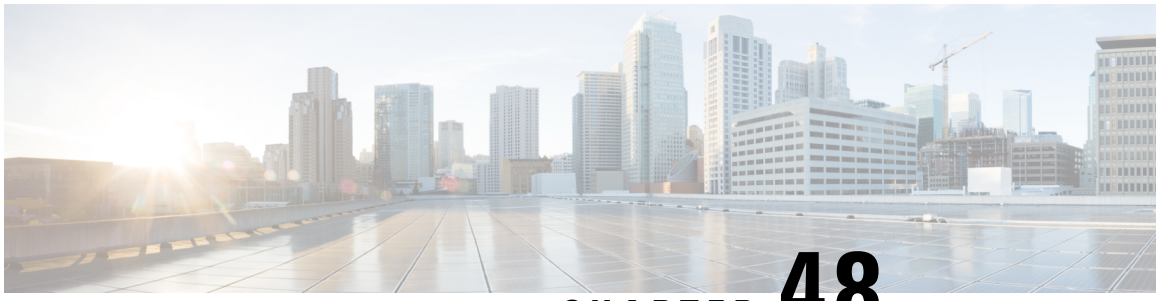
```
configure
   profile compliance profile_name
      service threegpp23502 version spec spec_version full version_format
uri_version uri_version
         range
         !
         !
```

NOTES:

- **full**: Specifies the full version in the format — <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]
- **spec**: Specifies the 3GPP specification version number. It can be one of the following values:
  - 15.4.0
  - 15.6.0

  To support 3GPP December 2018 specification compliance, configure the specification version as 15.4.0. The default version is 15.4.0.

  To support 3GPP June 2019 specification compliance, configure the specification version as 15.6.0.
- **uri**: Specifies the URI version in the format — "v" concatenated with a number. It can be both v1 and v2, or either v1 or v2.



CHAPTER 48

Wireless Priority Services

Feature Summary and Revision History

Summary Data

Table 201: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 202: Revision History

Revision Details	Release
First introduced. This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.0

Feature Description

The Wireless Priority Services (WPS) feature is supported on the SMF+PGW-C over 5GC. The SMF+PGW-C validates prioritization of WPS services for Session Creation/Modification and various handover scenarios. It also evaluates the WPS services for Paging-Policy Differentiation for Network Triggered Service Request procedures.

Use Cases

The WPS feature implements the 3GPP recommendations for wireless priority support for the following use cases in 5GS and EPS. The use cases are defined as per 3GPP TS 23.501 (sections 5.16.3, 5.16.4, 5.16.5, 5.16.6, 5.19, and 5.21).

WPS supports the following use cases:

- Multimedia Priority Services , on page 664
- Mission Critical Services, on page 667
- Expanded Prioritization for VoLTE/VoNR/Emergency Calls, on page 668
- DSCP Marking for N3/S5-U/S2-B over PFCP, on page 668

Multimedia Priority Services

The Multimedia Priority Service (MPS) allows priority access to system resources to Service Users, creating the ability to deliver or complete sessions of a high priority nature. Service Users are government-authorized personnel, emergency management officials and/or other authorized users. MPS supports priority sessions on an "end-to-end" priority basis. MPS includes signalling priority and media priority.

MPS provides the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions.

All MPS-subscribed UEs get priority for QoS Flows (for example, used for IMS signalling) when established to the DN that is configured to have priority for a given Service User by setting MPS-appropriate values in the QoS profile in the UDM. Service Users are treated as On Demand MPS subscribers and not On Demand MPS subscribers, based on regional/national regulatory requirements. On Demand service is based on Service User invocation/revocation explicitly and applied to the media QoS Flows being established. Not On Demand MPS service does not require invocation and provides priority treatment for all QoS Flows only to the DN that is configured to have priority for a given Service User after attachment to the 5G network.

Priority treatment for MPS includes priority message handling for Mobility Management procedures. Priority treatment for MPS session requires appropriate ARP and 5QI setting for QoS Flows according to the operator's policy.

MPS priority mechanisms can be classified as subscription-related and invocation-related. Subscription related mechanisms are divided into - always applied and conditionally applied. Invocation-related mechanisms are divided into - for mobile originated SIP call/sessions, for mobile terminated SIP call/sessions and for Priority PDU connectivity services.

Subscription-related mechanisms that are conditionally applied include:

UDM: One or more ARP priority levels are assigned for prioritized or critical services. The ARP of the prioritized QoS Flows for each DN is set to an appropriate ARP priority level.

PCF: The "IMS Signalling Priority" information is set for the subscriber in the UDM, and the PCF modifies the ARP of the QoS Flow used for IMS signalling.

On-Demand MPS Service

The invocation-related priority mechanisms for prioritized services are based on interaction with an Application Server and between the Application Server and the PCF over Rx/N5 interface (as described in TS 23.228 clause 5.21 in the case of MPS using IMS).

Invocation-related mechanisms for Mobile Originations (for example, via SIP/IMS) are explained below:

- PCF:
  - When an indication for a session arrives over the Rx/N5 interface and the UE does not have priority for the signaling QoS Flow, the PCF derives the ARP and 5QI parameters plus associated QoS characteristics as appropriate, as per the Service Provider policy (specified in clause 6.1.3.11 of TS 23.503).
  - For MPS sessions, when establishing or modifying a QoS Flow as part of the session origination procedure, the PCF selects the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to provide priority treatment to the QoS Flows.
  - When all active sessions to a particular DN are released and the UE is not configured for priority treatment to that particular PDU session, the PCF downgrades the IMS Signaling QoS Flows from appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to those entitled by the UE based on subscription.

Invocation-related mechanisms for Mobile Terminations (for example, via SIP/IMS) are explained below:

- PCF: When an indication for a session arrives over the Rx/N5 interface, the mechanisms as described above for Mobile Originations are applied.
- UPF: If an IP packet arrives at the UPF for a UE that is CM-IDLE, the UPF sends a "Data Notification" including the information to identify the QoS Flow for the DL data packet to the SMF (specified in clause 4.2.3.3 of TS 23.502).
- SMF: If a "Data Notification" message arrives at the SMF for a QoS Flow associated with an ARP priority level value for priority use, delivery of priority indication during the Paging procedure is provided by inclusion of the ARP in the N11 interface "N1N2MessageTransfer" message (specified in clause 4.2.3.3 of TS 23.502).
- AMF: If an "N1N2MessageTransfer" message arrives at the AMF containing an ARP priority level value for priority use, the AMF handles the request with priority and includes the "Paging Priority" IE in the N2 "Paging" message set to a value assigned to indicate that there is an IP packet at the UPF entitled to priority treatment (specified in clause 4.2.3.3 of TS 23.502).
- SMF: For a UE that is not configured for priority treatment, upon receiving the "N7 Session Management Policy Modification" message from the PCF with an ARP priority level for priority use, the SMF sends an "N1N2MessageTransfer" to update the ARP for the Signaling QoS Flows (specified in clause 4.3.3.2 of TS 23.502).
- AMF: Upon receiving the "N1N2MessageTransfer" message from the SMF with an ARP priority level for priority use, the AMF updates the ARP for the Signaling QoS Flows (specified in clause 4.3.3.2 of TS 23.502).

- (R)AN: Inclusion of the "Paging Priority" in the N2 "Paging" message triggers priority handling of paging in times of congestion at the (R)AN (specified in clause 4.2.3.3 of TS 23.502).

Invocation-related mechanisms for the Priority PDU connectivity services:

- PCF:
  - If the state of the Priority PDU connectivity services is modified from disabled to enabled, the QoS Flows controlled by the Priority PDU connectivity services are established/modified to have the service appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, using the PDU Session Modification procedure (specified in clause 4.3.3 of TS 23.502).
  - If the state of Priority PDU connectivity services is modified from enabled to disabled, the QoS Flows controlled by the Priority PDU connectivity services are modified from service appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to those entitled by the UE as per subscription, using the PDU Session Modification procedure (specified in clause 4.3.3 of TS 23.502).

Message-Priority Indication over GTP-C

An overloaded node performs message prioritization when handling incoming messages during an overloaded condition based on the relative GTP-C message priority signaled in the GTP-C header.

When message throttling is performed:

- GTP requests related to priority traffic (eMPS as described in 3GPP TS 22.153) and emergency have the highest priority. Depending on regional/national requirements and network operator policy, these GTP requests are the last to be throttled when applying traffic reduction. The priority traffic is exempted from throttling due to GTP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.
- For other types of sessions, message throttling considers the relative priority of the messages so that low priority messages are considered for throttling before the other messages. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent (as specified in clause 12.3.9.3.2) or derived from the session parameters such as APN and ARP.

The high priority messages are given lower preference to throttle and low priority messages are given higher preference to throttle. An overloaded node also applies these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of the self-protection mechanism.

A sending GTP-C entity determines the relative message priority to signal in the message according to either procedure based or session parameters. If the message affects multiple bearers (for example, Modify Bearer Request), the relative message priority considers the highest priority ARP among all the bearers.

A GTP-C entity sets the same message priority in a Triggered message or Triggered Reply message as received in the corresponding Initial message or Triggered message respectively. For incoming GTP-C messages that do not have a message priority in the GTP-C header, the receiving GTP-C entity:

- Applies a default priority if the incoming message is an Initial message.
- Applies the message priority sent in the Initial message or Triggered message if the incoming message is a Triggered or Triggered Reply message respectively.

The nodes in the network homogenously support this feature; otherwise an overloaded node processes initial messages received from the non-supporting nodes according to the default priority and processes initial messages received from the supporting nodes according to the message priority signaled in the GTP-C message.

Message-Prioritization based on Session Parameters

Message prioritization is also performed based on the session parameters such as APN and ARP. The procedures and messages associated with the higher priority sessions are given lesser preference while throttling, as compared to the procedures and messages associated with the lower priority sessions. Within each group of sessions, the messages are further prioritized based on the category of the procedure for which the message is being sent.

Message-Priority Header for PFCP

When the message throttling is performed:

- PFCP requests related to priority traffic (that is, eMPS as described in 3GPP TS 22.153) and emergency have the highest priority. Depending on regional/national requirements and network operator policy, these PFCP requests are the last to be throttled when applying traffic reduction. Throttling exempts the priority traffic due to PFCP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.
- For other types of sessions, the message throttling considers the relative priority of the messages so that the messages with low priority are first considered for the throttling. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent or derived from the session parameters such as APN and ARP.

An overloaded node (UPF, SMF) may apply these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of a self-protection mechanism. Incoming messages are handled during an overloaded condition based on the relative PFCP message priority signaled in the PFCP header.

A PFCP entity determines whether to set and use the message priority in PFCP signalling, based on operator policy. A sending PFCP entity determines the relative message priority to signal in the message which are derived from the session parameters such as APN and ARP. If the message affects multiple bearers, the relative message priority is determined considering the highest priority ARP among all the bearers. A PFCP entity must set the same message priority in a Response message as received in the corresponding Request message.

For incoming PFCP messages that do not have a message priority in the PFCP header, the receiving PFCP entity:

- Applies a default priority if the incoming message is a Request message.
- Applies the message priority sent in the Request message if the incoming message is a Response message.

The SMF and UPF functions in the network homogenously support this feature; otherwise an overloaded node will process the Request messages received from the non-supporting nodes according to the default priority and Request messages received from supporting nodes will be processed according to the message priority signalled in the PFCP message.

Mission Critical Services

A Mission Critical Service (MCX Service) is a communication service that enables capabilities of Mission Critical Applications. The MCX service is provided to end users from Mission Critical Organizations and mission critical applications for businesses and organizations. An MCX Service is either Mission Critical

Push To Talk (MCPTT), Mission Critical Video (MCVideo), or Mission Critical Data (MCData) and represents a set of requirements between two or more MCX Service types.

MCX Services are based on the ability to invoke, modify, maintain, and release sessions with priority, and deliver the priority media packets under network congestion conditions. These services are supported in a roaming environment when roaming agreements are in place and where regulatory requirements apply.

An MCX subscription allows users to receive priority services if the network supports MCX. MCX Users require the 5GS functionality for real-time, dynamic, secure and limited interaction with the QoS and policy framework for modification of the QoS and policy framework by authorized users.

Expanded Prioritization for VoLTE/VoNR/Emergency Calls

The SMF+PGW-C supports Expanded Prioritization for VoLTE/VoNR/Emergency calls. The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers. The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is particularly needed when the Service Providers' networks are impaired due to congestion and/or damage from natural disasters (such as floods, earthquakes and hurricanes) and man-made disasters (such as physical, cyber or other forms of terrorist attacks).

As part of this feature, the PGW-C control message is marked with DSCP marking and also for control message belonging to the eMPS session or containing Allocation and Retention Priority (ARP) associated with the eMPS profile.

DSCP Marking for N3/S5-U/S2-B over PFCP

Transport Level Marking

Transport level marking is the process of marking traffic with a DSCP value based on the locally configured mapping from the QCI and optionally the ARP priority level. For EPC, the S-GW and P-GW perform transport level marking on a per EPS bearer basis. For 5GC, the S-GW and P-GW perform transport level marking on a per QoS flow basis.

The UPF performs transport level marking with a DSCP value based on the mapping from the 5QI, the Priority Level (if explicitly signaled), and optionally the ARP priority level configured at the SMF. The CP function controls transport level marking by providing the DSCP in the ToS or Traffic Class within the Transport Level Marking IE in the FAR (associated to the PDR matching the traffic to be marked).

The UP function performs transport level marking for the detected traffic and sends the marked packet to the peer entity. The CP function changes transport level marking by changing the Transport Level Marking IE in the related FAR.

WPS Profile Support

The SMF+PGW-C supports the WPS profile defined with ARP and DSCP marking value to be set for GTP-C and PFCP Protocol IP-headers. The WPS profile sets the message priority in the GTP-C and PFCP protocols.

The SMF+PGW-C allows a maximum of 64 WPS profiles and each WPS profile will be associated under the DNN profile. See the Configuring Wireless Priority Services, on page 669 section for more information.

How it Works

License Information

The WPS feature requires a license to be enabled on the SMF+PGW-C to support the related features - MPS, MCX, Prioritization for VoLTE/VoNR/Emergency Service. Contact your Cisco account representative for more information on how to obtain a license.

Standards Compliance

The Wireless Priority Services feature complies with the following standards:

- 3GPP TS 22.153
- 3GPP TS 23.228
- 3GPP TS 23.282
- 3GPP TS 23.379
- 3GPP TS 23.501
- 3GPP TS 23.502
- 3GPP TS 23.503
- 3GPP TS 24.301

Configuring Wireless Priority Services

This section describes how to configure the Wireless Priority Services feature.

Configuring the WPS Profile

Use the following configuration to configure the WPS profile.

```
configure
  profile wps wps_profile_name
    arp arp_value
    dscp n3 n3_value
    message-priority [ gtpc pfcp ]
    end
```

NOTES:

- **profile wps** *wps_profile_name*: Accesses the Wireless Priority Services Profile configuration. *wps_profile_name* must be an alphanumeric string of 1 to 63 characters.
- **arp** *arp_value*: Specifies the range of ARP levels. *arp_value* must be an inetger from 1 to 15 separated either by "," or "-".

- **dscp n3** *n3_value*: Specifies the DSCP marking value for N3. *n3_value* specifies the UP DSCP marking value within the range 0 to 0x3F.
- **message-priority { gtpc pfcp }**: Specifies the message priority for GTP-C and PFCP.

Verifying the WPS Profile Configuration

This section describes how to verify the WPS Profile configuration.

Execute the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```
show running-config profile wps wps1
profile wps wps1
arp 1,4-6,9
dscp n3 10
message-priority [ pfcp gtpc ]
exit
```

Associating WPS Profile under DNN Profile

Use the following configuration to associate the WPS profile with the configured DNN profile.

```
configure
  profile dnn intershat
    wps-profile wps_profile_name
    end
```

NOTES:

- **wps-profile** *wps_profile_name*: Enables the Wireless Priority Services Profile configuration. This profile is configured under the existing DNN profile configuration.

Verifying WPS Profile under DNN Profile

This section describes how to verify the WPS profile configuration under the DNN profile.

Execute the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```
show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
wps-profile wps1
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
exit
```

WPS OAM Support

SMF Session Gauge Counters

The "wps" label is introduced at the SMF service to account for session-level gauage counters that support WPS and non-WPS functionality.

For example:

```
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="non_wps"}
 10
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="wps"}
 20
```

N4 Interface Metrics

The N4 interface counters related to message priority include:

- N4_MSG_SESSION_DELETION_REQUEST
- N4_MSG_SESSION_ESTABLISHMENT_REQUEST
- N4_MSG_SESSION_MODIFICATION_REQUEST

An example of the N4 interface metrics:

```
smf_proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="N4_MSG_SESSION_DELETION_REQUEST",msgpriority=true,
service_name="smf-protocol",status="accepted",transport_type="origin"} 4
smf_proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="N4_MSG_SESSION_ESTABLISHMENT_REQUEST",msgpriority=true,
service_name="smf-protocol",status="accepted",transport_type="origin"} 6
smf_proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="N4_MSG_SESSION_MODIFICATION_REQUEST",msgpriority=true,
service_name="smf-protocol",status="accepted",transport_type="origin"} 20
```

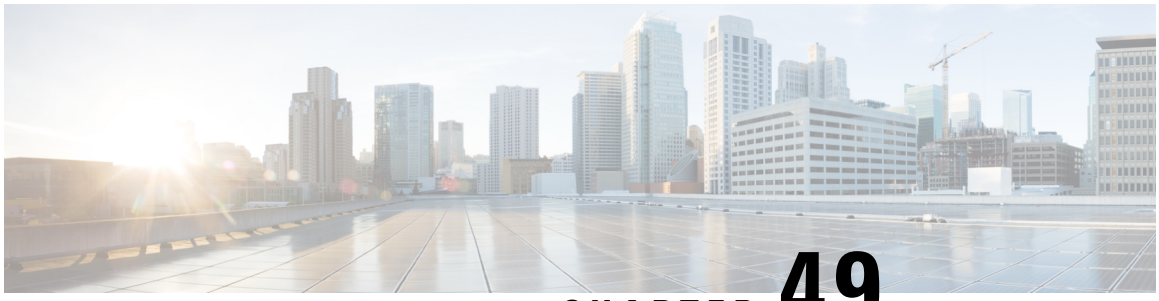
GTPv2 Metrics

The GTPv2 counters related to message priority include:

- NumCreateBearerSuccess
- NumRxCreateBearerRes
- NumTxCreateSessionReq

An example of the GTPv2 metrics:

```
smf_gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumCreateBearerSuccess",instance_id="0",priority_msg="true",service_name="gtpc-ep"}
 2
smf_gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumRxCreateBearerRes",instance_id="0",priority_msg="true",service_name="gtpc-ep"}
 2
smf_gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumTxCreateSessionReq",instance_id="0",priority_msg="true",service_name="gtpc-ep"}
 2
```



CHAPTER 49

5G SMF Serviceability CLI Enhancements

Feature Summary and Revision History

Summary Data

Table 203: Summary Data

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 204: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

This chapter describes serviceability CLI enhancements to display the information about the deployed pods.

show subscriber pei <imei>

Table 205: show subscriber pei <imei>

Field	Description
policy	Specifies policy information.
ipv4-addr	Specifies IPv4 pool name.
dnn	Specifies DNN value.
pcf	Specifies PCF Address.
rat	Specifies RAT Type - nr/e-utran/wlan information.
connectivity	Specifies connectivity 4g/5g
ipv4-range	Specifies IPv4 address range.
chf	Specifies CHF address.
pei	Specifies Permanent Equipment Identifier.
udm	Specifies the UDM address.
upfEpKey	Specifies the UPF address EP key information.
ipv6-pfx	Specifies the IPv6 prefix information.
ipv6-pool	Specifies IPv6 Pool name.
chfGroupId	Specifies the CHF address group ID information.
gpsi	Specifies Generic Public Subscription Identifier.
pcfGroupId	Specifies PCF Address group ID.
upf	Specifies UPF Address.
ipv4-pool	Specifies IPv4 Pool name.
ipv6-range	Specifies IPv4 Address-Range.
amf	Specifies AMF address.
supi	Specify SUPI value.
access	Specifies access information.

show subscriber <gpsi>

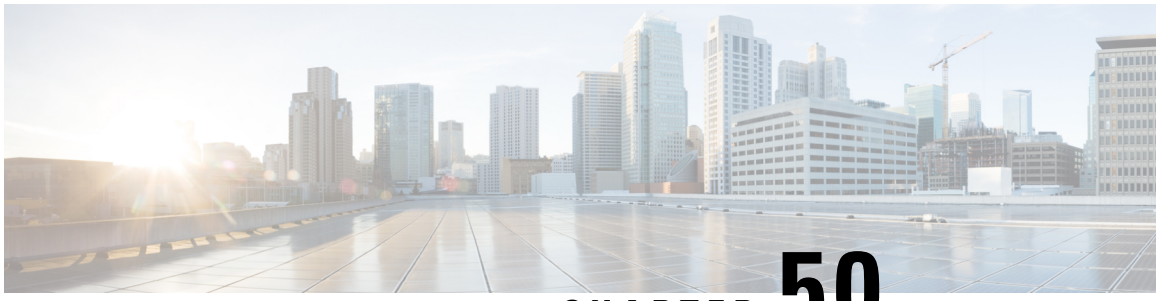
Table 206: show subscriber pei <imei>

Field	Description
policy	Specifies policy information.
ipv4-addr	Specifies IPv4 pool name.
dnn	Specifies DNN value.
pcf	Specifies PCF Address.
rat	Specifies RAT Type - nr/e-utran/wlan information.
connectivity	Specifies connectivity 4g/5g
ipv4-range	Specifies IPv4 address range.
chf	Specifies CHF address.
pei	Specifies Permanent Equipment Identifier.
udm	Specifies the UDM address.
upfEpKey	Specifies the UPF address EP key information.
ipv6-pfx	Specifies the IPv6 prefix information.
ipv6-pool	Specifies IPv6 Pool name.
chfGroupId	Specifies the CHF address group ID information.
gpsi	Specifies Generic Public Subscription Identifier.
pcfGroupId	Specifies PCF Address group ID.
upf	Specifies UPF Address.
ipv4-pool	Specifies IPv4 Pool name.
ipv6-range	Specifies IPv4 Address-Range.
amf	Specifies AMF address.
supi	Specify SUPI value.
access	Specifies access information.

show endpoint info

Table 207: show endpoint info

Field	Description
endpoint	Specifies the Name of the endpoint.
address	Specifies Host and Port of endpoint.
type	Specifies type of endpoint.
status	Specifies current Status of endpoint.
interface	Specifies Interface name of endpoint.
internal	Specifies type of endpoint (Internal/External).
start Time	Specifies Start time of endpoint.
stop Time	Specifies Stop time of endpoint.



CHAPTER 50

Troubleshooting Information

Feature Summary and Revision History

Summary Data

Table 208: Summary Data

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 209: Revision History

Revision Details	Release
Updated the Troubleshooting information for this release.	Pre-2020.02.0

clear subscriber

Table 210: clear subscriber Command Output Description

Field	Description
all	Clears all the sessions.
amf	Clears subscriber based on AMF address.
chf	Clears subscriber based on CHF address.
dnn	Clears subscriber based on DNN value.
gtp-peer	Clears subscriber based on GTP-PEER address.
ipv4-pool	Clears subscriber based on IPv4 pool name.
ipv4-range	Clears subscriber based on IPv4 address-range.
ipv6-pool	Clears subscriber based on IPv6 pool name.
ipv6-range	Clears subscriber based on IPv6 prefix-range.
pcf	Clears subscriber based on PCF address.
policy	Clears subscriber based on policy information.
purge	Clears true, if purged locally.

clear subscriber supi imsi <imsi_value>

Table 211: clear subscriber supi imsi <imsi_value> Command Output Description

Field	Description
ebi	Clears subscriber based on EPS bearer ID.
imsi	Clears subscriber based on IMSI.
purge	Clears true, if purged locally.
\| | Output modifier. |

clear subscriber supi imsi <imsi_value> psid <psid_value>

Table 212: clear subscriber supi imsi <imsi_value> psid <psid_value> Command Output Description

Field	Description
ebi	Clears subscriber based on EPS bearer ID.
imsi	Clears subscriber based on IMSI.
psid	Clears subscriber based on Service ID.
purge	Clears true, if purged locally.
|	Output modifier.

show subscriber

This commands displays the existing show subscriber CLI output with the newly added CLI output.

Table 213: show subscriber Command Output Description

Field	Description
amf	Displays the AMF address.
chf	Displays the CHF address.
count	Displays the number of sessions.
debug	Displays the debugging information.
dnn	Displays the DNN value.
gtp-peer	Displays the GTP-peer address.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
udm	Displays the UDM address.
upf	Displays the UPF address.
|	Displays the output modifiers.

show subscriber count

This command displays the CLI options for the count CLI command.

Table 214: show subscriber count Command Output Description

Field	Description
all	Displays all the SUPIs.
amf	Displays the AMF address.
chf	Displays the CHF address.
dnn	Displays the DNN value.
gtp-peer	Displays the GTP-peer address.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
supi	Displays the specific SUPI value.
udm	Displays the UDM address.
upf	Displays the UPF address.
|	Displays the output modifiers.

show subscriber count all

This command displays the total number of sessions for all the SUPIs.

Table 215: show subscriber count all Command Output Description

Field	Description
|	Displays the output modifiers.

show subscriber count chf <chf_address>

This command displays the total number of sessions for the specified parameters.

Table 216: show subscriber count chf <chf_address> Command Output Description

Field	Description
amf	Displays the AMF address.
dnn	Displays the DNN value.
gtp-peer	Displays the GTP-peer address.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
udm	Displays the UDM address.

Field	Description
upf	Displays the UPF address.
|	Displays the output modifiers.

show subscriber count chf <chf_address> dnn <dnn_value>

This command displays the total number of sessions for the specified parameters.

Table 217: show subscriber count chf <chf_address> dnn <dnn_value> Command Output Description

Field	Description
amf	Displays the AMF address.
gtp-peer	Displays the GTP-peer address.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
udm	Displays the UDM address.
upf	Displays the UPF address.
|	Displays the output modifiers.

show subscriber count supi <supi_value>

This command displays the total number of sessions for the specific SUPI value.

Table 218: show subscriber count supi <supi_value> Command Output Description

Field	Description
|	Displays the output modifiers.

show subscriber debug-info supi <supi_value>

This command displays the debug information for the specific SUPI value where the PSID value is optional.

Table 219: show subscriber debug-info supi <supi_value> Command Output Description

Field	Description
psid	Displays the Provider Service Identifier.

show subscriber debug-info supi <supi_value> psid <psid_value>

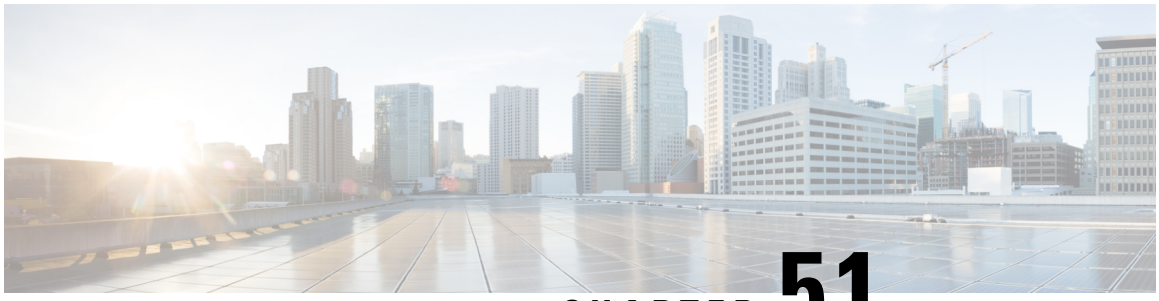
This command displays the debug information for the specific SUPI and PSID combination.

Table 220: show subscriber debug-info supi <supi_value> psid <psid_value> Command Output Description

Field	Description
|	Displays the output modifiers.

Note Currently, the SMF does not validate the serving PLMN received on N11 interface. Also, the SMF does not validate the UE PLMN when the N11 smContextCreate or GTP createSessionRequest is received.

The PLMN value received in the NSSAI included in the PCO request remain the same as the PLMN configured on the SMF.



CHAPTER 51

Sample SMF Configuration

Feature Summary and Revision History

Summary Data

Table 221: Summary Data

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 222: Revision History

Revision Details	Release
Updated the Sample SMF Configuration information for this release.	Pre-2020.02.0

Sample Configuration

The following is only a sample configuration file provided solely for your reference. You must create and modify your own configuration file according to the specific needs of your deployment.

```
===== snip ======
ipam
 source local
 address-pool ipv6
  vrf-name ISP
  tags
   dnn intershat
  exit
  ipv6
   prefix-ranges
    prefix-range 2001:4870:e00b:1500:: length 56
   exit
  exit
 exit
 address-pool poolv4
  vrf-name ISP
  tags
   dnn intershat
  exit
  ipv4
   split-size
    per-cache 1024
    per-dp    256
   exit
   address-range 15.0.0.1 15.0.0.254
  exit
 exit
exit
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
group nrf discovery udmdiscovery
 service type nrf nnrf-disc
  endpoint-profile epprof
   capacity   10
   priority   1
   uri-scheme http
   version
    uri-version v1
     full-version 1.1.1.[1]
    exit
   exit
   endpoint-name endpointName
    priority 1
    capacity 100
    primary ip-address ipv4 10.86.73.206
    primary ip-address port 8082
   exit
  exit
 exit
exit
group nrf mgmt MGMT
 service type nrf nnrf-nfm
  endpoint-profile mgmt-1
   priority   1
   uri-scheme http
   endpoint-name mgmt-1
    primary ip-address ipv4 10.86.73.206
    primary ip-address port 8082
    secondary ip-address ipv4 10.86.73.206
    secondary ip-address port 8083
    tertiary ip-address ipv4 10.86.73.206
    tertiary ip-address port 8084
```

```
   exit
  exit
 exit
exit
cdl node-type smf-cdl
cdl zookeeper replica 2
cdl kafka replica 2
etcd replicas 1
endpoint nodemgr
exit
endpoint gtp
 replicas 1
 vip-ip 10.86.73.208
exit
endpoint pfcp
 replicas 1
 nodes    2
exit
endpoint service
 replicas 1
 nodes    1
exit
endpoint protocol
 replicas 1
 nodes    2
 vip-ip 10.86.73.208
exit
endpoint sbi
 replicas 1
 nodes    2
 vip-ip 10.86.73.208
 interface nrf
  loopbackPort 7005
  vip-ip 20.20.20.5 vip-port 9005
 exit
 interface n7
  loopbackPort 7001
  vip-ip 20.20.20.1 vip-port 9001
 exit
 interface n10
  loopbackPort 7004
  vip-ip 20.20.20.4 vip-port 9004
 exit
 interface n40
  loopbackPort 7003
  vip-ip 20.20.20.3 vip-port 9003
 exit
exit
logging level application trace
logging level transaction trace
logging level tracing off
logging name infra.config.core level application debug
logging name infra.config.core level transaction warn
logging name infra.config.core level tracing warn
logging name infra.resource_monitor.core level application warn
logging name infra.resource_monitor.core level transaction warn
deployment
 app-name     SMF
 cluster-name Local
 dc-name      DC
 model        small
exit
k8 label protocol-layer key smi.cisco.com/node-type value smf-proto
exit
```

```
k8 label service-layer key vm-type value smf-svc
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit
system mode running
helm default-repository smf
helm repository smf
 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-smf/smf-products/master/
exit
helm repository smf-stage
 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-smf/smf-products/dev-smf-stage/
exit
k8s namespace     smf
k8s registry      dockerhub.cisco.com/smi-fuse-docker-internal
k8s single-node   false
k8s use-volume-claims false
k8s ingress-host-name 10.86.73.204.nip.io
profile dnn intershat
 dns primary ipv4 11.11.1.1
 dns primary ipv6 66:66:1::aa
 dns secondary ipv4 22.22.2.2
 dns secondary ipv6 66:66:2::bb
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 dnn starent.com network-function-list [ upf ]
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 pcscf-profile    pcscf1
 ssc-mode 1
 session type IPV4 allowed [ IPV4V6 ]
 upf apn cisco.com
exit
profile dnn profDnn1
 dnn cisco.com network-function-list [ chf pcf udm upf ]
 charging-profile chgprf1
 ssc-mode 1
 session type IPV4
exit
profile dnn profDnn2
 dnn cisco.com network-function-list [ chf pcf rmgr udm upf ]
 charging-profile chgprf1
 ssc-mode 1
 session type IPV4
exit
profile charging chgprf1
 method                  [ offline ]
 limit volume 20
 limit duration 60
 tight-interworking-mode true
 reporting-level online rating-group
 reporting-level offline service-id
exit
profile pcscf pcscf1
 v4-list
  precedence 3
   primrary 3.3.3.1
   secondary 3.3.3.2
  exit
```

```
  precedence 5
   primrary 5.5.5.1
   secondary 5.5.5.2
  exit
  precedence 7
   primrary 7.7.7.1
   secondary 7.7.7.2
  exit
 exit
 v6-list
  precedence 3
   primrary 33:33::1
   secondary 33:33::2
  exit
  precedence 5
   primrary 55:55::1
   secondary 55:55::2
  exit
 exit
 v4v6-list
  precedence 3
   primrary ipv4 46.46.33.1
   primrary ipv6 46:46:33::1
   secondary ipv4 46.46.33.2
   secondary ipv6 46:46:33::2
  exit
  precedence 5
   primrary ipv4 46.46.55.1
   primrary ipv6 46:46:55::1
   secondary ipv4 46.46.55.2
   secondary ipv6 46:46:55::2
  exit
  precedence 7
   primrary ipv4 46.46.77.1
   primrary ipv6 46:46:77::1
   secondary ipv4 46.46.77.2
   secondary ipv6 46:46:77::2
  exit
 exit
exit
profile charging-characteristics 1
 charging-profile chgprf1
exit
profile icmpv6 icmpprf1
 options virtual-mac b6:6d:57:45:45:45
exit
profile smf smf1
 locality      LOC1
 bind-address ipv4 10.86.73.208
 bind-port     8090
 fqdn          192.168.10.20
 allowed-nssai [ slice1 slice2 ]
 plmn-id mcc 123
 plmn-id mnc 456
 service name nsmf-pdu
  type               pdu-session
  schema             http
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile dec18
  access-profile     access1
  policy subscriber polSub
 exit
```

```
exit
profile compliance dec18
 service nsmf-pdusession
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service namf-comm
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service n1
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service n2
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service nudm-sdm
  version uri v1
  version full 1.0.0
  version spec 15.2.1
 exit
 service nudm-uecm
  version uri v1
  version full 1.0.0
  version spec 15.2.1
 exit
 service nnrf-disc
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service nnrf-nfm
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service npcf-smpolicycontrol
  version uri v1
  version full 1.0.0
  version spec 15.2.0
 exit
 service nchf-convergedcharging
  version uri v2
  version full 1.0.0
  version spec 15.2.1
 exit
exit
profile network-element amf amf1
 nf-client-profile        amfP1
 failure-handling-profile FH3
 query-params [ dnn ]
exit
profile network-element pcf pcf1
 nf-client-profile        pcfP1
 failure-handling-profile FH1
 rulebase-prefix          cbn#
 predefined-rule-prefix   crn#
exit
```

```
profile network-element udm udm1
 nf-client-profile        udmP1
 failure-handling-profile FH1
exit
profile network-element upf upf1
 n4-peer-address ipv4 10.106.183.240
 n4-peer-port 8805
 keepalive    60
 dnn-list     [ dnn1 intershat starent ]
exit
profile network-element chf chf1
 nf-client-profile                chfP1
 failure-handling-profile         FH2
 nf-client-profile-offline        CP2
 failure-handling-profile-offline FH2
exit
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
 dscp-map qi5 2 arp-priority-level 3 uplink user-datagram dscp-marking 0x1c
 dscp-map qi5 2 arp-priority-level 3 downlink user-datagram dscp-marking 0x1a encsp-header
 dscp-marking 0x1b
 dscp-map qi5 3 arp-priority-level 3 uplink user-datagram dscp-marking 0x4
 dscp-map qi5 3 arp-priority-level 3 downlink user-datagram dscp-marking 0x3 encsp-header
copy-inner
exit
profile access access1
 eps-fallback cbr delay 500 max-retry 10 timeout 3
 n26 idft enable timeout 15
 n2 idft enable timeout 15
exit
profile nf-client nf-type udm
 udm-profile udmP1
  locality LOC1
   priority 30
   service name type nudm-sdm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 10.86.73.206
      primary ip-address port 9007
     exit
    exit
   exit
   service name type nudm-uecm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 10.86.73.206
      primary ip-address port 9001
     exit
    exit
   exit
  exit
 exit
exit
```

```
profile nf-client nf-type pcf
 pcf-profile pcfP1
  locality LOC1
   priority 30
   service name type npcf-am-policy-control
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 50
      primary ip-address ipv4 10.86.73.206
      primary ip-address port 9003
     exit
    exit
   exit
   service name type npcf-smpolicycontrol
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 5
      primary ip-address ipv4 10.86.73.206
      primary ip-address port 9003
     exit
     endpoint-name realPCF
      priority 10
      primary ip-address ipv4 10.86.73.210
      primary ip-address port 9082
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type amf
 amf-profile amfP1
  locality LOC1
   priority 10
   service name type namf-comm
    endpoint-profile EP1
     capacity   20
     uri-scheme http
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 10.86.73.206
      primary ip-address port 9002
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type chf
 chf-profile CP2
  locality LOC1
   priority 31
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
```

```
      endpoint-name EP1
       priority 56
       primary ip-address ipv4 10.86.73.206
       primary ip-address port 9906
      exit
     exit
    exit
   exit
  exit
  chf-profile chfP1
   locality LOC1
    priority 10
    service name type nchf-convergedcharging
     endpoint-profile EP1
      capacity   30
      uri-scheme http
      version
       uri-version v2
       exit
      exit
      endpoint-name EP1
       priority 50
       primary ip-address ipv4 10.86.73.206
       primary ip-address port 9904
      exit
      endpoint-name EP2
       priority 80
       primary ip-address ipv4 10.86.73.206
       primary ip-address port 9905
      exit
     exit
    exit
   exit
  exit
 exit
exit
profile nf-pair nf-type UDM
 locality client LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type AMF
 locality client LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type PCF
 locality client LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type UPF
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type CHF
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-client-failure nf-type chf
 profile failure-handling FH2
  service name type nchf-convergedcharging
   message type ChfConvergedchargingCreate
    status-code httpv2 0
     action continue
```

```
    exit
   exit
   message type ChfConvergedchargingUpdate
    status-code httpv2 0
     action continue
    exit
   exit
  exit
 exit
exit
policy subscriber polSub
 precedence 1
  sst              01
  sdt              ABcd01
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range 100000000000001
  supi-stop-range  999999999999999
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  operator-policy  opPol1
 exit
exit
policy operator opPol1
 policy dnn opPolDnn1
exit
policy dnn dnnPol1
 profile default
 dnn starent profile abc.com
exit
policy dnn opPolDnn1
 dnn intershat profile intershat
 dnn intershat1 profile profDnn1
exit
policy dnn polDnn
 profile default
 dnn intershat profile intershat
 dnn intershat1 profile profDnn1
 dnn intershat2 profile profDnn2
exit
nssai name slice1
 sst 01
 sdt ABcd01
 dnn [ intershat ]
exit
nssai name slice2
 sst 02
 sdt 000003
 dnn [ cisco.com ]
exit
active-charging service acs1
 packet-filter pkt1
  ip local-port range 2 to 23
  ip protocol = 23
  ip remote-address = 10.10.10.0/24
  ip remote-port range 12 to 34
  ip tos-traffic-class = 23 mask = 23
  priority 23
 exit
 packet-filter pkt2
  direction uplink
  ip local-port = 100
  ip protocol = 100
  ip remote-address = 1.1.1.1/32
```

```
  ip remote-port = 140
  priority  100
 exit
 packet-filter pkt3
  direction downlink
  ip local-port = 111
  ip protocol = 111
  ip remote-address = 2.2.2.2/31
  ip remote-port = 111
  priority  111
 exit
 charging-action ca1
  allocation-retention-priority 12 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard committedDataRate 2000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 3
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
 exit
 charging-action ca10
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000000 peak-burst-size 100
 violate-action discard
  tos af11
 exit
 charging-action ca11
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000000 peak-burst-size 100
 violate-action discard
 exit
 charging-action ca12
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca13
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca2
  allocation-retention-priority 13 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000000 peak-burst-size 100
violate-action discard committedDataRate 3000000000 committed-burst-size 100 exceed-action
 discard
  flow limit-for-bandwidth direction downlink peak-data-rate 3000000000 peak-burst-size 100
 violate-action discard committedDataRate 4000000000 committed-burst-size 100 exceed-action
 discard
  qos-class-identifier 2
  tft-notify-ue
  tos af11
  tft packet-filter pkt2
 exit
 charging-action ca20
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
```

```
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca21
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca22
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca23
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000 peak-burst-size 100
violate-action discard
 exit
 charging-action ca3
  allocation-retention-priority 14 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 1000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 1
  tft-notify-ue
  tos af11
  tft packet-filter pkt3
 exit
 charging-action ca4
  allocation-retention-priority 11 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 4000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 4
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
 exit
 charging-action ca5
  allocation-retention-priority 11 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 4000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 4
  tft-notify-ue
  tos af11
  tft packet-filter pkt2
 exit
 charging-action ca6
  allocation-retention-priority 11 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
```

```
violate-action discard committedDataRate 3000000 committed-burst-size 100 exceed-action
discard
  flow limit-for-bandwidth direction downlink peak-data-rate 4000000 peak-burst-size 100
violate-action discard committedDataRate 4000000 committed-burst-size 100 exceed-action
discard
  qos-class-identifier 4
  tft-notify-ue
  tos af11
  tft packet-filter pkt3
 exit
 charging-action ca7
  allocation-retention-priority 1 pci NOT_PREEMPT pvi NOT_PREEMPTABLE
  flow limit-for-bandwidth direction uplink peak-data-rate 2000000 peak-burst-size 100
violate-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 400000 peak-burst-size 100
violate-action discard
  qos-class-identifier 7
  tft-notify-ue
  tos af11
 exit
 charging-action caGyGz
  billing-action egcdr
  cca charging credit rating-group 102
  content-id         102
  service-identifier 202
 exit
 charging-action caOffline
  billing-action egcdr
  content-id         100
  service-identifier 200
 exit
 charging-action caOffline1
  billing-action egcdr
  content-id         11
  service-identifier 21
 exit
 charging-action caOffline2
  billing-action egcdr
  content-id         12
  service-identifier 22
 exit
 charging-action caOffline3
  billing-action egcdr
  content-id         13
  service-identifier 23
 exit
 charging-action caOffline4
  billing-action egcdr
  content-id 40
 exit
 charging-action caOfflineOnline
  billing-action egcdr
  cca charging credit
  content-id         30
  service-identifier 60
 exit
 charging-action caOfflineOnline1
  billing-action egcdr
  cca charging credit
  content-id         31
  service-identifier 61
 exit
 charging-action caOnline
  cca charging credit rating-group 100
```

```
 content-id         100
 service-identifier 200
exit
charging-action caOnline1
 cca charging credit rating-group 101
 content-id         101
 service-identifier 201
exit
charging-action caOnline2
 cca charging credit
 content-id         102
 service-identifier 202
exit
charging-action caOnline3
 cca charging credit
 content-id         103
 service-identifier 203
exit
charging-action caOnline4
 cca charging credit
 content-id 110
exit
charging-action nocharging
exit
rulebase cbn#spp-tmobile
 action priority 1 ruledef crn#test_1 charging-action ca1
 action priority 2 ruledef crn#test_2 charging-action ca2
exit
rulebase rba1
 action priority 1 dynamic-only ruledef rda1 charging-action ca1 description myrule1
 action priority 2 dynamic-only ruledef rda2 charging-action ca2 description myrule2
 action priority 3 dynamic-only ruledef rda3 charging-action ca3 description myrule3
exit
rulebase rba2
 action priority 10 ruledef rda10 charging-action ca10 description myrule10
 action priority 11 ruledef rda11 charging-action ca11 description myrule11
 action priority 12 dynamic-only ruledef rda12 charging-action ca12 description myrule12
 action priority 13 dynamic-only ruledef rda13 charging-action ca13 description myrule13
exit
rulebase rba3
 action priority 20 ruledef rda20 charging-action ca20 description myrule20
 action priority 21 ruledef rda21 charging-action ca21 description myrule21
 action priority 22 dynamic-only ruledef rda22 charging-action ca22 description myrule22
 action priority 23 dynamic-only ruledef rda23 charging-action ca23 description myrule23
exit
rulebase rba4
 action priority 30 ruledef rda3 charging-action ca3 description myrule3
 action priority 31 dynamic-only ruledef rda3 charging-action ca3 description myrule3
exit
rulebase rba5
 action priority 50 dynamic-only ruledef rda50 charging-action ca4 description myrule50
 action priority 51 dynamic-only ruledef rda51 charging-action ca5 description myrule51
 action priority 52 dynamic-only ruledef rda52 charging-action ca6 description myrule52
exit
rulebase rba6
 action priority 60 dynamic-only ruledef rda60 charging-action ca1 description myrule60
 action priority 61 dynamic-only ruledef rda61 charging-action ca1 description myrule61
 action priority 62 dynamic-only ruledef rda62 charging-action ca1 description myrule62
exit
rulebase rba7
 action priority 50 ruledef rda50 charging-action ca4 description myrule50
 action priority 51 ruledef rda51 charging-action ca5 description myrule51
 action priority 52 ruledef rda52 charging-action ca6 description myrule52
exit
```

```
rulebase rba8
 action priority 60 ruledef rda60 charging-action ca1 description myrule60
 action priority 61 ruledef rda61 charging-action ca1 description myrule61
 action priority 62 ruledef rda62 charging-action ca1 description myrule62
exit
rulebase rbaStatic
 action priority 10 ruledef rda20 charging-action caOffline
exit
rulebase rbaStatic-Online
 action priority 20 ruledef rdaStatic charging-action caOnline
exit
rulebase rbaStatic1
 action priority 10 ruledef rda20 charging-action caOffline
exit
rulebase rba_GyGz
 egcdr threshold volume downlink 100000 uplink 100000
 action priority 20 dynamic-only ruledef rdaPredefined charging-action caGyGz
 action priority 30 ruledef rda20 charging-action caGyGz
exit
rulebase rba_charging_StaticDynamic_Offline_Online_mix
 cca diameter requested-service-unit sub-avp volume cc-input-octets 11000 cc-output-octets
12000 cc-total-octets 23000
 credit-control-group onlineoffline
 egcdr threshold interval 100
 egcdr threshold volume downlink 150000 uplink 150000 total 300000
 action priority 20 dynamic-only ruledef rdaPredefined charging-action caOffline1
 action priority 21 dynamic-only ruledef rdaPredefined1 charging-action caOnline1
 action priority 31 ruledef rdaStatic charging-action caOfflineOnline
exit
rulebase rba_charging_StaticDynamic_offline
 egcdr threshold volume downlink 100000 uplink 100000
 action priority 20 dynamic-only ruledef rdaPredefined charging-action caOffline1
 action priority 30 ruledef rda20 charging-action caOffline
exit
rulebase rba_charging_StaticDynamic_online
 action priority 20 ruledef rda20 charging-action caOnline
 action priority 30 dynamic-only ruledef rdaPredefined charging-action caOnline1
exit
rulebase rbs1
 action priority 1 ruledef rds1 charging-action ca1 description myrules1
 action priority 2 ruledef rds2 charging-action ca2 description myrules2
exit
urr-list urr_smf
 rating-group 10 service-identifier 20 urr-id 1
 rating-group 11 service-identifier 21 urr-id 2
 rating-group 12 service-identifier 22 urr-id 3
 rating-group 13 service-identifier 23 urr-id 4
 rating-group 30 service-identifier 60 urr-id 20
 rating-group 31 service-identifier 61 urr-id 21
 rating-group 100 service-identifier 200 urr-id 5
 rating-group 101 service-identifier 201 urr-id 6
 rating-group 102 service-identifier 202 urr-id 7
 rating-group 103 service-identifier 203 urr-id 8
exit
ruledef rda1
 ip server-ip-address = 10.10.10.10
exit
ruledef rda10
 ip any-match = TRUE
exit
ruledef rda11
 ip any-match = TRUE
exit
ruledef rda12
```

```
 ip any-match = TRUE
exit
ruledef rda13
 ip any-match = TRUE
exit
ruledef rda2
 ip server-ip-address = 10.165.161.77/32
exit
ruledef rda20
 ip any-match = TRUE
exit
ruledef rda21
 ip any-match = TRUE
exit
ruledef rda22
 ip any-match = TRUE
exit
ruledef rda23
 ip any-match = TRUE
exit
ruledef rda3
 ip server-ip-address = 10.198.87.48/28
exit
ruledef rda40
 ip any-match = TRUE
exit
ruledef rda50
 ip server-ip-address = 50.50.50.50
exit
ruledef rda51
 ip server-ip-address = 51.51.51.51
exit
ruledef rda52
 ip server-ip-address = 52.52.52.52
exit
ruledef rda60
 ip dst-address = 60.60.60.60
exit
ruledef rda61
 ip dst-address = 61.61.61.61
exit
ruledef rda62
 ip dst-address = 62.62.62.62
exit
ruledef rdaPredefined
 ip any-match = TRUE
exit
ruledef rdaStatic
 ip any-match = TRUE
exit
ruledef rdaStatic1
 ip any-match = TRUE
exit
ruledef rdaStatic2
 ip any-match = TRUE
exit
ruledef rds1
 ip any-match = TRUE
exit
ruledef rds2
 ip any-match = TRUE
exit
credit-control group onlineoffline
 diameter ignore-service-id true
```

```
 exit
exit
apn intershat
 gtpp group group1
 active-charging rulebase rba1
exit
gtpp group group1
 gtpp egcdr service-data-flow threshold interval 60
 gtpp egcdr service-data-flow threshold volume downlink 100000 uplink 100000 total 200000
exit
aaa authentication users user admin
 uid        117
 gid        1117
 password   $1$cRyjDAuU$7t8iCDDjhDcKdQ1/YHM2J1
 ssh_keydir /tmp/admin/.ssh
 homedir    /tmp/admin
exit
aaa ios level 0
 prompt "\h> "
exit
aaa ios level 15
 prompt "\h# "
exit
aaa ios privilege exec
 level 0
  command action
  exit
  command autowizard
  exit
  command enable
  exit
  command exit
  exit
  command help
  exit
  command startup
  exit
 exit
 level 15
  command configure
  exit
 exit
exit
nacm write-default deny
nacm groups group admin
 user-name [ admin ]
exit
nacm rule-list admin
 group [ admin ]
 rule any-access
  action permit
 exit
exit
nacm rule-list confd-api-manager
 group [ confd-api-manager ]
 rule any-access
  action permit
 exit
exit
```