5G SMF Overview

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
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

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.

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
- DNS Proxy Integration
- IP Pool Allocation per DNN
- Load-based Selection of UPF
- Protocol Data Unit RAN Tunnel Endpoint Identifier Session

- Resource Management
- Session and Service Continuity Mode

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
- Timers Support
- EPS Interworking
- Flow Failure Handling for Access and Mobility Procedures

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
- Inter gNodeB Handover
- Multiple and Virtual DNN Support
- Network-initiated Messages Support
- Policy and User Plane Management
- 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:

- SMF 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 features are related to this use case:

- NRF Discovery
- Policy and User Plane Management
- Router Solicit and Router Advertisement
- Static IP Support

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

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.

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

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

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

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

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

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

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
- Router Solicit and Router Advertisement

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

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

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
- Wi-Fi Handovers

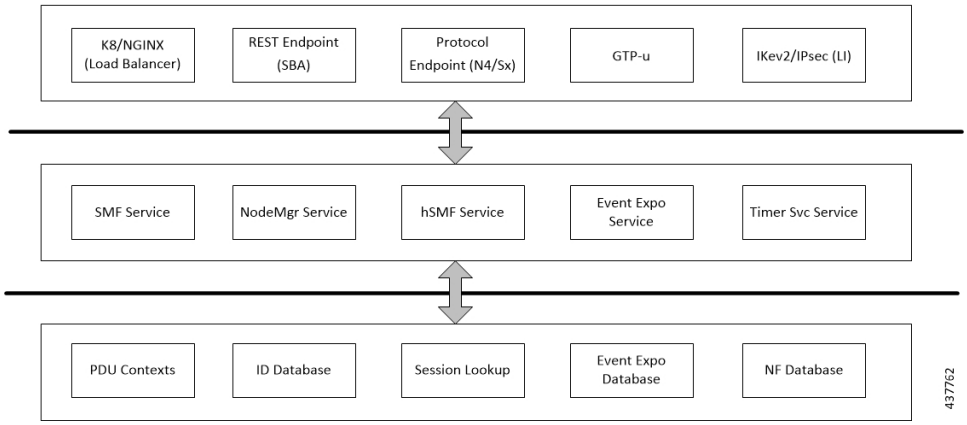
Deployment Architecture and Interfaces

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)

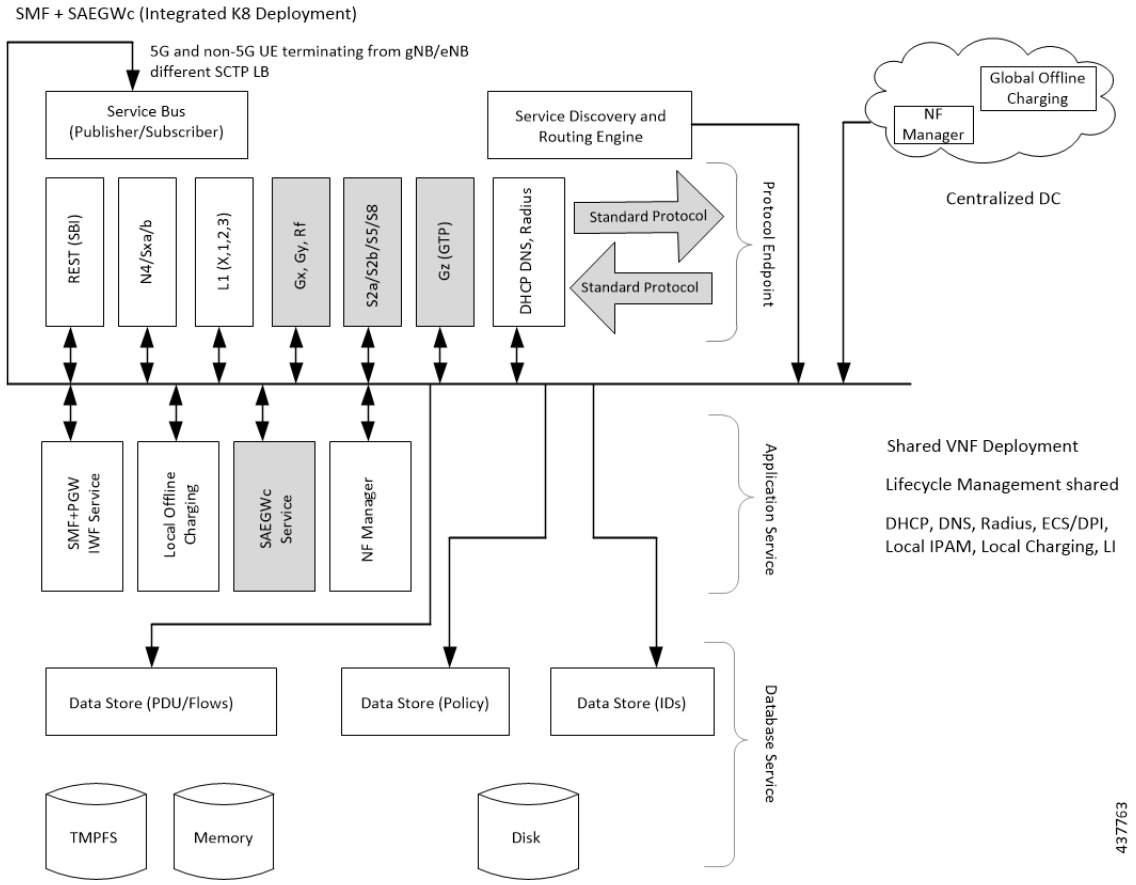
SMF Deployment

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.

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

Figure 2: 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 3: End-to-End PDU Session Establishment Call Flow for Data Packets

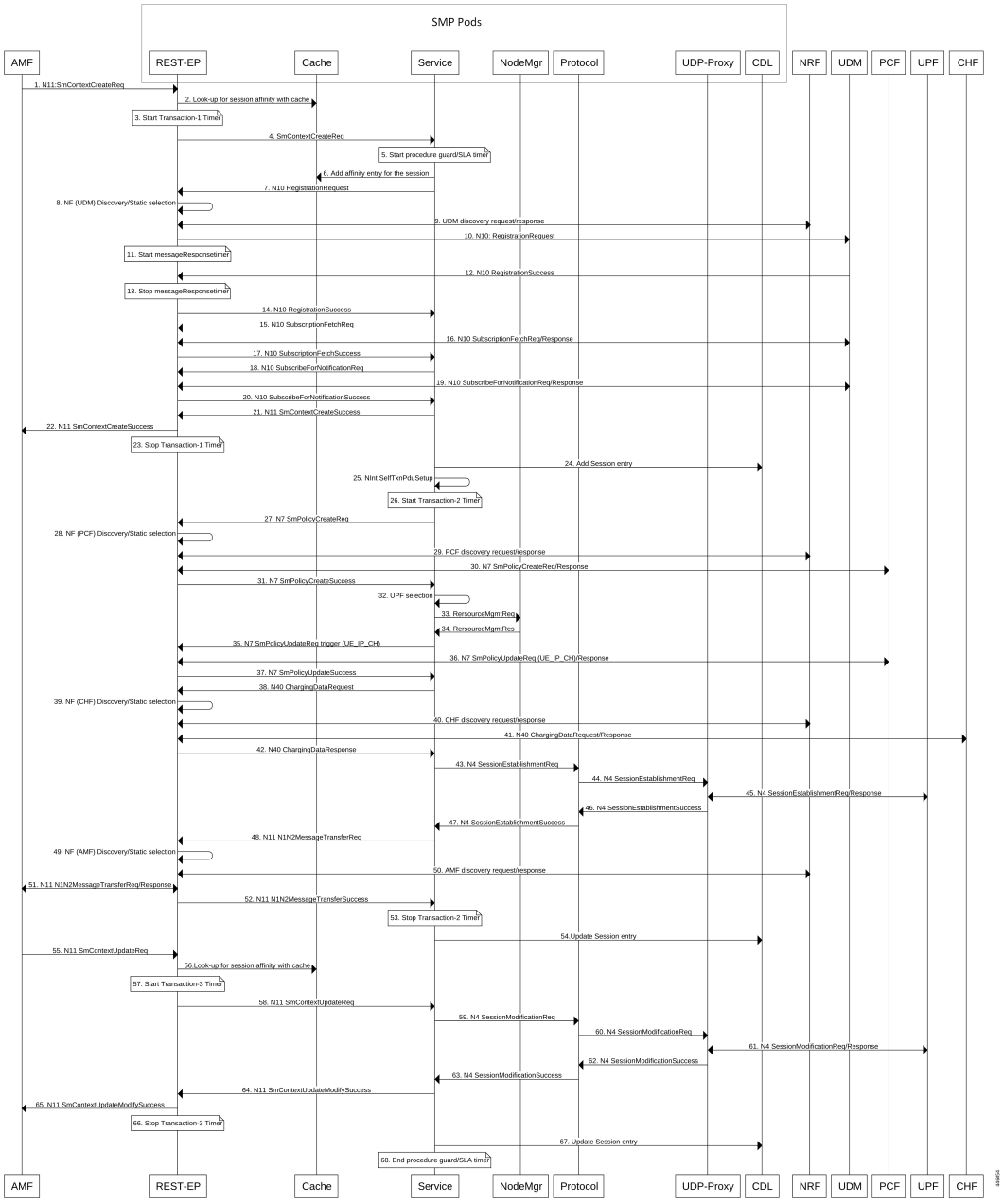


Table 3: End-to-End PDU Session Establishment Call Flow Description

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 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.