

# 5G SMF Overview


- Feature Summary and Revision History, on page 1
- Product Description, on page 2
- Converged Core Overview, on page 3
- Use Cases and Features, on page 5
- Deployment Architecture and Interfaces, on page 13
- Life Cycle of Data Packet, on page 17
- Session Affinity, on page 23
- License Information, on page 24
- Standards Compliance, on page 24


# Feature Summary and Revision History

## Summary Data

***Table 1: 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 2: Revision History***

| Revision Details | Release |
|---|---|
| The converged core support for combined SMF + cnSGWc is added in this release. | 2021.01.0 |

| 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 functionality of the SMF. As specified in *3GPP TS 23.501*, the SMF supports the following functionality:

- 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 Address Resolution Protocol (ARP) proxying and IPv6 Neighbor Solicitation Proxying functionality for the Ethernet PDUs. The SMF responds to 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 functionality:
  - 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 DN. The communication is for the transport of signaling for the PDU session authorization or authentication by an external DN.

The SMF also provides support for an enterprise mobile virtual network operator (MVNO) model, which enables a mobile network operator (MNO) to perform secondary authentication for the leased MVNO subscribers. Additionally, the SMF supports other MVNO features, but is not limited to, RADIUS Client, vDNN, and so on.

# Converged Core Overview

The converged core solution provides an advanced, cloud-native, converged control plane with the capability to support 4G and 5G devices, and use cases.



**Important** This release supports only the cloud-native integrated S-GW and SMF instance with S5C and cnSGW-C functionalities.

The converged core solution removes the operational complexity by providing a unified core network to handle all types of subscribers and use cases.

The operator has the following benefits:

- Improves the overall network efficiency by reducing signaling between cnSGW-C and SMF while handling a 4G subscriber or handoff from 5G to 4G coverage area.
- Reduces latency introduced due to the extra hop SGW-U for a subscriber in 4G coverage area, by collapsing the data path in the Converged UPF, thus improving the overall user experience.
- Provides ability to use a unified subscriber policy and billing infrastructure using SBA interfaces for 4G and 5G devices.

The solution supports the following converged control plane and user plane functions:

- Converged Control Plane Functions
  - Integrates S-GW and SMF network functions as a single deployment, under a single Kubernetes namespace, to support 4G and 5G devices from E-UTRAN/NR (converged core gateway)
  - Supports logical network functions (data)
- Converged User Plane Functions
  - Integrates UPF and SGW-U functionalities as a single network function
  - Provides simultaneous support for N4 and Sxa interfaces
  - Terminates multiple control planes in a single deployment

# Interservice Pod Communication

## Feature Description

When the cnSGW service and SMF service selected for a subscriber are on the same cluster and same rack, the messages exchanged between the two services flow through the gtpc-ep pod.

If a collocated session is identified and **enable-gtpc-bypass** CLI command is configured under GTP endpoint, then the SMF and cnSGW-C directly communicate with each other without exchanging the messages through the gtpc-ep pod. This approach reduces the latency and the processing load on the gtpc-ep. For details on the command, see the Feature Configuration, on page 5 section.

The SMF service directly communicates with cnSGW service for processing the following requests:

- Create Bearer Request
- Update Bearer Request (UBR) (expect Modify Bearer Command (MBC) triggered UBR)
- Delete Bearer Request (DBR) (expect Delete Bearer Command (DBC) triggered DBR)

The cnSGW service directly communicates with SMF service for processing the following requests:

- Create Session Request
- Modify Bearer Request
- Delete Session Request

If the subscriber session is not collocated, the inbound and outbound messages from SMF or cnSGW-C continue to be exchanged through the gtpc-ep pod.

For this feature support on cnSGW, see the *UCC 5G cnSGWc Configuration and Administration Guide*.

## How it Works

This section describes how this feature works.

Perform the following steps to implement this feature.

1. Identify the deployment type of SMF and cnSGW-C.

   To identify the deployment type, the SMF or cnSGW-C compares the target GTPC peer IP address of the message with the locally configured IP address of S5e or S5 interface for the concerned GR instance. The SMF or cnSGW-C marks the subscriber session as collocated service based on the comparison result.

2. Identify the target service pod

   SMF uses session affinity in cnSGW namespace based on TEID, which is derived from Common ID to appropriately route the message towards cnSGW service pod instance.

3. Route the messages to the appropriate peers based on the identified deployment type and target service pod.

   Interservice pod communication uses the existing framework along with protocol buffer to carry the signaling message content.

   The interservice communication between SMF and cnSGW-C happens with the following exceptions:

   - GTPC messages cannot be captured using the packet sniffer tool and **monitor subscriber** command.
   - Path management is not performed for collocated GTPC peers.
   - GTPC message level metrics (at GTPC endpoint) will not be pegged for interservice GTPC messages as GTPC endpoint is bypassed for such messages.
   - Existing interservice metrics will be pegged for interservice messages.

- UBR and DBR initiated on Command Messages follow the existing message flow path. That is, the SMF sends the command messages to cnSGW service through gtpc-ep pod.

## Feature Configuration

To enable GTPC bypass between cnSGW and SMF service, use the following sample configuration:

```
config
  instance instance-id gr_instance_id
    endpoint gtp
      enable-gtpc-bypass { false | true }
      end
```

**NOTES**:

- **endpoint gtp**: Enter the GTP endpoint configuration.
- **enable-gtpc-bypass { false | true }**: Specify the option to enable or disable the GTPC bypass between cnSGW and SMF service.

  When set to true, the GTPC bypass is enabled between SMF and cnSGW. That is, SMF and cnSGW directly communicate without involving the gtpc-ep pod. By default, it is false.

## OAM Support

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

### Bulk Statistics Support

The following statistics is updated to support this feature.

- smf_service_stats: This statistics includes gtpc_bypass label to track the GTPC bypass messages.

For more information on bulk statistics support, see the *UCC 5G SMF Metrics Reference*.

# Use Cases and Features

This section describes the use cases that SMF supports.

# 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

# 4G Session Support

*Table 3: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| FWA Support | 2025.01.0 | SMF validates and supports 4G Fixed Wireless Access (FWA) for separate subscriber groups: those using 4G interfaces (RADIUS and Gz) and those using 5G SBA interfaces (N7 and N40). |

For UEs, the SMF supports both 5G and 4G NAS to connect to both 4G and 5G core networks. 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 SMF supports interworking with EPS by 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.

Following are the two scenarios that are validated to ensure the support from SMF to handle the FWA subscribers:

1. Subscribers using RADIUS Accounting and Gz Accounting.
2. Subscribers using N7 for policy and N40 for online charging.

Following table lists the details of the supported and unsupported interfaces for FWA subscribers in the precding scenarios.

| | RADIUS Auth | RADIUS Acct | N7 | N40 | N10 | Gz (CDR) | Gy | Gx |
|---|---|---|---|---|---|---|---|---|
| Scenario 1 | No | Yes | No | No | No | Yes | No | No |
| Scenario 2 | No | No | Yes | Yes (only Online) | No | No | No | No |

**Note** SMF supports both types of subscribers using 4G and 5G SBI interfaces on the converged core across different DNNs.

SMF allows all the subscribers for:

- QoS Class Identifier (QCI) upgrade and downgrade for default QoS Flow Identifier (QFI)
- APN-AMBR upgrade and downgrade: Capability to adjust the APN Aggregate Maximum Bit Rate.

The following features are related to this use case:

- 4G to 5G Data Session Handover
- EPS Interworking
- Flow Failure Handling for Access and Mobility Procedures
- Managing Multi-Generation Device Support with Unified SMF
- Session Timers

# 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
- IP Pool Allocation per DNN
- UP Session Activation and Deactivation Service Request Procedures
- Session and Service Continuity Mode
- Static IP Support
- TAI Selection from AMF

# 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-SMF 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:

- 5GSM Cause Code Handling
- AN-initiated Session Modification and Release
- CHF and PCF Integration for Access and Mobility Procedures
- Inter gNodeB Handover
- MTU Support in PCO
- DNN Support
- Network-initiated Session Modification Procedures
- Policy and User Plane Management
- UDM Integration
- Voice over New Radio

# 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:

- Subscriber Charging

# 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 feature is related to this use case:

- Load and Overload Management

# Converged Core Network

The SMF supports standalone deployment or an integrated deployment with cnSGWc for serving 4G and 5G subscribers. Converged Control Plane function comprises a combination of 4G and 5G control plane instances, that is, SMF and cnSGWc.

With converged core deployment, for the same PDN session, the S-GW and SMF select the same UPF instance so that the data path is optimized. The converged core architecture reduces the operational cost and the complexity of maintaining multiple different networks, leverages new interfaces and business avenues.

The converged core deployment involves changing some basic configurations of SMF, pod layout, and optimizing performance with call processing.

The following features are related to this use case:

- Alerts
- Deploying and Configuring SMF through Ops Center
- Dynamic Routing
- EPS Interworking
  - GTP Path Failure Handling, Restoration, and Recovery
  - Support for UE Initial Attach
- Monitor Subscriber and Monitor Protocol
- Pods and Services Reference
- Policy and User Plane Management
  - Support for UPF Node Reports and Proprietary Session Reports
  - Static PCC Rules Support
- Metrics
- UPF Path Management and Restoration
- Wireless Priority Services

# IMS Support

The IP Multimedia Subsystem (IMS) connects to the LTE network and 5G core (through UPF node) for delivering voice services such as Voice over LTE (VoLTE) and Voice over New Radio (VoNR).

The following features are related to this use case:

- Voice Over LTE Support
- Voice over New Radio
- NPLI Support for VoLTE and VoNR

# 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

# 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.

# MVNO Support

The SMF provides support for an enterprise MVNO model. A mobile network operator can perform secondary authentication for the leased MVNO subscribers and also support any additional features related to the AAA server. The SMF uses the RADIUS protocol for such secondary authentication purposes.

The following features are related to this use case:

- Multiple and Virtual DNN Support
  - DNN Case Insensitive Support
- Policy and User Plane Management
  - Increase Max Groups Per Bandwidth Policy
- RADIUS Client
  - Handling RADIUS Disconnect and CoA Requests
  - RADIUS Access Management
  - RADIUS Accounting
  - RADIUS PAP/CHAP/MSCHAP Support
  - RADIUS NAS-IP Support

# NF Management

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 features are related to this use case:

- NF Discovery and Management
- Failure Handling Support

# OAM Support

This use case covers all the Operation, Administration, and Maintenance (OAM) functions of the SMF.

The following features are related to this use case:

- Alerts
- Bulk Statistics and Key Performance Indicators
- Deploying and Configuring SMF through Ops Center
- Logs
- Metrics
- Monitor Subscriber and Monitor Protocol
- Pods and Services Reference
- Smart Licensing
- SMF Rolling Software Update

# Policy Integration

The SMF communicates with the Unified Data Management (UDM) and Policy Control Function (PCF) to perform 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 features are related to this use case:

- DSCP Marking
- Policy and User Plane Management
- Wireless Priority Services

# 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.

The following feature is related to this use case:

- RADIUS Authentication and Accounting

# Redundancy Support

The SMF deployment in K8 cluster plays a vital role to support High Availability (HA) and Geographic Redundancy (GR). The redundancy support ensures stateful session continuity among the clusters during the rack or cluster failures.

The SMF achieves HA through redundant set-up of each cluster component such that any single point of failure is avoided.

The GR provides rack-level redundancy to replicate data between two separate K8 clusters across racks so that, on rack or cluster failure, traffic can switch to a remote rack to process the traffic. Rack or cluster failure can be due to power failure, multi-compute failures, network failure, multi-pod failure, BFD link failure, and so on.

The following features are related to this use case:

- High Availability Support
- Inter-Rack Redundancy Support
- Mesh Connectivity to All UPFs

# Roaming Support

Mobile network operators make roaming partnerships to provide services to the subscribers seamlessly in geographies beyond their network reach. PLMNs define the operator network boundaries. HPLMN is the Subscriber's home network and VPLMN is the visited network from where the service is rendered.

The following features are related to this use case:

- Roaming Support
- Multiple PLMN Support

# 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:

- Event Detail Records
- Policy and User Plane Management

# 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:

- Interfaces Support

## Subscription Management

The SMF handles the user subscription management over the N10 interface.

The following feature is related to this use case:

- UDM Integration

## 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:

- Policy and User Plane Management
- IPv6 PDU Sessions
- UPF Path Management and Restoration

## Wi-Fi 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 features are related to this use case:

- VoWi-Fi Support
- Wi-Fi Handover

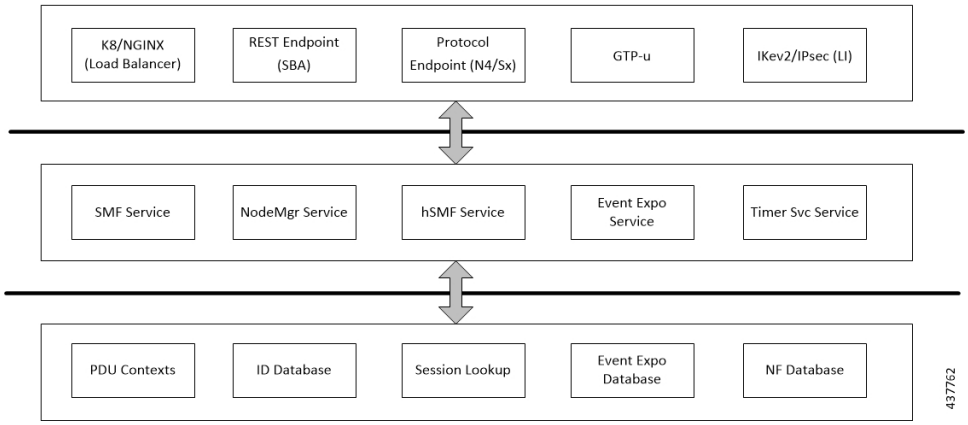
# Deployment Architecture and Interfaces

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 1: 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.

# Converged Core Architecture

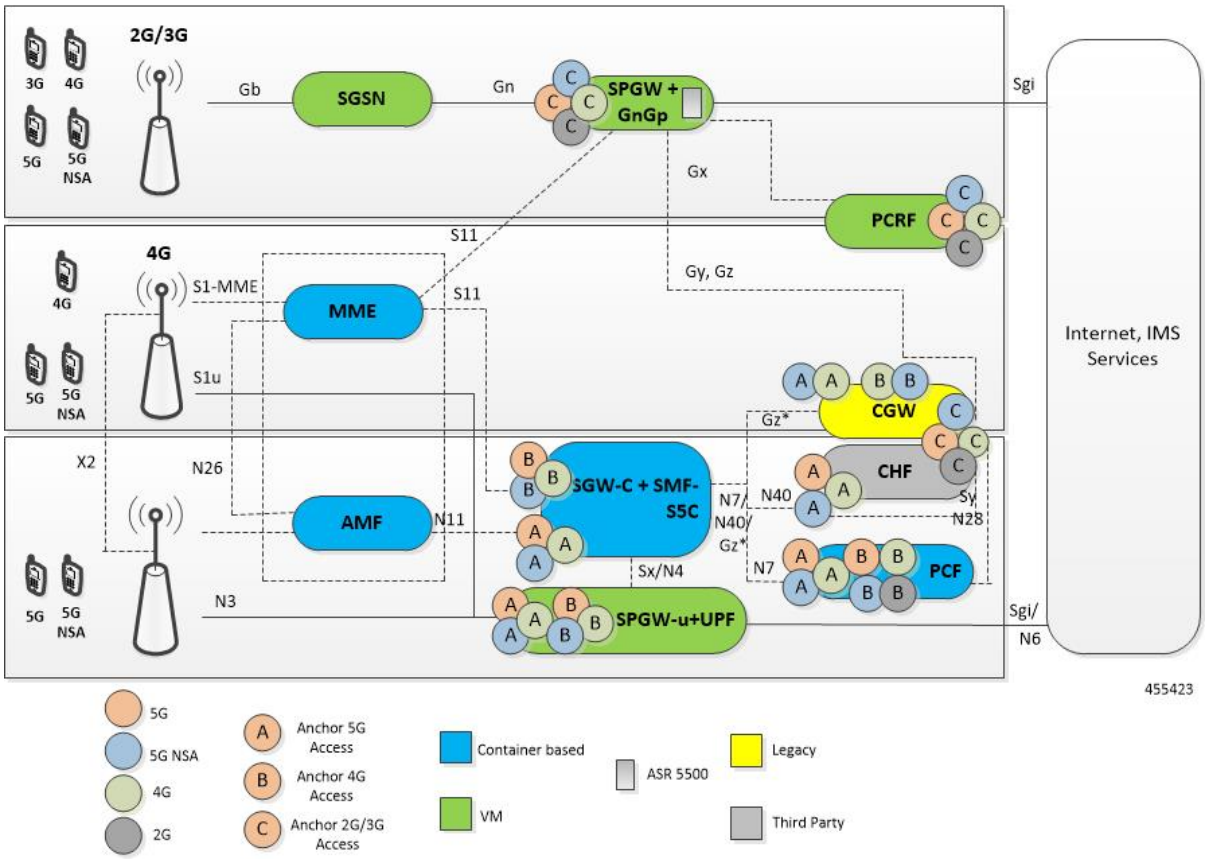
The converged core solution provides a single unified platform which is based on SMI architecture. The supporting architecture integrates the cloud-native S-GW and SMF deployment with 5GC and cnSGW-C functionalities. The solution uses 3GPP-defined SBA interfaces for policy and charging functions.

In the converged core architecture, the 4G and 5G capable UEs are anchored on the same control plane instance. The control plane instance provides the SMF, 5GC, and cnSGW-C functionalities.

The handoffs between 4G and 5G access types are seamless for 5G capable devices. The handoffs from LTE to UTRAN (bi-directional communication between 4G/5G and 3G/2G) are not seamless for 4G capable devices.

The following figure illustrates the supported network architecture.

*Figure 2: Converged Core Architecture*




The UPF deployed as a part of this solution is a VPC-SI VM. The UPF deployment is VM-based, and supports:

- SGW-U, PGW-U, and UPF functionalities in the same instance, and exposes the Sxa, Sxb, Sxab, or N4 interface towards the control plane.
- Multiple CP instances (up to 4) simultaneously.

# Converged Core Deployment

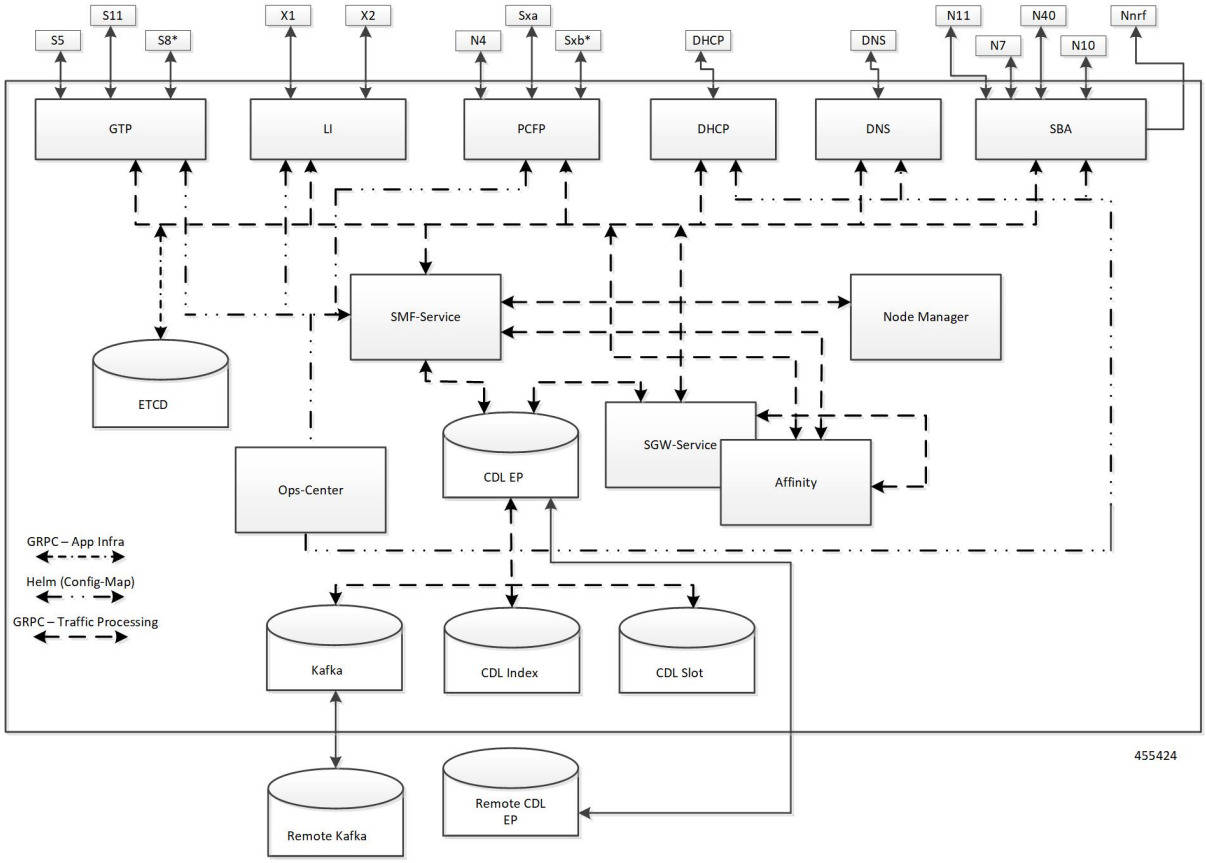
The converged core deployment is based on the converged control plane and unified user plane infrastructure for all use cases.

In the converged core deployment, all 4G and 5G-capable UEs are anchored on the 5G core (SMF) with SBA interfaces towards PCF.

The converged core deployment has a converged Ops Center that allows the configuration of cnSGW-C and SMF services along with other microservices. A single product helm chart is used to install components.

The following figure illustrates the Kubernetes deployment for the converged S-GW and SMF network function.

*Figure 3: Kubernetes Deployment*




The protocol layer services are shared across SMF and S-GW. The GTP endpoint terminates the S11 interface and S5/S8 interface. Similarly, the PFCP (protocol) endpoint terminates the N4 and Sxa interfaces.

The SMF and S-GW services are deployed as distinct pods and the session processing is segregated. Both the service pods use CDL for storing subscriber sessions.

# Supported Interfaces

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

- Diameter—Interface that provides framework for services that require Access, Authorization, and Accounting (AAA) or Policy support across IP-based networks.
- GTP—Uses the N9 interface as the reference point between two core UPFs.
- Gx—Interface between SMF and PCRF.
- Gy—Interface between SMF CTF and OCS Charging Data Function (CDF).
- N1/NAS—Reference point between the UE and AMF.
- N2/NGAP—Reference point between the RAN and AMF.
- 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.
- Nnrf—Interface displayed by NRF on 3GPP 5G system architecture.
- RADIUS—Interface that manages network access.
- S2b—Interface between the PGW-C and ePDG.
- S5—Interface between the PGW-C and S-GW.
- SBA—Interface for NFs to communicate with each other.

For details on the supported interfaces, see the Interfaces Support chapter.

# 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 4: 4G Session Procedure - Complete ByPass(PFCP and GTP)*

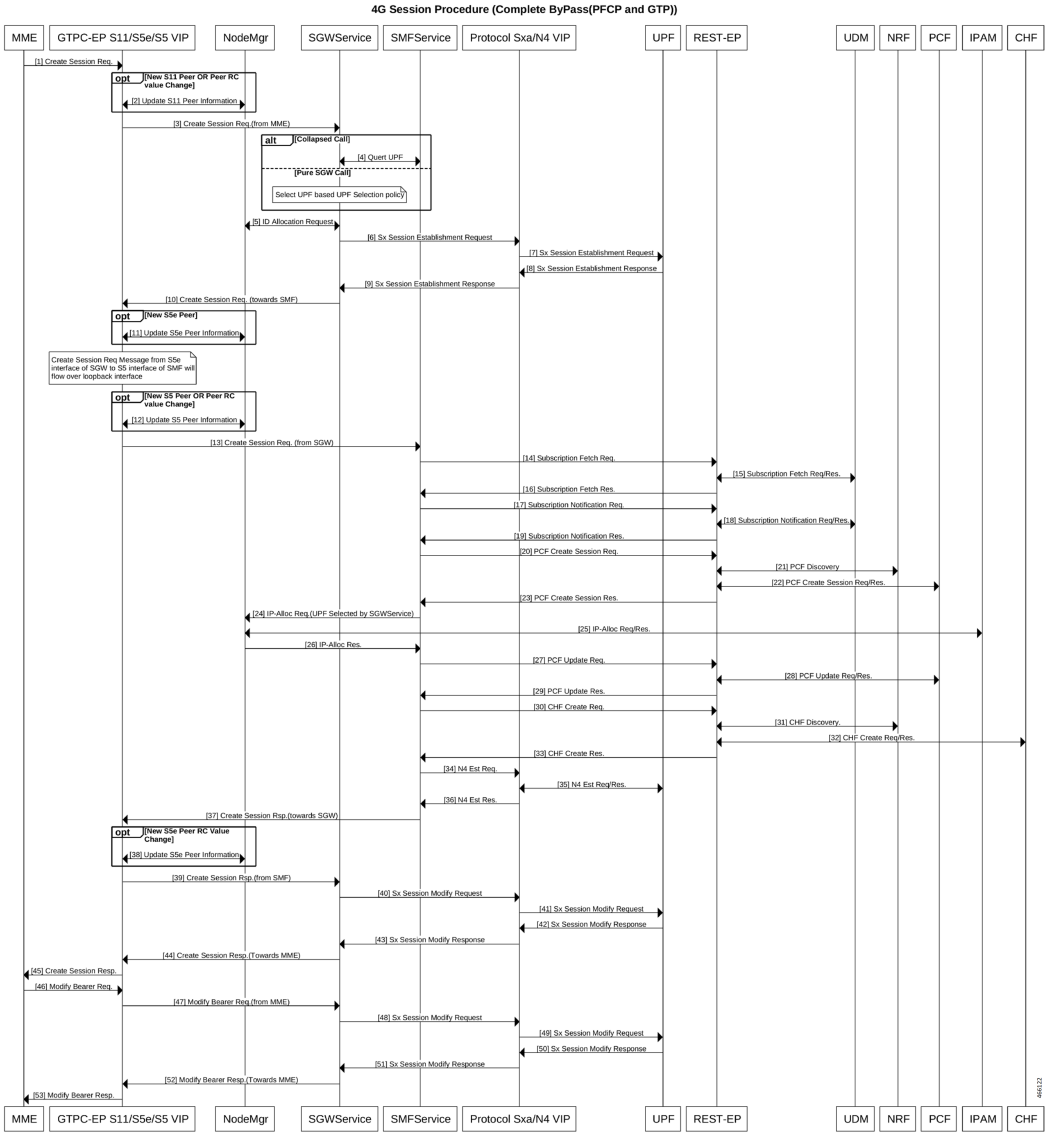


***Figure 5: 4G Session Procedure with UDP Proxy for PFCP and GTP***

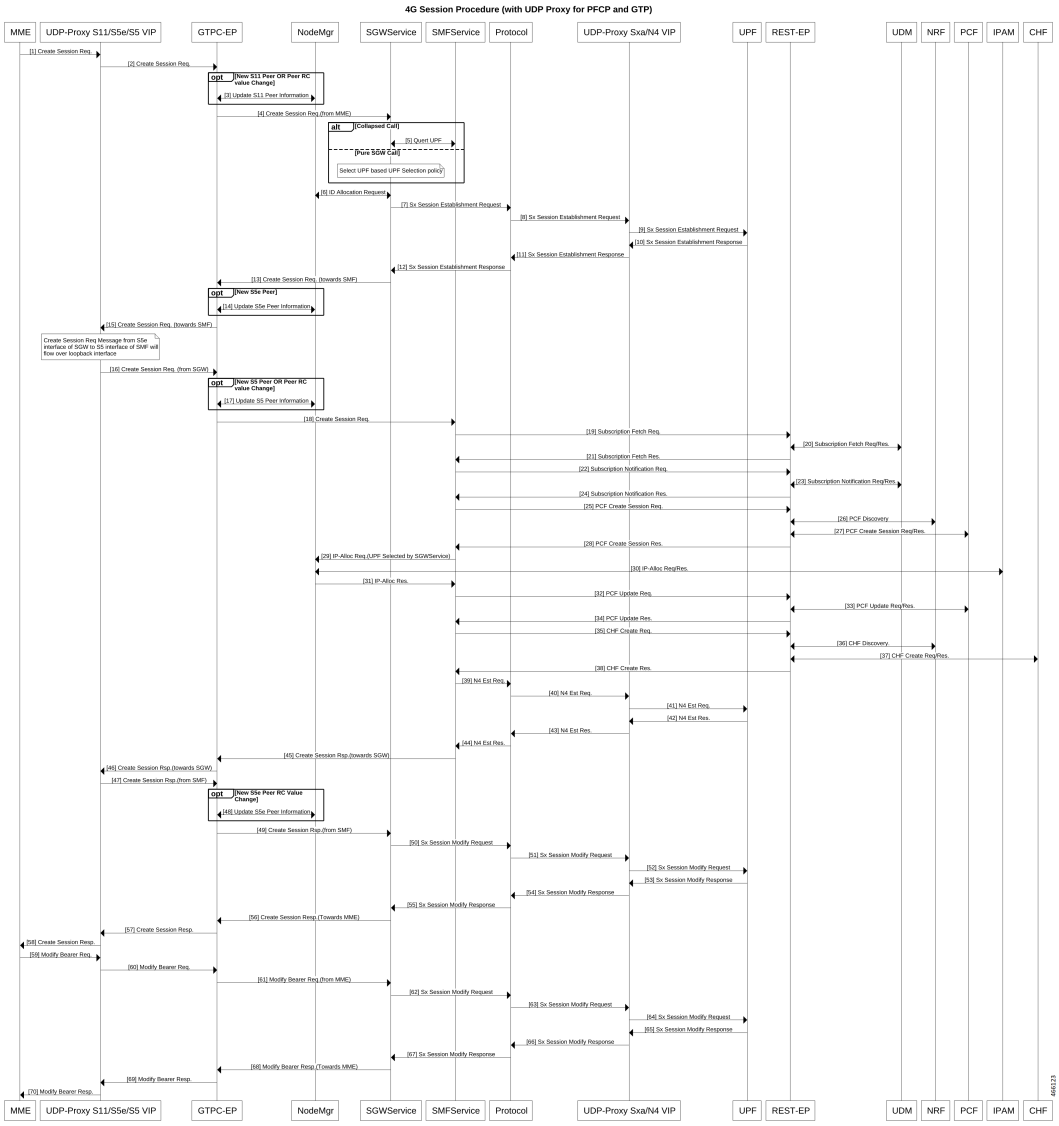


*Figure 6: End-to-End PDU Session Establishment Call Flow for Data Packets*

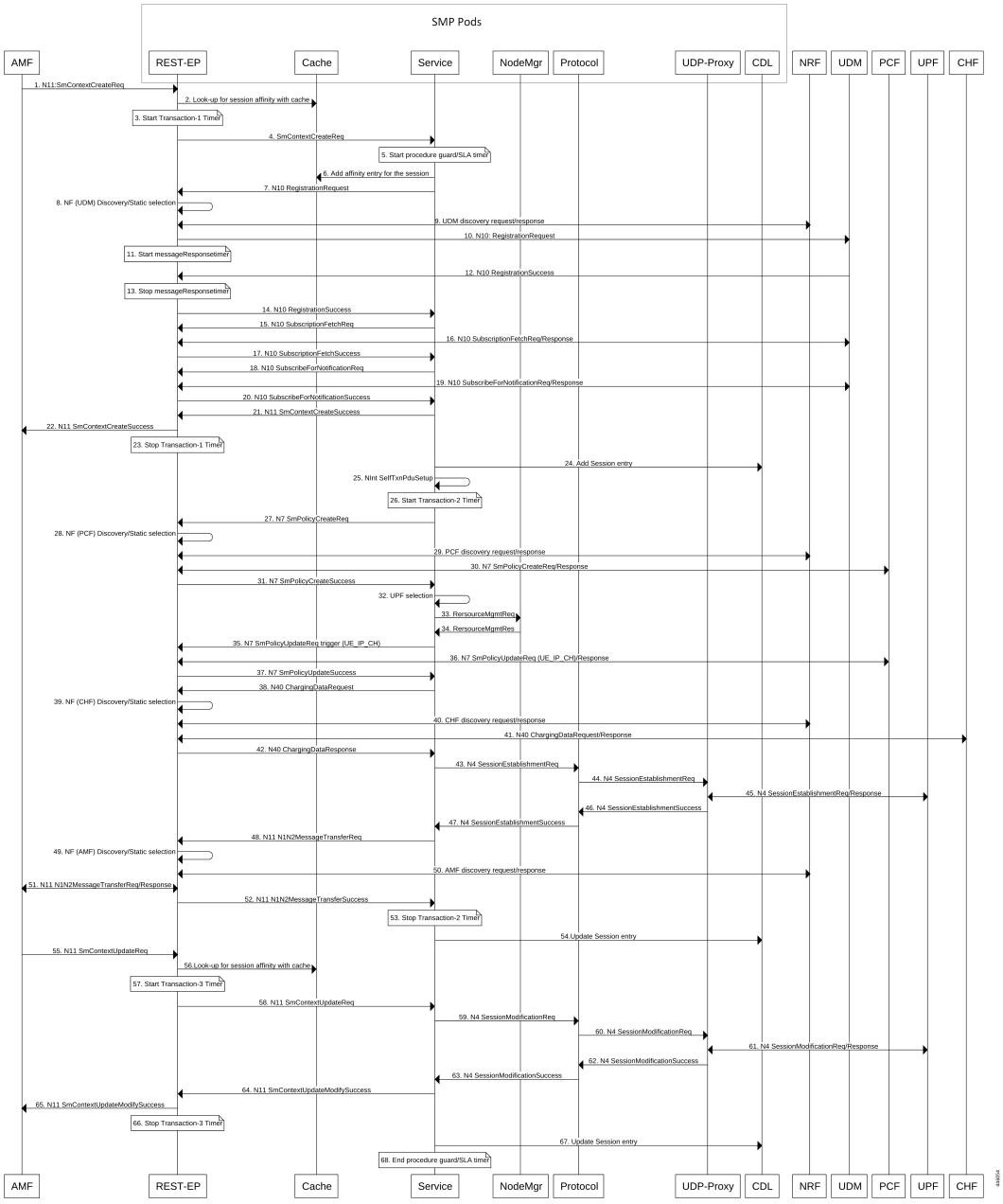



*Table 4: End-to-End PDU Session Establishment Call Flow Description*

| 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.<br>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.<br>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. |
| 21 | The SMF-service sends N11:SMContextCreateResponse to the REST-EP. |
| 22 | The REST-EP forwards the N11:SMContextCreateResponse to the AMF. |

| Step | Description |
|---|---|
| 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. |
| 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. |

| Step | Description |
|---|---|
| 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). |

# Session Affinity

The SMF supports session affinity 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.

# License Information

The SMF supports Cisco Smart Licensing. For more information, see the Smart Licensing chapter.

# Standards Compliance

Cisco SMF complies with the following 3GPP standards as per Release 15 June 2019:

- *3GPP TS 23.510, version 15.4.0*
- *3GPP TS 29.274, version 15.8.0*
- *3GPP TS 23.007, version 15.4.0*
- *3GPP TS 23.501, version 15.6.0*
- *3GPP TS 29.244, version 15.6.0*
- *3GPP TS 33.515, version 0.4.0*
- *3GPP TS 29.510, version 15.3.0*
- *3GPP TS 32.255, version 15.3.0*
- *3GPP TS 32.291, version 15.3.0*
- *3GPP TS 32.290, version 15.4.0*
- *3GPP TS 29.501, version 15.4.0*
- *3GPP TS 23.503, version 15.6.0*
- *3GPP TS 24.501, version 15.4.0*
- *3GPP TS 24.502, version 15.4.0*
- *3GPP TS 24.503, version 15.4.0*
- *3GPP TS 29.518, version 15.4.0*
- *3GPP TS 23.402, version 15.3.0*
- *3GPP TS 38.413, version 15.4.0*
- *3GPP TS 23.401, version 15.8.0*
- *3GPP TS 29.500, version 15.8.0*