Ultra Cloud Core 5G Access and Mobility Management Function, Release 2021.04 - Configuration and Administration Guide

First Published: 2021-10-29

Last Modified: 2021-11-12

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

About this Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This preface describes the *Ultra Cloud Core 5G Access and Mobility Management Function - Configuration and Administration Guide*, the document conventions, and the customer support details.

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:`

Typeface Conventions	Description
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.
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 applicable 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**

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.

CHAPTER 1

5G Architecture

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) (for example CUPS) functionality for increased network performance and capabilities.

Control Plane Network Functions

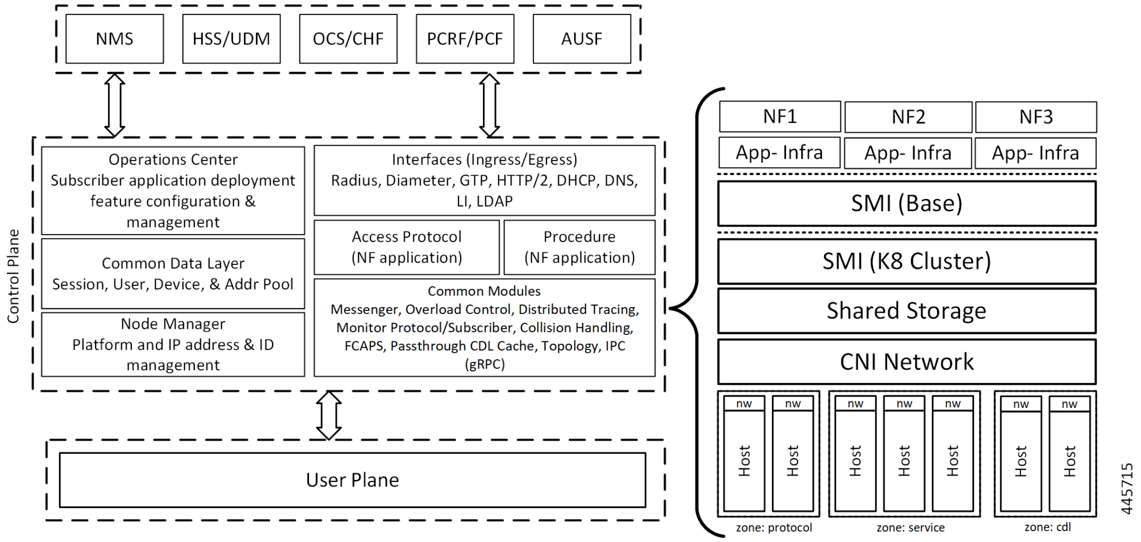
The CP-related NFs that comprise the Ultra Cloud Core are based on a common architecture designed around the following tenants:

- 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 (for example 5G, 4G, 3G, Wi-Fi, and so on).

These CP NFs are each designed as containerized applications (for example 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


NMS
HSS/UDM
OCS/CHF
PCRF/PCF
AUSF
Control Plane
Operations Center
Subscriber application deployment feature configuration & management
Interfaces (Ingress/Egress)
Radius, Diameter, GTP, HTTP/2, DHCP, DNS, LI, LDAP
Access Protocol
(NF application)
Procedure
(NF application)
Common Data Layer
Session, User, Device, & Addr Pool
Common Modules
Messenger, Overload Control, Distributed Tracing, Monitor Protocol/Subscriber, Collision Handling, FCAPS, Passthrough CDL Cache, Topology, IPC (gRPC)
Node Manager
Platform and IP address & ID management
User Plane
NF1
NF2
NF3
App- Infra
App- Infra
App- Infra
SMI (Base)
SMI (K8 Cluster)
Shared Storage
CNI Network
nw
Host
zone: protocol
zone: service
zone: cdl
445715

User Plane Network Function

The 5G UP NF within the Ultra Cloud Core is the User Plane Function. Unlike the CP-related NFs, the 5G UPF 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.

For more information on UPF, see *Ultra Cloud Core 5G UPF Configuration and Administration Guide*.

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.

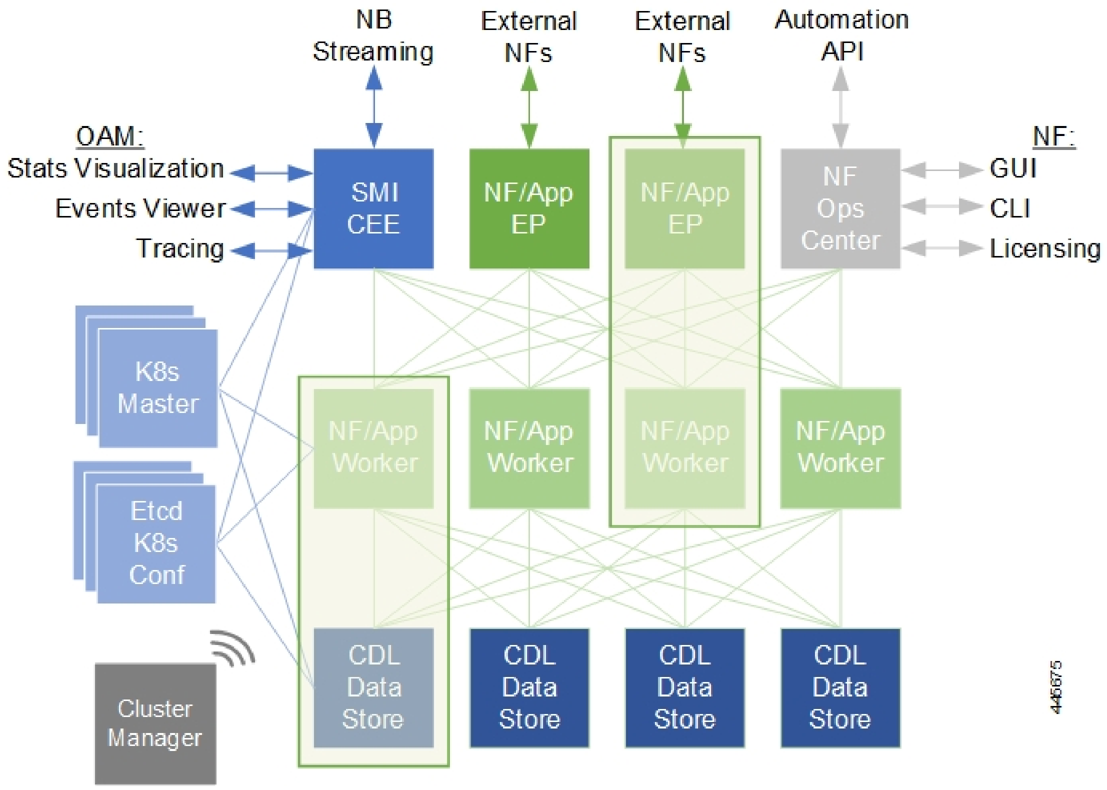
The SMI stack consists of the following:

- 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.
- NB Streaming—Provides Northbound Data Streaming service for billing and charging systems.
- 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)—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



For more information on SMI components, see Ultra Cloud Core Subscriber Microservices Infrastructure documentation— *Deployment Guide* > *Overview* chapter.

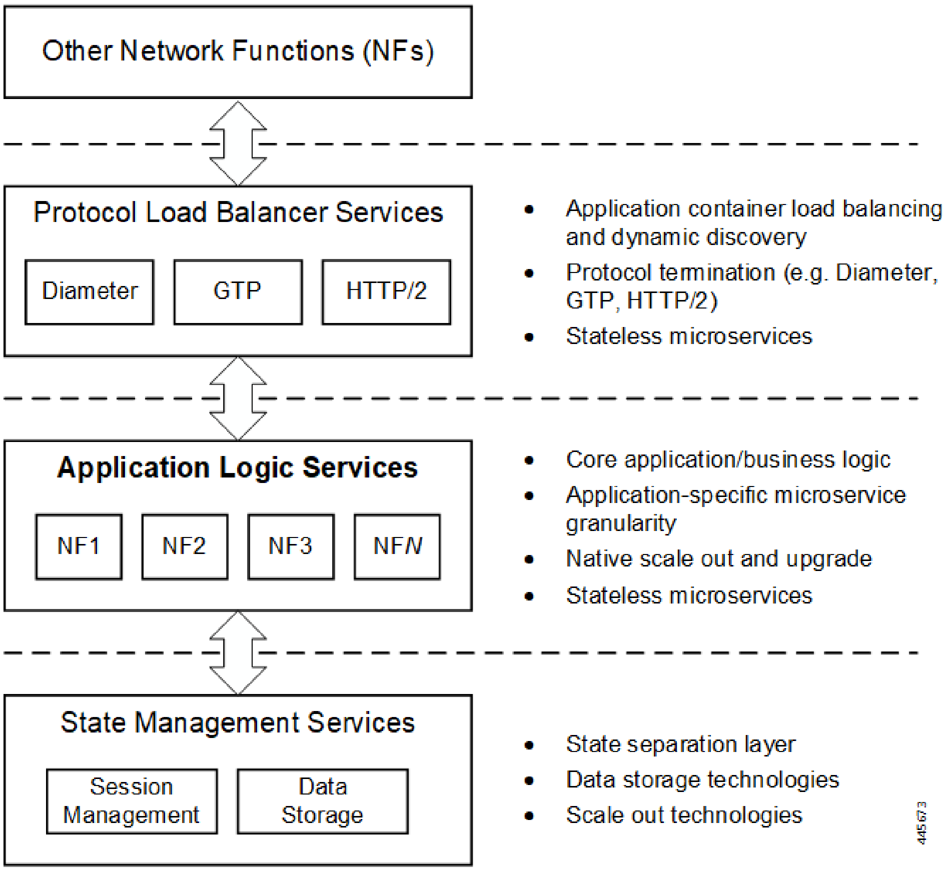
Control Plane Network Function Architecture

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:

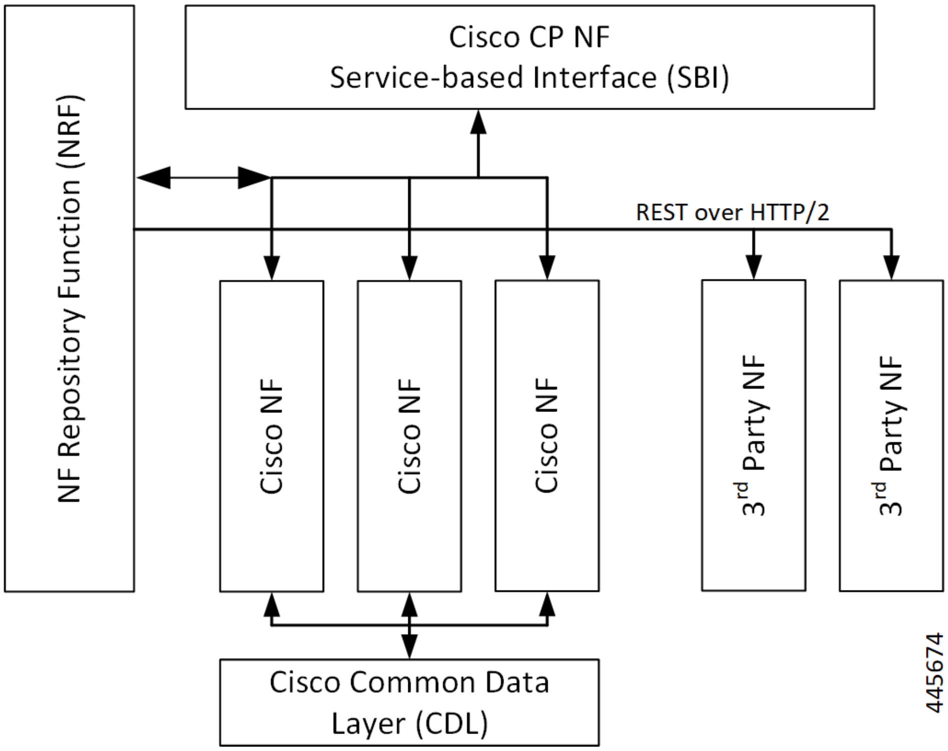
- Protocol Load Balancer Services—These are stateless microservices that are primarily responsible for dynamic discovery of application containers as well as for protocol proxy and termination. These include traditional 3GPP protocols and new protocols introduced with 5G.
- Applications Services—Responsible 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 (for example 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


Other Network Functions (NFs)
Protocol Load Balancer Services
Diameter
GTP
HTTP/2
• Application container load balancing and dynamic discovery
• Protocol termination (e.g. Diameter, GTP, HTTP/2)
• Stateless microservices
Application Logic Services
NF1
NF2
NF3
NFN
• Core application/business logic
• Application-specific microservice granularity
• Native scale out and upgrade
• Stateless microservices
State Management Services
Session Management
Data Storage
• State separation layer
• Data storage technologies
• Scale out technologies
445673

The three-tiered architecture on which Cisco's CP NFs are designed fully 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


Cisco CP NF
Service-based Interface (SBI)
NF Repository Function (NRF)
REST over HTTP/2
Cisco NF
Cisco NF
Cisco NF
3rd Party NF
3rd Party NF
Cisco Common Data Layer (CDL)
445674

For more information on the Cisco network functions, see their corresponding network function documentation.

CHAPTER 2

AMF Overview

Product Description

The Access and Mobility Management Function (AMF) is one of the control plane network functions (NF) of the 5G core network (5GC). The 5G AMF, is an evolution of 4G MME, continuing with the Control Plane and User Plane Separation, and with further simplifications like moving the Sessions Management functions to the SMF and, providing common SBA interfaces.

Figure 5: EPC with Control Plane User Plane Separation Enhancement

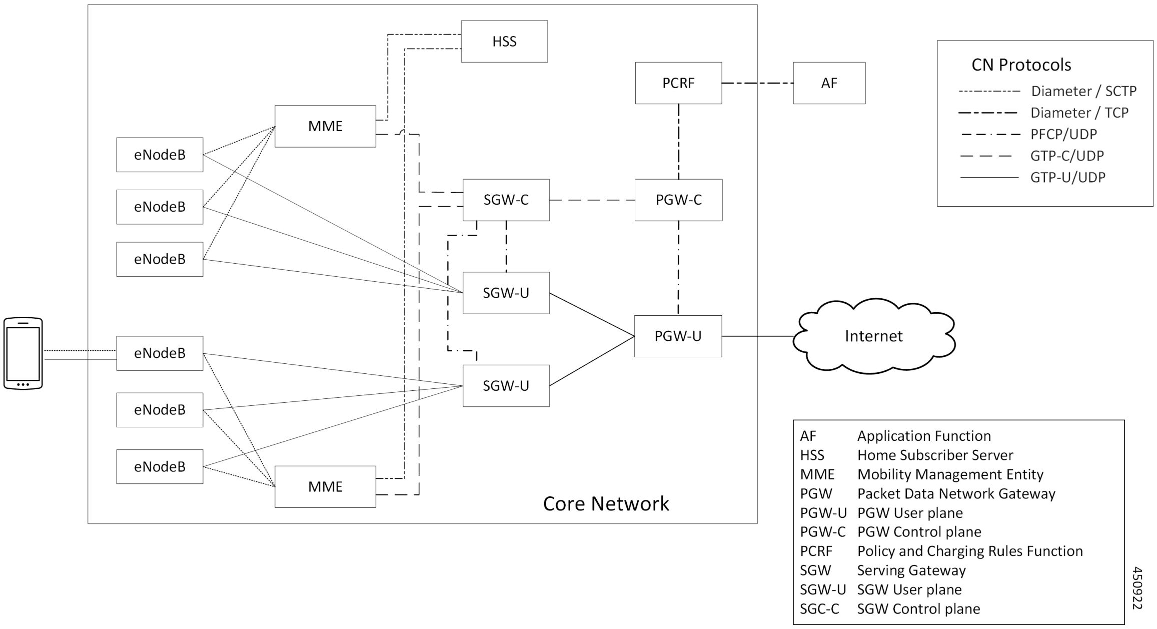
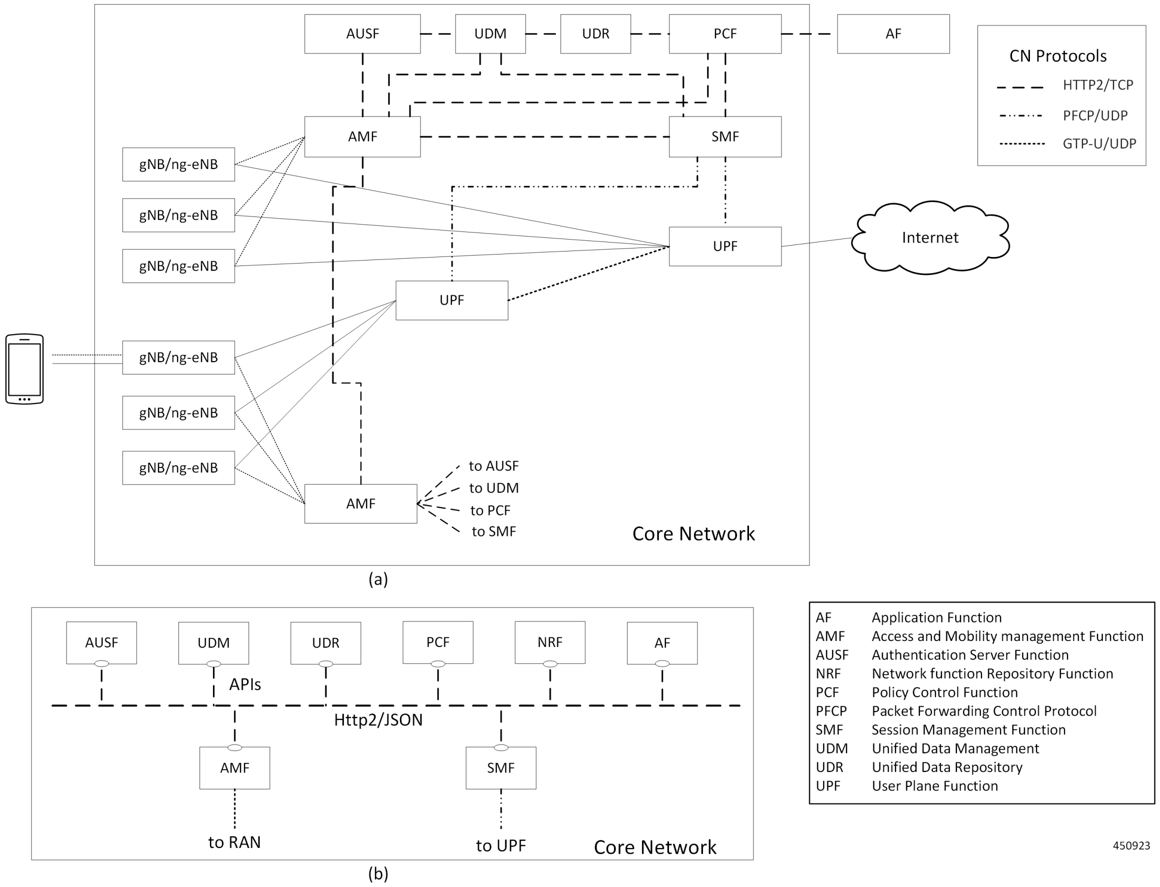


Figure 6: 5G Core Network - (a) Interface Representation, and (b) API Level Representation



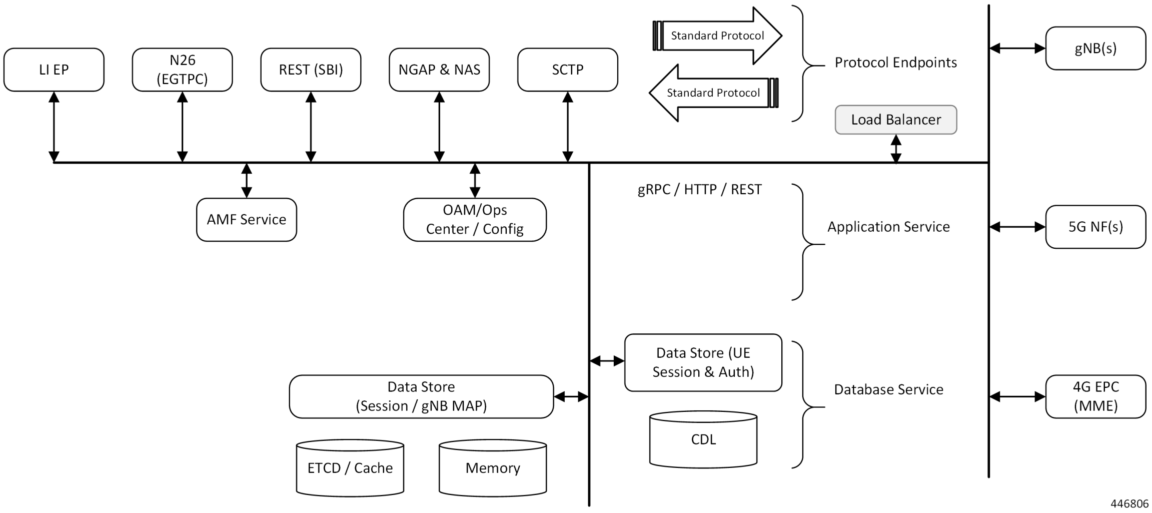
Deployment Architecture and Interfaces

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

AMF Architecture

The software architecture of the AMF is shown in the following diagram.

Figure 7: AMF Architecture



The SCTP endpoint (EP) pod type supports the SCTP interface between the AMF and gNB. Only a single SCTP EP pod is run at a time. In addition to a GUAMI, the SCTP bind address is also unique to an AMF. If multiple SCTP EPs are run, they have to bind to different SCTP addresses, at which time they would not be part of the same AMF.

The SCTP EP converts each message into a GRPC message with the SCTP Payload. Unlike TCP, SCTP messages are delimited by the protocol, so there is no other knowledge that the SCTP EP needs to figure out message boundaries.

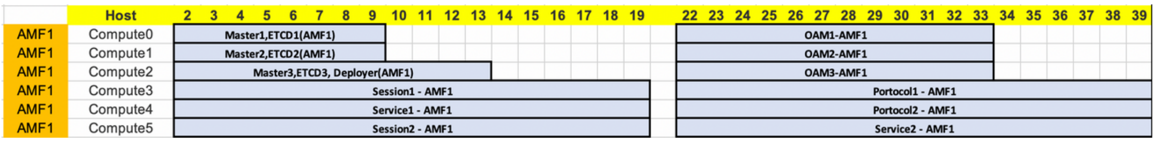
The NGAP EP or Node Manager provides termination for NGAP messages. Node Manager terminates the handling of all NGAP messages from a gNB. All messages from gNB are handled by a single Node Manager, but one Node Manager can handle messages from multiple gNBs. This allows a Node Manager to manage the state of both gNB, and one connection between a UE, gNB and AMF. If messages from the same gNB were distributed across multiple instances of Node Manager, there is no single entity in the AMF that is responsible for the state of a gNB in the AMF.

The AMF Service pods implement the logic that is necessary to provide Access and Mobility functions to the UE. This includes handling registration, handover and PDU session related procedures.

AMF Deployment

The AMF deployment supports standalone mode. In this mode, each NF together with the required microservices is deployed in a separate namespace in Kubernetes.

Figure 8: AMF Deployment



	Host	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19		22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
AMF1	Compute0	Master1,ETCD1(AMF1)																			OAM1-AMF1																	
AMF1	Compute1	Master2,ETCD2(AMF1)																			OAM2-AMF1																	
AMF1	Compute2	Master3,ETCD3, Deployer(AMF1)																			OAM3-AMF1																	
AMF1	Compute3	Session1 - AMF1																			Portocol1 - AMF1																	
AMF1	Compute4	Service1 - AMF1																			Portocol2 - AMF1																	
AMF1	Compute5	Session2 - AMF1																			Service2 - AMF1																	

Supported Interfaces

This section lists the interfaces supported between the AMF and other network functions in the 5GC.

- N1 - Reference point between UE and AMF.
- N2 - Reference point between R(AN) and AMF.
- N8 - Reference point between AMF and UDM.
- N11 (Namf) - Reference point between AMF and SMF.
- N11 (Nsmf) - Reference point between AMF and SMF.
- N12 - Reference point between AUSF and AMF.
- N14 - Reference point between AMF and AMF.
- N15 - Reference point between AMF and PCF.

Life Cycle of Control Plane Message

This call flow uses initial registration by a UE at the AMF using a GUTI assigned by a MME. All the steps in the call flow are not shown. The procedure level call flow has all the messages. The intent here is to show all the components, and the actions that are taken by each component.

Figure 9: End-to-End Registration by an UE Call Flow

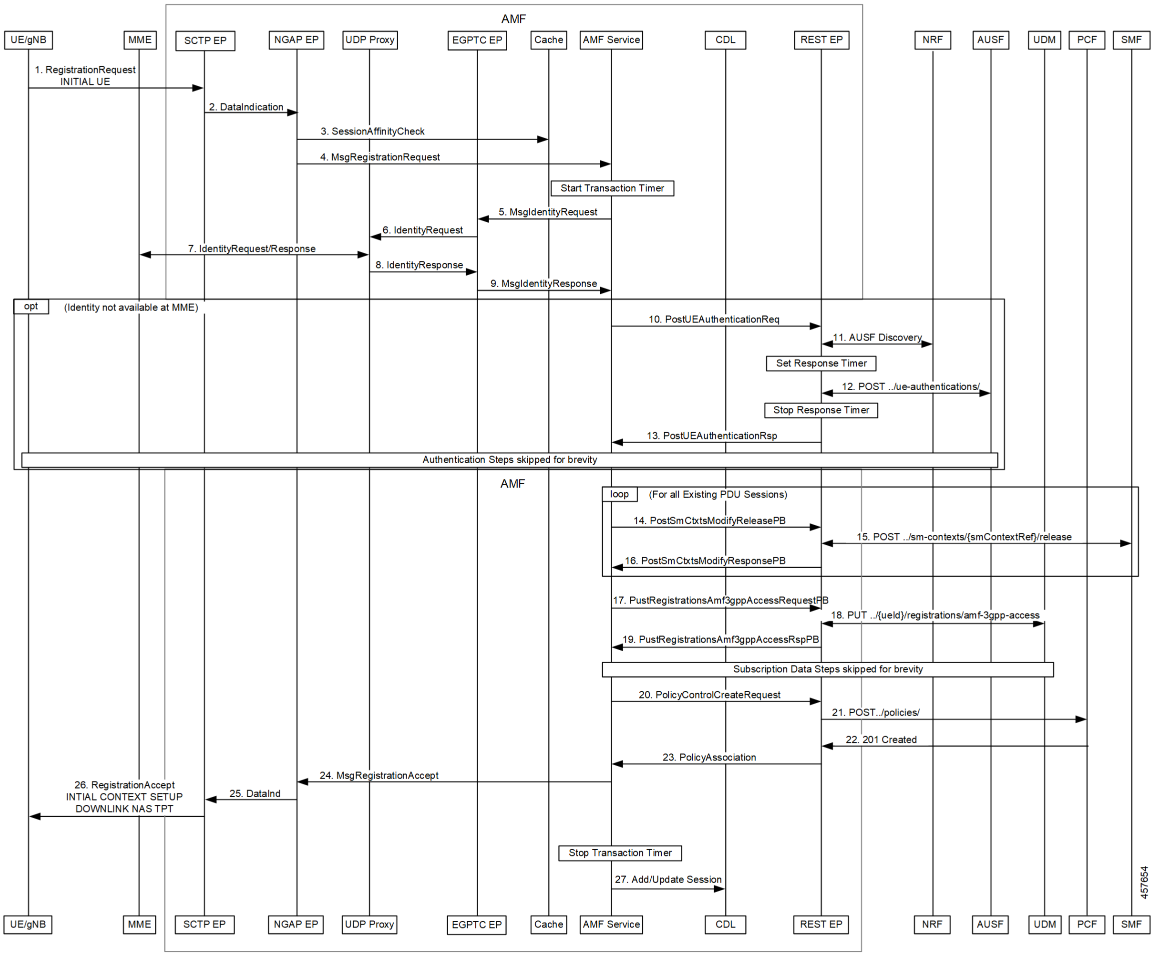

AMF
UE/gNB
MME
SCTP EP
NGAP EP
UDP Proxy
EGPTC EP
Cache
AMF Service
CDL
REST EP
NRF
AUSF
UDM
PCF
SMF
1. RegistrationRequest INITIAL UE
2. DataIndication
3. SessionAffinityCheck
4. MsgRegistrationRequest
Start Transaction Timer
5. MsgIdentityRequest
6. IdentityRequest
7. IdentityRequest/Response
8. IdentityResponse
9. MsgIdentityResponse
opt
(Identity not available at MME)
10. PostUEAuthenticationReq
11. AUSF Discovery
Set Response Timer
12. POST ../ue-authentications/
Stop Response Timer
13. PostUEAuthenticationRsp
Authentication Steps skipped for brevity
AMF
loop
(For all Existing PDU Sessions)
14. PostSmCtxtsModifyReleasePB
15. POST ../sm-contexts/{smContextRef}/release
16. PostSmCtxtsModifyResponsePB
17. PustRegistrationsAmf3gppAccessRequestPB
18. PUT ../{ueId}/registrations/amf-3gpp-access
19. PustRegistrationsAmf3gppAccessRspPB
Subscription Data Steps skipped for brevity
20. PolicyControlCreateRequest
21. POST../policies/
22. 201 Created
23. PolicyAssociation
24. MsgRegistrationAccept
25. DataInd
26. RegistrationAccept INTIAL CONTEXT SETUP DOWNLINK NAS TPT
Stop Transaction Timer
27. Add/Update Session
457654
UE/gNB
MME
SCTP EP
NGAP EP
UDP Proxy
EGPTC EP
Cache
AMF Service
CDL
REST EP
NRF
AUSF
UDM
PCF
SMF

Table 1: End-to-End Registration by an UE Call Flow Description

Step	Description
1	The UE sends a Initial Registration Request to the gNB, which sends it to the AMF in a INITIAL UE message.
2	On the AMF, the message reaches the SCTP Endpoint (EP). The SCTP EP terminates SCTP protocol, extracts the payload. It sends a DataInd GRPC message to the NGAP EP.
3	The NGAP EP parses the request. Both NGAP message parsing and NAS parsing is done by the NGAP EP. It takes the ID that came in the initial message, and checks for any existing state in any AMF service by looking up the Session Affinity Cache.
4	To optimally serve UE, AMF maintains affinity of subscriber with service pod internally. If there is session affinity information for the UE, the NGAP EP forwards the message to that AMF service pod. Otherwise, it load balances the request to any available AMF service pod.
5	The AMF service finds the MME to check the identity of the UE. Currently, the MME information is locally configured. The AMF service sends this request to the EGTPC EP.

Step	Description
6	The EGTPC EP forwards the request to the UDP proxy after a transaction ID has been allocated.
7	UDP proxy forwards this message to the MME and gets a response.
8	The response from the MME is forwarded to EGTPC EP. The EGTPC EP does the transaction matching for the request.
9	The identity response is sent to the AMF service.
10	If the security context is not present in the response from the MME, the AMF service decides to authenticate the UE. The authentication procedure is started by sending a AuthenticationRequest to the REST EP.
11	REST EP handles all the client and server requests for the AMF, and all NRF interactions. REST EP makes a query to the NRF to find the AUSF to serve the UE. In further steps, the interaction with the NRF to resolve UDM and PCF have been skipped.
12	REST EP sends an AuthenticationInformationRequest to the AUSF and gets a response.
13	The response from the AUSF is forwarded to the AMF service. The authentication procedure between the AMF service and the UE is not explained here.
14	If there is any vestigial PDU state for the UE in the SMF, the AMF clears the state. The AMF service sends a message to REST EP for each SMF that needs to be cleared of state.
15	On the REST EP, there is no NRF interaction for this message, and the REST-EP forwards this to the SMF identified in the request from the AMF service.
16	The response from the SMF is sent to the AMF service by REST EP.
17	The AMF service sends a UECM registration request to the REST EP.
18	REST EP uses the NRF to resolve UDM selection for this request and sends a request to the UDM.
19	The response from the UDM is forwarded to the AMF Service. Retrieval of subscription data information and registering for notifications for change is not explained here.
20	The AMF service checks the configuration to see if an AM policy association needs to be done for this registration, and if it is, sends a request to REST EP.
21	REST EP does NRF discovery for PCF and sends a request to the PCF.
22	Response from the PCR is forwarded to the AMF service.
23	The AMF service sends a registration accept message to NGAP.
24	NGAP encodes both the NAS message and the NGAP message and sends a message to the SCTP EP.
25	SCTP EP sends the message out to the gNB.
26	The rest of the message has been excluded.

License Information

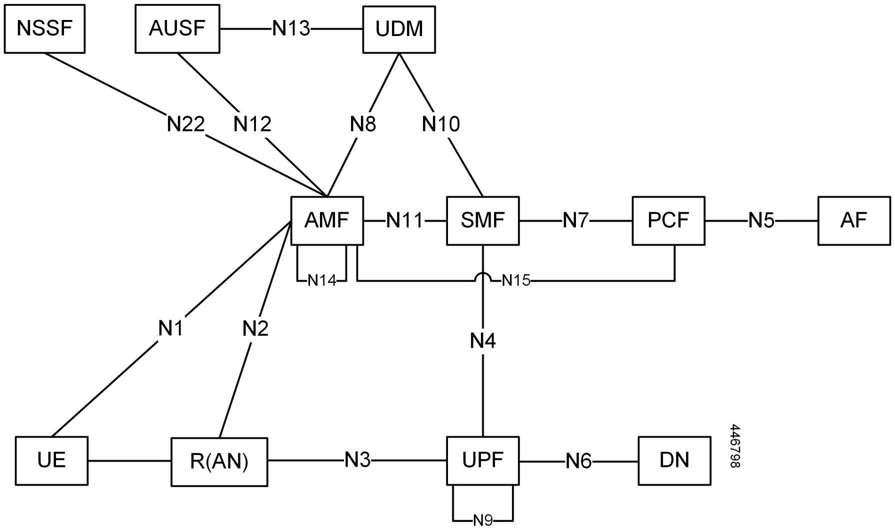
The AMF supports Cisco Smart Licensing. For more information, see the *Smart Licensing* chapter in this document.

Standards Compliance

Cisco AMF complies with the 3GPP standards.

The AMF is one of the control plane (CP) NFs of the 5G core network. The AMF uses different interfaces to communicate with the other NFs or nodes. For example, the N11 interface exists between the AMF and Session Management Function (SMF). Each of the AMF interfaces comply to a specific version of the 3GPP specification depending on the compliance version supported.

Figure 10: Interfaces



Use the following table to determine the compliance mapping for each AMF interface and the 3GPP Standards specification versions for April 2020.

Table 2: Compliance Mapping

Interface	Relationship	3GPP Specification	Version
N1	Between UE and AMF	24.501	Compliance Support: 15.4.0
N2	Between R(AN) and AMF	38.413	Compliance Support: 15.4.0
N8	Between AMF and UDM	29.503	Compliance Support: 15.4.0

Interface	Relationship	3GPP Specification	Version
N11 (Namf)	Between AMF and SMF	29.518	Compliance Support: 15.5.1
N11 (Nsmf)	Between AMF and SMF	29.502	Compliance Support: 15.4.0
N12	Between AUSF and AMF	29.509	Compliance Support: 15.4.0
N14	Between AMF and AMF	29.518	Compliance Support: 15.5.1
N15	Between AMF and PCF	29.507	Compliance Support: 15.4.0

Limitations

The AMF has the following limitations:

- Emergency services are not supported.
- VoNR is not supported.
- Location services are not supported.
- NGRAN location services are not supported.
- Notifications from UDM subscriptions are not supported.
- NSSF interactions are not supported.
- UE Policy interface is not supported.

CHAPTER 3

Deploying and Configuring AMF through Ops Center

Feature Summary and Revision History

Summary Data

Table 3: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled-Always-on
Related Documentation	Not Applicable

Revision History

Table 4: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF deployment and configuration procedure involves deploying AMF through the Subscriber Microservices Infrastructure (SMI) Cluster Deployer and configuring the settings or customizations through the AMF Ops Center which is based on the Confd CLI.

The AMF configuration includes the NRF profile data configuration and the externally visible IP addresses and ports.

AMF Ops Center

The Ops Center is a system-level infrastructure that provides the following user interface to:

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

To view the sample of the web-based CLI, use the following `show` command.

```
show running-config amf-services
amf-services am1
 amf-name              AMF
 validate-Tais         false
 relative-amf-capacity 127
 locality              LOC1
 operator-policy-name  local
 guamis mcc 123 mnc 456 region-id 1 set-id 14 pointer 3
 tai-groups test1
 exit
 slices name s1
  sst 11
  sdt 111111
 exit
 slices name s2
  sst 2
  sdt 000003
 exit
 slices name s3
  sst 3
  sdt 000004
 exit
exit
```

Prerequisites

Before deploying AMF on the SMI layer:

- Ensure that all the virtual network functions (VNFs) are deployed.

- Run the SMI synchronization operation for the AMF Ops Center and Cloud Native Common Execution Environment (CN-CEE).

AMF Sysctl Tuning Parameters and Hyperthreading Enable

In case the total number of AMF peers exceed 500, the following recommended sysctl parameter values should be configured:

```
net.ipv4.neigh.default.gc_thresh1=4096
net.ipv4.neigh.default.gc_thresh2=8192
net.ipv4.neigh.default.gc_thresh3=8192
net.ipv6.neigh.default.gc_thresh1=4096
net.ipv6.neigh.default.gc_thresh2=8192
net.ipv6.neigh.default.gc_thresh3=8192
```

1. Create a `sysctl.yaml` file and add the following contents:

   ```
   cat sysctl.yaml

   ---
   profiles:
     bios:
       name: cndp_default_settings
       description: "HyperThreading Enabled CIMC BIOS settings for CNDP"
       pids:
         ULTM-C220-M5SX-CM:
           description: "HyperThreading Enabled CIMC BIOS settings for ULTM-C220-M5SX-CM"
           tokens:
             cpuPerformance: hpc
             cpuEnergyPerformance: balanced-performance
             eppProfile: Performance
             intelHyperThreadingTech: enabled
             packageCstateLimit: C0 C1 State
             usbPortInternal: disabled
             usbPortKvm: enabled
             usbPortRear: disabled
             usbPortSdCard: disabled
     linux:
       name: sysctl_settings
       sysctl:
         net.ipv4.neigh.default.gc_thresh1: 4096
         net.ipv4.neigh.default.gc_thresh2: 8192
         net.ipv4.neigh.default.gc_thresh3: 8192
         net.ipv6.neigh.default.gc_thresh1: 4096
         net.ipv6.neigh.default.gc_thresh2: 8192
         net.ipv6.neigh.default.gc_thresh3: 8192
   ```

2. Run the following commands:

   ```
   tar -czvf sysctl.tgz ./sysctl.yaml
   ./sysctl.yaml

   sha256sum sysctl.tgz
   d3496cd26cbd7a35b06581ad4af7cd507b89000a34f6531b990edc4a14326e26  sysctl.tgz
   ```

3. Host `sysctl.yaml` file in any HTTP server accessible from the setup.

4. Add the new host-profile in cluster deployer Ops Center configuration.

Note Create a new host profile instance and link it to node. Do not update the existing one.

```
config
 software host-profile sysctl
 url http://10.84.114.208:9080/sysctl.tgz
  allow-dev-image true
 sha256          42b64b2860826136079e8c7146086fce3e98fd8933ef837e1484f2682abdb38f
 exit
commit
```

5. Link the host profile in each of the nodes using the following in cluster deployer Ops Center:

```
config
 clusters <cluster-name> nodes <node-name> host-profile sysctl
 clusters <cluster-name> nodes <node-name> os tuned enabled
commit
```

6. After cluster sync is complete, verify whether the changes are complete on each server.

```
sysctl -a | grep -i net.ipv6.neigh.default.gc_thresh

net.ipv6.neigh.default.gc_thresh1 = 4096
net.ipv6.neigh.default.gc_thresh2 = 8192
net.ipv6.neigh.default.gc_thresh3 = 8192
```

```
sysctl -a | grep -i net.ipv4.neigh.default.gc_thresh

net.ipv4.neigh.default.gc_thresh1 = 4096
net.ipv4.neigh.default.gc_thresh2 = 8192
net.ipv4.neigh.default.gc_thresh3 = 8192
```

```
lscpu | grep Thread
Thread(s) per core: 2
```

Deploying and Accessing AMF

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

Deploying AMF

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

For information on how to deploy AMF Ops Center on a vCenter environment, see *Deploying and Upgrading the Product* section in the *Ultra Cloud Core Subscriber Microservices Infrastructure — Operations Guide*.

For information on how to deploy AMF Ops Center on bare metal servers (currently Cisco UCS-C servers) environment, see *Operating the SMI Cluster Manager on Bare Metal* section in the *Ultra Cloud Core Subscriber Microservices Infrastructure — Operations Guide*.

Accessing the AMF Ops Center

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

- SSH:
  1. Log in to Master node.
  2. SSH to Ops Center pod IP using the following command:

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 AMF 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 AMF.

Configuring Ops Center

This section describes how to configure the AMF Ops center.

1. Log in to Master node.
2. SSH to Ops Center pod IP using the following command.

   ssh admin@*ops_center_pod_ip* **-p 2024**
3. Copy the contents from the configuration file and paste it in the AMF Ops Center CLI to load the configuration.

   ```
   config
     <Paste the contents from configuration file here>
     commit
     exit
   ```

Sample Configuration

You can use `show running-config` command to view the sample configuration that is provided only for reference. You must create and modify your own configuration file according to the specific needs of your deployment.

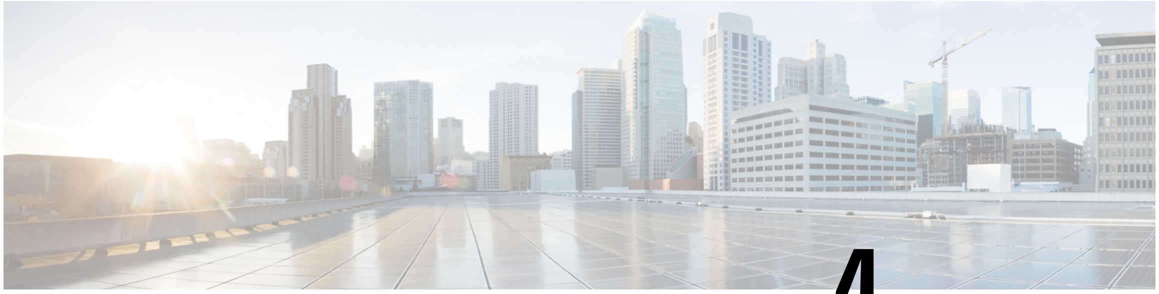
To check the sample configuration file, refer to Sample Configuration, on page 239.

Post Configuration Check

You can use the following commands from AMF Ops Center to check AMF status post configuration.

- **show system**
- **show helm**

Additionally, log in to master node and check AMF pod health and running state using **kubectl get pod -n** *amf_namespace* command.



CHAPTER 4

Smart Licensing

Feature Summary and Revision History

Summary Data

Table 5: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 6: Revision History

Revision Details	Release
First introduced.	2021.04.0

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 through Cisco Commerce Workspace (CCW) and immediately deposited into your Virtual Account for usage. This eliminates the need to install license files on every device. Smart-enabled products communicate directly to Cisco to report consumption. A single location—Cisco Software Central—is available for customers to manage Cisco software licenses. License ownership and consumption are readily available to help make a better purchase decision that is based on consumption or business need.

For more information on Cisco Smart Licensing, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html.

Cisco Software Central

Cisco Software Central (CSC) enables the management of software licenses and the smart account from a single portal. The CSC interface allows you to enable your product, manage entitlements, renew, and upgrade software. You need a functioning smart account to complete the registration process.

To access Cisco Software Central, see https://software.cisco.com.

Smart Accounts and Virtual Accounts

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

A Virtual Account exists as a sub-account within the smart account. Virtual Accounts are customer-defined based on the organizational layout, business function, geography, or any defined hierarchy. Smart account administrator creates and maintains the virtual accounts.

To learn about the set up or to manage a smart account, see https://software.cisco.com.

Requesting a Cisco Smart Account

A Cisco Smart Account is an account where smart licensing-enabled products are available. 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 the organization's smart account through Cisco Software Central.

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

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

Step 2 Log in using your credentials, and 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 authorize to create and manage product and service entitlements, users, and roles, on behalf of the 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 creates 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 is approved by the Account Domain Identifier. After the approval, you will receive an email confirmation with instructions for completing the setup process.

AMF Smart Licensing

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

Note All licenses in use are granted a 90-day evaluation period. Currently, the functionality and operation of the 5G applications is unrestricted even after the end of the evaluation period.

Software Tags and Entitlement Tags

The following sections provide information on software and entitlement tags that are created to identify, report, and enforce licenses.

Software Tags

A Software tag or a Product tag is a unique identifier that helps Smart Licensing system identify the software product family. During the addition of Smart product instance in Cisco Smart Software Manager, the Smart client uses the software/product tag for identification.

The following software tags exist for the AMF.

Product Type / Description	Software Tag
Ultra Cloud Core - Access and Mobility Management Function (AMF), Base Minimum	regid.2020-04.com.cisco.AMF,1.0_d9b74814-21c2-4667-a1b2-e27165bfc533

Entitlement Tags

An Entitlement tag is a part of the software that identifies the features that are being used in a software image. These tags underlay the communication on usage and entitlements of the software products that are installed on the devices. The entitlement tags map to both the PID license and the Software image. Every Smart-enabled PID may contain one or more entitlement tags.

The following entitlement tags identify licenses in use.

Product Type / Description	Entitlement Tag
Ultra Cloud Core - Access and Mobility Management Function (AMF), Base Minimum	regid.2020-04.com.cisco.AMF_BASE,1.0_9aa44be9-ee64-4e65-ac3d-b4040c108180

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

Configuring Smart Licensing

You can configure Smart Licensing after a new AMF 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

To set up your product and entitlement in CSC:

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. Example: AMF.
   - **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 list and select **Create New Entitlement**.
6. Select **New Entitlement** in **Add Entitlement** and enter the following details:
   - **Entitlement Name**—Specify the license entitlement name. Example: AMF_BASE.
   - **Description**—(Optional) Specify a brief 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**, enter 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**.

Registering Smart Licensing

You must register the product that is entitled to the license with CSC. To register, 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 for 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 AMF Ops Center CLI and paste the **ID token** using the following command:

    ```
    license smart register idtoken
    ```

    NOTES:

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

    Example:

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

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

   `show license all`

   Example:

```
show license all
Smart Licensing Status
=======================
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: CN-5G-NF
  Virtual Account: Default
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jun 15 12:12:38 2020 GMT
  Last Renewal Attempt: SUCCEEDED on Jun 15 12:12:38 2020 GMT
  Next Renewal Attempt: Dec 12 12:12:38 2020 GMT
  Registration Expires: Jun 15 12:02:50 2021 GMT

License Authorization:
  Status: AUTHORIZED on Jun 15 12:12:44 2020 GMT
  Last Communication Attempt: SUCCEEDED on Jun 15 12:12:44 2020 GMT
  Next Communication Attempt: Jul 15 12:12:44 2020 GMT
  Communication Deadline: Sep 13 12:09:43 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: 87 days, 10 hr, 3 min, 3 sec

License Usage
=============
License Authorization Status: AUTHORIZED as of Jun 15 12:12:44 2020 GMT

AMF_BASE (AMF_BASE)
  Description: 5G AMF Base Entitlement
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:AMF,SN:JEZZ35Q-ZF6DE7Y

Agent Version
=============
Smart Agent for Licensing: 3.1.4
```

Deregistering Smart Licensing

To deregister Smart Licensing:

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

   `license smart deregister`

   NOTES:

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

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

   `show license all`

   Example:

```
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: 84 days, 22 hr, 58 min, 0 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: 84 days, 22 hr, 58 min, 0 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 84 days, 22 hr, 58 min, 0 sec

 (AMF_BASE)
  Description: <empty>
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:AMF,SN:5DSFOZQ-DMKWHEA
```

```
Agent Version
=============
Smart Agent for Licensing: 3.1.4
```

Users without Access to CSC

The Smart License Reservation feature—Perpetual Reservation—is reserved for customers without access to CSC from their internal environments. 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 AMF Ops Center CLI, log in to AMF Ops Center CLI and use the following configuration:

```
config terminal
  license smart reservation
  exit
```

NOTES:

- **license smart reservation**—Enables license reservation.

Enabling and Generating Smart License Reservation Request Code

To enable and generate the Smart License reservation request code:

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

   ```
   config terminal
     license smart reservation
     exit
   ```

   NOTES:

   - **license smart reservation**—Enables license reservation request code.

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

   ```
   license smart reservation request
   ```

   NOTES:

   - **license smart reservation request**—Generates the license reservation request code.

   Important Copy the generated license request code from the AMF Ops Center CLI to your local machine for further use.

Example:

```
license smart reservation request
reservation-request-code CB-ZAMF:JEZZ35Q-ZF6DE7Y-A5QHppdj5-21
Message from confd-api-manager at 2020-06-15 12:18:47...
Global license change NotifyReservationInProgress reason code Success - Successful.
```

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 AMF 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 AMF 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 AMF Ops Center CLI and use the following command:

   license smart reservation install *authorization_code*

   NOTES:

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

   Example:

   ```
   license smart reservation install
   Value for 'key' (<string>): CAACfW-Wb5cMa-jEZjtU-M2KnU5-toCZBA-iaVr
   ```

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

   show license all

   Example:

   ```
   show license all

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

```
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Mon Jun 15 12:22:25 GMT 2020
  Last Renewal Attempt: None

License Authorization:
  Status: AUTHORIZED - RESERVED on Mon Jun 15 12:22:25 GMT 2020

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 87 days, 9 hr, 55 min, 44 sec

License Usage
=============
License Authorization Status:
  Status: AUTHORIZED - RESERVED on Mon Jun 15 12:22:25 GMT 2020
  Last Communication Attempt: SUCCEEDED on Jun 15 12:22:25 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

AMF_BASE (AMF_BASE)
  Description: 5G AMF Base Entitlement
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:AMF,SN:JEZZ35Q-ZF6DE7Y

Agent Version
=============
Smart Agent for Licensing: 3.1.14
```

Returning the Reserved License

To return the reserved license, use the following procedure:

1. When the license reservation authorization code is installed in the AMF Ops Center:

   a. Log in to the AMF Ops Center CLI and use the following command:

      ```
      license smart reservation return
      ```

      NOTES:

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

      Example:

```
license smart reservation return
reservation-return-code CACfWm-rdGtXu-kP1YtP-hPNELK-63EC7s-7oK
```

b. Copy the license reservation return code generated in AMF 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.

2. When the license reservation authorization code is not installed in the AMF Ops Center:

   a. Log in to the AMF 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:

   ```
   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: 84 days, 22 hr, 58 min, 0 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: 84 days, 22 hr, 58 min, 0 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 84 days, 22 hr, 58 min, 0 sec

 (AMF_BASE)
  Description: <empty>
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:AMF,SN:5DSFOZQ-DMKWHEA

Agent Version
=============
Smart Agent for Licensing: 3.1.4
```

OAM Support

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

Use the following show command to view the Smart Licensing information in the AMF 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

Pods and Services Reference

Feature Summary and Revision History

Summary Data

Table 7: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 8: Revision History

Revision Details	Release
First introduced.	2021.04.0

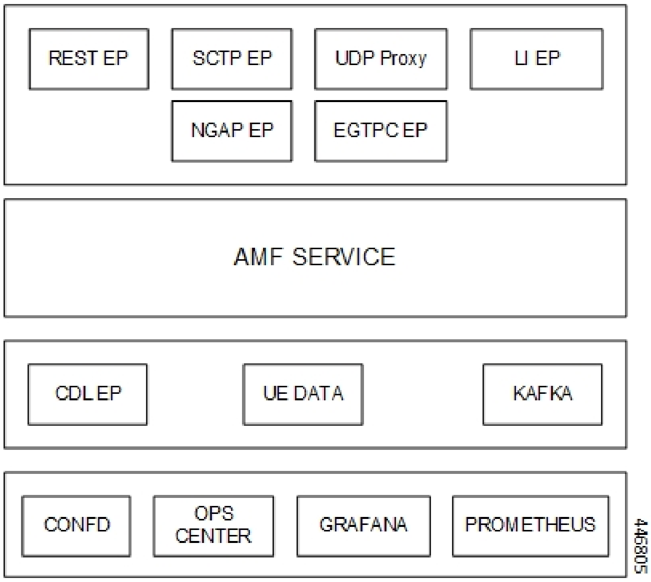
Feature Description

The AMF 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, AMF uses the construct that includes the components such as pods and services.

Depending on your deployment environment, the AMF 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 AMF 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 11: Communication Workflow of Pods



Note Currently, LI endpoint is not supported.

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 or multiple nodes 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 AMF pod names and the Kubernetes node names 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, on page 40.

Note Maximum number of pods that can be configured per node is 256.

Note In case of separate CDL deployment, CDL pods are visible under CDL namespace.

Table 9: AMF Pods

Pod Name	Description	Kubernetes Node Name
base-entitlement-amf	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-amf-etcd-cluster	Hosts the etcd for the AMF application to store information, such as pod instances, leader information, NF-UUID, endpoints, and so on.	OAM
georeplication	Contains business logic for Geographic Redundancy (Currently, GR is not fully supported in AMF).	Protocol
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-amf	Contains the default dashboard of AMF-service metrics in Grafana.	OAM
gtpc-ep-n0	Operates as GTPC endpoint of AMF.	Protocol
kafka	Hosts the Kafka details for the CDL replication.	Protocol

Pod Name	Description	Kubernetes Node Name
nodemgr-n0	Performs node level interactions, such as N4 link establishment, management (heart-beat). It also generates unique identifiers, such as UE IP address, SEID, CHF-ID, Resource URI.	Service
oam-pod	Operates as the pod to facilitate Ops Center actions, such as show commands, configuration commands, monitor protocol monitor subscriber, and so on.	OAM
ops-center-amf-ops-center	Acts as the AMF Ops Center.	OAM
smart-agent-amf-ops-center	Operates as the utility pod for the AMF Ops Center.	OAM
amf-amf-service-0	Contains main business logic of AMF.	Service
amf-amf-rest-ep-0	Operates as REST endpoint of AMF for HTTP2 communication.	Protocol
amf-amf-protocol-ep	Processes NGAP/NAS Protocol Messages.	Protocol
amf-amf-sctp-lb	Operates as SCTP end point for AMF.	Protocol
amf-udp-proxy-0	Operates as proxy for all UDP messages. Owns UDP client and server functionalities.	Protocol
swift-amf-ops-center	Operates as the utility pod for the AMF Ops Center.	OAM
zookeeper	Assists Kafka for topology management.	OAM

Services

The AMF configuration is composed of several microservices that run on a set of discrete pods. Microservices are deployed during the AMF deployment. AMF 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 AMF services and the pod on which they run.

Note In case of separate CDL deployment, CDL related services are visible under CDL namespace.

Table 10: AMF Services and Pods

Service Name	Pod Name	Description
alert-frwd-ops-center	ops-center-amf-ops-center	Responsible for forwarding SNMP alerts.
amf-gosctp-lb	amf-gosctp-lb	Responsible for receving incoming traffic over SCTP from N1 interface.
amf-nrf-service	amf-rest-ep	Responsible for providing API for NRF CLIs.
amf-protocol-ep	amf-protocol-ep	Responsible for inter-pod communication with amf-protocol-ep pod.
amf-rest-ep	amf-rest-ep	Responsible for inter-pod communication with amf-rest-ep pod.
amf-sbi-service	amf-rest-ep	Responsible for routing incoming SBI messages to REST-EP pods.
amf-service	amf-service	Responsible for inter-pod communication with amf-service pod.
base-entitlement-amf	ops-center-amf-ops-center	Supports Smart Licensing feature.
bgpspeaker-pod	georeplication-pod-0	Responsible for providing Geo replication support.
datastore-ep-session	cdl-ep-session	Responsible for the CDL session.
datastore-notification-ep	amf-rest-ep	Responsible for sending the notifications from the CDL to the smf-service through amf-rest-ep.
datastore-tls-ep-session	cdl-ep-session	Responsible for the secure CDL connection.
documentation	documentation	Responsible for the AMF documents.
etcd	etcd-cluster	Responsible for pod discovery within the namespace.
etcd-amf-ins1-etcd-cluster-0	etcd-cluster	Responsible for synchronization of data among the ETCD cluster.
etcd-amf-ins1-etcd-cluster-1	etcd-cluster	Responsible for synchronization of data among the ETCD cluster.

Service Name	Pod Name	Description
etcd-amf-ins1-etcd-cluster-2	etcd-cluster	Responsible for synchronization of data among the ETCD cluster.
grafana-dashboard-amf	grafana-dashboard-amf	Responsible for the default dashboard of AMF-service metrics in Grafana.
grafana-dashboard-app-infra-amf	grafana-dashboard-app-infra	Responsible for the default dashboard of App-Infra metrics in Grafana.
grafana-dashboard-cdl-cdl-amf	grafana-dashboard-cdl	Responsible for the default dashboard of CDL metrics in Grafana.
grafana-dashboard-etcd-amf	grafana-dashboard-etcd	Responsible for the default dashboard of ETCD metrics in Grafana.
gtpc-ep	gtpc-ep	Responsible for inter-pod communication with GTP-C pod.
kafka	kafka	Processes the Kafka messages.
local-ldap-proxy-amf-ins1-ops-center	ops-center-amf-ops-center	Responsible for leveraging Ops Center credentials by other applications, such as Grafana.
netconf-ops-center-amf-ins1-ops-center	ops-center-amf-ops-center	Responsible for providing/exposing netconf interface to configure AMF.
nodemgr	nodemgr	Responsible for inter-pod communication with nodemgr pod.
oam-pod	oam-pod	Responsible to facilitate Exec commands on the Ops Center.
ops-center-amf-ops-center	ops-center-amf-ops-center	Operates as the utility pod for the SMF Ops Center.
prometheus-rules-etcd	prometheus-rules-etcd	Responsible for the default Prometheus rules of ETCD in Prometheus.
smart-agent-amf-ops-center	smart-agent-amf-ops-center	Responsible for smart licensing.
ssh-ops-center-amf-ops-center	ops-center-amf-ops-center	To access AMF Ops Center using SSH IP.
zookeeper	zookeeper	Assists Kafka for topology management.

Service Name	Pod Name	Description
zookeeper-service	zookeeper	Assists Kafka for topology management.

Open Ports and Services

The AMF uses different ports for communication. The following table describes the default open ports and the associated services.

Table 11: Open Ports and Services

Port	Service	Usage
22	SSH	SMI uses TCP port to communicate with the virtual machines.
80	HTTP	SMI uses TCP port for providing Web access to CLI, Documentation, and TAC.
443	SSL/HTTP	SMI uses TCP port for providing Web access to CLI, Documentation, and TAC.
6443	HTTP	SMI uses port to communicate with the Kubernetes API server.
9100	jetdirect	SMI uses TCP port to communicate with the Node Exporter. Node Exporter is a Prometheus exporter for hardware and OS metrics with pluggable metric collectors. It allows you to measure various machine resources, such as memory, disk, and CPU utilization.
10250	SSL/HTTP	SMI uses TCP port to communicate with Kubelet. Kubelet is the lowest level component in Kubernetes. It is responsible for what is running on an individual machine. It is a process watcher or supervisor focused on active container. It ensures the specified containers are up and running.
10251	SSL/HTTP	SMI uses TCP port to interact with the Kube scheduler. Kube scheduler is the default scheduler for Kubernetes and runs as part of the control plane. A scheduler watches for newly created pods that have no node assigned. For every pod that the scheduler discovers, the scheduler becomes responsible for finding the best node for that pod to run on.
10252	apollo-relay	SMI uses this TCP port to interact with the Kube controller. The Kubernetes controller manager is a daemon that embeds the core control loops shipped with Kubernetes. The controller is a control loop that watches the shared state of the cluster through the API server and makes changes to move the current state to the desired state.

Port	Service	Usage
10256	HTTP	SMI uses TCP port to interact with the Kube proxy. Kube proxy is a network proxy that runs on each node in your cluster. Kube proxy maintains network rules on nodes. These network rules allow network communication to your pods from network sessions inside or outside of your cluster.
2024	SSH	AMF Ops Center uses this port to provide the ConfD CLI access.
9090	HTTP	AMF REST endpoint pods use this port to expose the APIs to support NRF interface specific CLIs.
8090	HTTP	AMF REST endpoint pods use this port for routing incoming SBI messages to REST-EP pods.
8890	gRPC/HTTP	AMF REST endpoint pods use this port to receive timer notification from CDL.

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.

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

```
config
  k8 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
    sctp-layer
      key key_value
      value value
      end
```

NOTES:

- **label { cdl-layer { key** *key_value* **| value** *value* **}**—Specify the key value pair for CDL.
- **oam-layer { key** *key_value* **| value** *value* **}**—Specify the key value pair for OAM layer.
- **protocol-layer { key** *key_value* **| value** *value* **}**—Specify the key value pair for protocol layer.
- **service-layer { key** *key_value* **| value** *value* **}**—Specify the key value pair for the service layer.
- **sctp-layer { key** *key_value* **| value** *value* **}**—Specify the key value pair for the SCTP layer.

Note If you opt not to configure the labels, then AMF assumes the labels with the default key-value pair.

Viewing the Pod Details and Status

If the service requires additional pods, AMF creates and deploys the pods. You can view the list of pods that are participating in your deployment through the AMF Ops Center. You can run the kubectl command from the master node to manage the Kubernetes resources.

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

  kubectl get pods -n *amf_namespace 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.

  Sample Output:

```
kubectl get pod -n amf-ins1 cache-pod-0 -o yaml
apiVersion: v1
kind: Pod
metadata:
  annotations:
    cni.projectcalico.org/podIP: 41.41.13.51/32
    cni.projectcalico.org/podIPs: 41.41.13.51/32,4141:4141::d32/128
    prometheus.io/port: "10080"
    prometheus.io/scrape: "true"
    sidecar.istio.io/inject: "false"
  creationTimestamp: "2021-10-16T18:03:32Z"
  generateName: cache-pod-
  labels:
    component: cache-pod
    controller-revision-hash: cache-pod-56dc45d7df
    release: amf-ins1-infra-charts
    statefulset.kubernetes.io/pod-name: cache-pod-0
  name: cache-pod-0
  namespace: amf-ins1
  ownerReferences:
  - apiVersion: apps/v1
    blockOwnerDeletion: true
    controller: true
    kind: StatefulSet
    name: cache-pod
    uid: 18dfdb38-ca20-47ab-b525-770be9ace57c
  resourceVersion: "5770907"
  uid: 088c4f8d-143b-4096-ad03-f95409c16db9
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
        - matchExpressions:
          - key: smi.cisco.com/node-type-2
            operator: In
            values:
            - protocol
.
.
.
status:
  conditions:
  - lastProbeTime: null
    lastTransitionTime: "2021-10-16T18:03:47Z"
    status: "True"
    type: Initialized
  - lastProbeTime: null
    lastTransitionTime: "2021-10-16T18:04:52Z"
    status: "True"
    type: Ready
  - lastProbeTime: null
    lastTransitionTime: "2021-10-16T18:04:52Z"
    status: "True"
    type: ContainersReady
  - lastProbeTime: null
    lastTransitionTime: "2021-10-16T18:03:32Z"
    status: "True"
    type: PodScheduled
  containerStatuses:
  - containerID: docker://68f5c45ed73ee311a05a32be4fadca0cb9fda0742a01d303fe5115dfa7573a48

    image:
docker.171.11.189.41.nip.io/amf.2021.04.m0.i80/mobile-cnat-app-infra/cache-pod/main/cache_pod:0.1.0-32e359a

    imageID:
docker-pullable://docker.171.11.189.41.nip.io/amf.2021.04.m0.i80/mobile-cnat-app-infra/cache-pod/main/cache_pod@sha256:d2c82e1af506cf92c04d93f40ef8a1dfcf830d457bfeab04d8aba7c63e894

    lastState: {}
    name: cache-pod
    ready: true
    restartCount: 0
    started: true
    state:
      running:
        startedAt: "2021-10-16T18:03:49Z"
  hostIP: 171.11.189.42
  phase: Running
  podIP: 41.41.13.51
  podIPs:
  - ip: 41.41.13.51
  - ip: 4141:4141::d32
  qosClass: Burstable
  startTime: "2021-10-16T18:03:47Z"
```

- To view the summary of the pod details, use the following command.

  kubectl get pods -n *amf_namespace* **-o wide**

  Sample Output:

```
kubectl get pod -n amf-ins1 -o wide
NAME                                                  READY   STATUS    RESTARTS   AGE
   IP               NODE                       NOMINATED NODE   READINESS GATES
amf-ins1-amf-gosctp-lb-0                              1/1     Running   0          37h
   171.11.189.42   amf-cndp-b19-4-master-1   <none>           <none>
amf-ins1-amf-gosctp-lb-1                              1/1     Running   0          37h
   171.11.189.43   amf-cndp-b19-4-master-2   <none>           <none>
amf-ins1-amf-protocol-ep-0                            2/2     Running   1          37h
   41.41.13.137    amf-cndp-b19-4-master-1   <none>           <none>
amf-ins1-amf-protocol-ep-1                            2/2     Running   1          37h
   41.41.43.4      amf-cndp-b19-4-master-2   <none>           <none>
amf-ins1-amf-rest-ep-0                                2/2     Running   1          37h
   41.41.13.189    amf-cndp-b19-4-master-1   <none>           <none>
amf-ins1-amf-rest-ep-1                                2/2     Running   1          37h
   41.41.43.46     amf-cndp-b19-4-master-2   <none>           <none>
amf-service-n0-0                                      2/2     Running   1          37h
   41.41.13.135    amf-cndp-b19-4-master-1   <none>           <none>
amf-service-n0-1                                      2/2     Running   1          37h
   41.41.13.49     amf-cndp-b19-4-master-1   <none>           <none>
amf-service-n1-0                                      2/2     Running   0          37h
   41.41.59.62     amf-cndp-b19-4-master-3   <none>           <none>
amf-service-n1-1                                      2/2     Running   1          37h
   41.41.59.19     amf-cndp-b19-4-master-3   <none>           <none>
base-entitlement-amf-6cf5fb484d-4w7cg                 1/1     Running   0          37h
   41.41.59.51     amf-cndp-b19-4-master-3   <none>           <none>
cache-pod-0                                           1/1     Running   0          37h
   41.41.13.51     amf-cndp-b19-4-master-1   <none>           <none>
cache-pod-1                                           1/1     Running   0          36h
   41.41.43.49     amf-cndp-b19-4-master-2   <none>           <none>
documentation-556f8dcc5c-pnlnn                        1/1     Running   0          37h
   41.41.59.61     amf-cndp-b19-4-master-3   <none>           <none>
etcd-amf-ins1-etcd-cluster-0                          2/2     Running   2          37h
   41.41.13.173    amf-cndp-b19-4-master-1   <none>           <none>
etcd-amf-ins1-etcd-cluster-1                          2/2     Running   0          37h
   41.41.43.5      amf-cndp-b19-4-master-2   <none>           <none>
etcd-amf-ins1-etcd-cluster-2                          2/2     Running   0          37h
   41.41.59.8      amf-cndp-b19-4-master-3   <none>           <none>
georeplication-pod-0                                  1/1     Running   0          37h
   171.11.189.43   amf-cndp-b19-4-master-2   <none>           <none>
grafana-dashboard-amf-695457b77d-gdhf5                1/1     Running   0          37h
   41.41.13.52     amf-cndp-b19-4-master-1   <none>           <none>
grafana-dashboard-app-infra-amf-ins1-cfb8b656d-54s9z   1/1     Running   0          37h
   41.41.13.150    amf-cndp-b19-4-master-1   <none>           <none>
grafana-dashboard-etcd-amf-ins1-5c7d9d75db-729sl      1/1     Running   0          37h
   41.41.13.191    amf-cndp-b19-4-master-1   <none>           <none>
gtpc-ep-n0-0                                          2/2     Running   1          37h
   41.41.13.160    amf-cndp-b19-4-master-1   <none>           <none>
li-ep-n0-0                                            2/2     Running   0          37h
   41.41.13.30     amf-cndp-b19-4-master-1   <none>           <none>
li-ep-n0-1                                            2/2     Running   0          37h
   41.41.43.29     amf-cndp-b19-4-master-2   <none>           <none>
nodemgr-n0-0                                          2/2     Running   1          37h
   41.41.13.144    amf-cndp-b19-4-master-1   <none>           <none>
nodemgr-n0-1                                          2/2     Running   1          37h
   41.41.59.36     amf-cndp-b19-4-master-3   <none>           <none>
```

```
oam-pod-0                                            2/2     Running   1          37h
   41.41.13.133    amf-cndp-b19-4-master-1   <none>          <none>
ops-center-amf-ins1-ops-center-5bf9df44b6-pn5ds       5/5     Running   0          36h
   41.41.59.41     amf-cndp-b19-4-master-3   <none>          <none>
prometheus-rules-etcd-796ffd6cdf-w48rj                1/1     Running   0          37h
   41.41.13.169    amf-cndp-b19-4-master-1   <none>          <none>
smart-agent-amf-ins1-ops-center-8475b6559d-q9gb2      1/1     Running   0          37h
   41.41.13.152    amf-cndp-b19-4-master-1   <none>          <none>
udp-proxy-0                                          1/1     Running   0          37h
   171.11.189.42   amf-cndp-b19-4-master-1   <none>          <none>
udp-proxy-1                                          1/1     Running   0          37h
   171.11.189.43   amf-cndp-b19-4-master-2   <none>          <none>
```

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 12: 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.

Viewing the Service Details

To view service summary, use the following command.

kubectl get svc -n *amf_namespace*

Sample Output:

```
kubectl get svc -n amf-ins1
NAME                                    TYPE        CLUSTER-IP      EXTERNAL-IP    PORT(S)
                                         AGE
alert-frwd-ops-center                  ClusterIP   46.46.34.111    <none>         8080/TCP
                                        29d
amf-gosctp-lb                          ClusterIP   46.46.149.12    <none>         7084/TCP
                                        36h
```

```
amf-nrf-service                        ClusterIP   46.46.227.164   172.16.186.4   9090/TCP
                                        36h
amf-protocol-ep                         ClusterIP   46.46.155.167   <none>
9003/TCP,8080/TCP                              36h
amf-rest-ep                             ClusterIP   46.46.171.99    <none>
9003/TCP,8080/TCP,9201/TCP                     36h
amf-sbi-service                        ClusterIP   46.46.241.2     172.16.186.4   8070/TCP
                                        36h
amf-service                             ClusterIP   46.46.168.108   <none>
9003/TCP,8080/TCP                              36h
base-entitlement-amf                   ClusterIP   46.46.114.105   <none>         8000/TCP
                                        29d
bgpspeaker-pod                          ClusterIP   46.46.238.2     <none>
9008/TCP,7001/TCP,8879/TCP                     36h
datastore-notification-ep              ClusterIP   46.46.82.153    172.16.184.4   8012/TCP
                                        36h
documentation                          ClusterIP   46.46.73.219    <none>         8080/TCP
                                        29d
etcd                                    ClusterIP   None            <none>
2379/TCP,7070/TCP                              36h
etcd-amf-ins1-etcd-cluster-0            ClusterIP   46.46.167.73    <none>
2380/TCP,2379/TCP                              36h
etcd-amf-ins1-etcd-cluster-1            ClusterIP   46.46.144.110   <none>
2380/TCP,2379/TCP                              36h
etcd-amf-ins1-etcd-cluster-2            ClusterIP   46.46.51.186    <none>
2380/TCP,2379/TCP                              36h
grafana-dashboard-amf                  ClusterIP   46.46.124.50    <none>         9418/TCP
                                        36h
grafana-dashboard-app-infra-amf-ins1    ClusterIP   46.46.72.66     <none>        9418/TCP
                                        36h
grafana-dashboard-etcd-amf-ins1        ClusterIP   46.46.152.59    <none>         9418/TCP
                                        36h
gtpc-ep                                 ClusterIP   46.46.197.81    <none>
9003/TCP,8080/TCP                              36h
ldap-proxy-amf-ins1-oam-pod             ClusterIP   46.46.71.103    <none>
636/TCP,389/TCP                                36h
li-ep                                   ClusterIP   46.46.225.162   <none>
9003/TCP,8080/TCP                              36h
local-ldap-proxy-amf-ins1-ops-center    ClusterIP   46.46.178.218   <none>
636/TCP,369/TCP                                29d
netconf-ops-center-amf-ins1-ops-center  ClusterIP   46.46.239.155   10.84.125.82   2024/TCP
                                        29d
nodemgr                                 ClusterIP   46.46.232.17    <none>
9003/TCP,8884/TCP,8879/TCP,9201/TCP,8080/TCP   36h
oam-pod                                 ClusterIP   46.46.178.171   <none>
9008/TCP,7001/TCP,8879/TCP,10080/TCP,8080/TCP   36h
ops-center-amf-ins1-ops-center          ClusterIP   46.46.230.116   <none>
8008/TCP,8080/TCP,2024/TCP,2022/TCP,7681/TCP   29d
prometheus-rules-etcd                   ClusterIP   None            <none>        9419/TCP
                                        36h
smart-agent-amf-ins1-ops-center         ClusterIP   46.46.9.52      <none>        8888/TCP
                                        29d
ssh-ops-center-amf-ins1-ops-center      ClusterIP   46.46.97.118    10.84.125.82   2025/TCP
                                        29d
```

To view the comprehensive service details, use the following command.

kubectl get svc -n *amf_namespace service_name* **-o yaml**

Sample Output:

```
kubectl get svc amf-rest-ep -n amf-ins1 -o yaml
apiVersion: v1
kind: Service
metadata:
  annotations:
    meta.helm.sh/release-name: amf-ins1-amf-rest-ep
    meta.helm.sh/release-namespace: amf-ins1
  creationTimestamp: "2021-10-16T18:00:23Z"
  labels:
    app: amf-rest-ep
    app.kubernetes.io/managed-by: Helm
    chart: amf-rest-ep-0.1.0-main-2464-211014124230-2d34ce7
    component: amf-rest-ep
    heritage: Helm
    release: amf-ins1-amf-rest-ep
  name: amf-rest-ep
  namespace: amf-ins1
  resourceVersion: "5768444"
  uid: 65cb4204-8914-4b71-aa3c-809238dd755e
spec:
  clusterIP: 46.46.171.99
  clusterIPs:
  - 46.46.171.99
  ipFamilies:
  - IPv4
  ipFamilyPolicy: SingleStack
  ports:
  - name: grpc
    port: 9003
    protocol: TCP
    targetPort: 9003
  - name: metrics
    port: 8080
    protocol: TCP
    targetPort: 8080
  - name: nrfrestep
    port: 9201
    protocol: TCP
    targetPort: 9201
  selector:
    component: amf-rest-ep
    release: amf-ins1-amf-rest-ep
  sessionAffinity: None
  type: ClusterIP
status:
  loadBalancer: {}
```

CHAPTER 6

Compliance to 3GPP Specifications

Feature Summary and Revision History

Summary Data

Table 13: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 14: Revision History

Revision Details	Release
First introduced.	2021.04.0

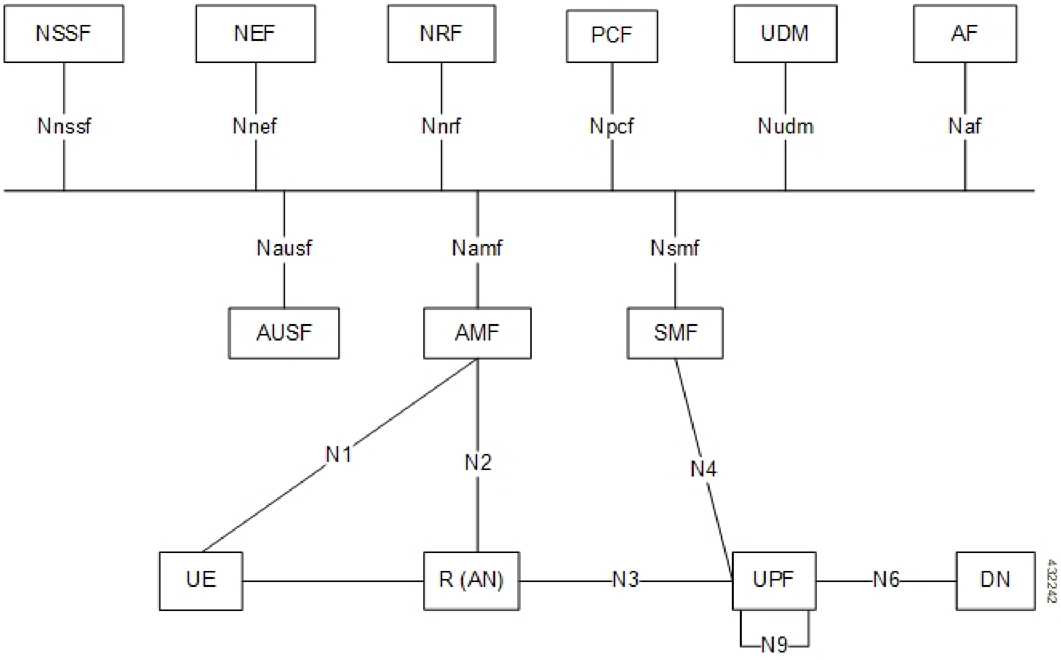
Feature Description

The Access and Mobility Management Function (AMF) supports the 3GPP-released June-19 specifications on all the interfaces.

In the 5G network, the AMF offers services to the other AMF, PCF, NSSF, NRF, NEF, UDM, and AF via the Namf service-based interface (see 3GPP TS 23.501 and 3GPP TS 23.502).

The SMF, PCF, NRF, AUSF and UDM interfaces are currently supported from AMF. For more information, see http://www.3gpp.org/ftp/Specs/archive/29_series/29.518/29518-f00.zip.

The following reference diagram represents a high-level network containing AMF connected to other nodes.



Standards Compliance

Cisco AMF complies with the 3GPP standards. For more information, refer to Standards Compliance, on page 13.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows of compliance to 3GPP specifications.

UE Registration

To enable UE tracking and reachability, a UE must register with the network to be authorized to receive services.

Initial Registration Request Call Flow

This section describes the Initial Registration Request call flow.

Figure 12: Initial Registration Request Call Flow

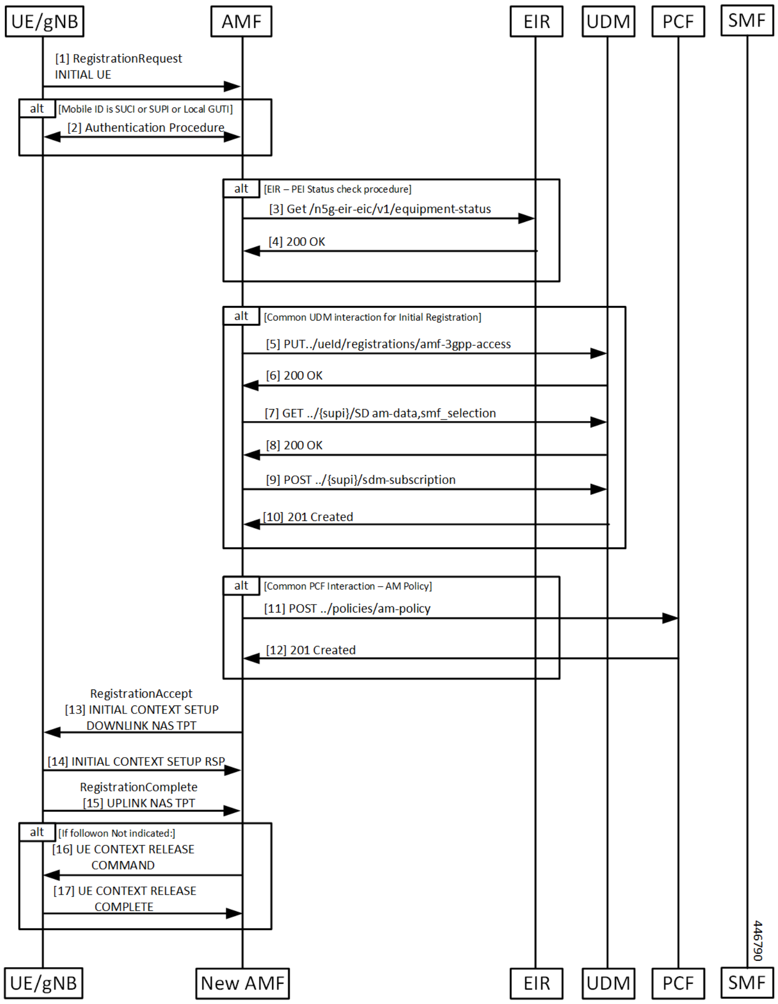

UE/gNB
AMF
EIR
UDM
PCF
SMF
[1] RegistrationRequest
INITIAL UE
alt
[Mobile ID is SUCI or SUPI or Local GUTI]
[2] Authentication Procedure
alt
[EIR – PEI Status check procedure]
[3] Get /n5g-eir-eic/v1/equipment-status
[4] 200 OK
alt
[Common UDM interaction for Initial Registration]
[5] PUT../ueId/registrations/amf-3gpp-access
[6] 200 OK
[7] GET ../{supi}/SD am-data,smf_selection
[8] 200 OK
[9] POST ../{supi}/sdm-subscription
[10] 201 Created
alt
[Common PCF Interaction – AM Policy]
[11] POST ../policies/am-policy
[12] 201 Created
RegistrationAccept
[13] INITIAL CONTEXT SETUP
DOWNLINK NAS TPT
[14] INITIAL CONTEXT SETUP RSP
RegistrationComplete
[15] UPLINK NAS TPT
alt
[If followon Not indicated:]
[16] UE CONTEXT RELEASE
COMMAND
[17] UE CONTEXT RELEASE
COMPLETE
446790
UE/gNB
New AMF
EIR
UDM
PCF
SMF

Table 15: Initial Registration Request Call Flow Description

Step	Description
1	An UE which wants to register itself with the 5G core sends a Registration-Request N1 message towards AMF with the contents (registration type, SUCI, or 5G-GUTI, last visited TAI (if available), security parameters, requested NSSAI, UE radio capability, UE MM core network capability, PDU session status, list of PDU sessions to be activated, follow on request). If the subscriber is unknown, AMF allocates AMF-NGAP-id to the NGAP connection and subscriber data-store. The AMF-NGAP-id to AMF-Service is stored in etcd so that subsequent messages over the NGAP connection reach same AMF-Service. gNB selects an AMF and forwards the registration-request message to AMF.
2	If the identity received from the UE was either a SUCI/SUPI/GUTI allocated by this AMF, the AMF authenticates the UE as presented in the authentication procedure.

Step	Description
3	If the AMF is configured to do EIR checks during registration, the AMF retrieves the PEI from the UE during security mode command procedure. It then checks the status of the equipment during registration procedure.
4	Depending on the status of the equipment from EIR, the AMF either rejects the registration or proceeds with the call. Actions to be taken when the status is grey listed is configurable on the call control policy currently active for the UE.
5	The AMF selects an UDM based on the PLMN information through NRF query or via static configuration and registers the UE with the UDM using Nudm_UECM_Registration.
6	The UDM stores the AMF identity and responds to the AMF request.
7	The AMF requests from the UDM the Access and Mobility Subscription, and SMF Selection Subscription Data using Nudm_SDM_Get and using multiple data set names. If integrity check passes and UDM subscription data already exits in UE context, AMF skips Steps 7 - 10.
8	The UDM responds to the request from the AMF. The AMF stores the subscription information.
9	The AMF subscribes to be notified using Nudm_SDM_Subscribe when the data requested is modified.
10	The UDM registers the AMF and responds to the AMF.
11	AMF selects PCF based on PLMN-info and slice-info and performs a policy association establishment. PCF sends policy data to AMF with restrictions and other policies to be applied for the UE. **Note** If integrity check passes and PCF subscription data already exits in UE context, AMF skips this step.
12	The PCF responds to the AMF request along with AM-Policy configurations for the subscriber.
13	The AMF sends a Registration Accept message to the UE indicating that the Registration Request has been accepted. Registration Accept contains (registration area, mobility restrictions, PDU session status, allowed NSSAI, configured NSSAI for the serving PLMN, periodic registration update timer, emergency service support indicator, accepted DRX parameters).
14	If the AMF sends a INITIAL CONTEXT SETUP REQUEST, the gNB responds with a INITIAL CONTEXT SETUP RESPONSE. This message could come after the message in Step 12.
15	The UE sends a Registration Complete message to the AMF to acknowledge that a new 5G-GUTI was assigned if a new 5G GUTI was included in the Registration Accept message.
16	If the UE did not include a follow-on indication in the request, the AMF releases the UE gNB context by sending a UE CONTEXT RELEASE COMMAND to the gNB
17	The gNB responds with a UE CONTEXT RELEASE COMPLETE message to the AMF.

Mobility Updating or Periodic Registration with no AMF Change Call Flow

This section describes the Mobility Updating or Periodic Registration with no AMF Change call flow.

Figure 13: Mobility Updating or Periodic Registration Call Flow

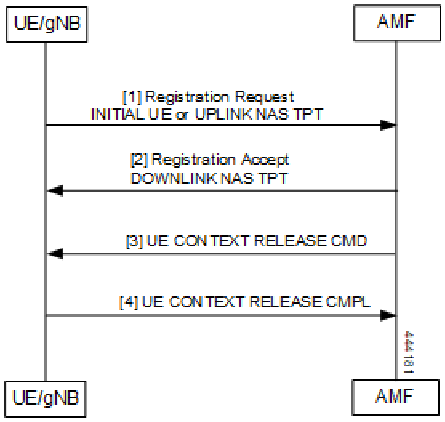


Table 16: Initial Registration Request Call Flow Description

Step	Description
1	The UE triggers this procedure under the following conditions: **1.** The Periodic Registration timer in the UE expires. The UE sets up the registration type as "Periodic" in this case, and the message arrives on the AMF as an INITIAL UE NGAP message. **2.** The UE is in IDLE state and moves to an area that is not currently part of its Tracking Area List. In this case, the UE sets the type to "Mobility Updating", and the NGAP message is the INITIAL UE message. **3.** After or during handover, the UE is an area that is not part of the current Tracking Area List. In this case, the UE sets the type to "Mobility Updating", and the NGAP message is the UPLINK NAS TRANSPORT.
2	If the Registration Type is Mobility Updating, the AMF computes a new Tracking Area List for the UE. The AMF then adds this to a Registration Accept and uses a DOWNLINK NAS TRANSPORT NGAP message to send it to the UE.
3	If the registration request in the INITIAL UE message registration type is not Mobility Updating, and the FollowOn IE was not set by the UE, the AMF sends a UE CONTEXT RELEASE COMMAND to the gNB to release the resources at the gNB. If the registration type is Mobility Updating, AMF service ignores FollowOn IE and does not initiate UE CONTEXT RELEASE COMMAND.
4	The gNB responds with a UE CONTEXT RELEASE COMPLETE.

PDU Session Establishment Call Flow

This section describes the PDU Session Establishment call flow.

UE receives data services through a Protocol Data Unit (PDU) session, which is a logical connection between the UE and core network.

In PDU session establishment, UE establishes a PDU session for accessing data services. Unlike EPS, where a default PDU session is always created while the UE registers to the network, in 5G, the UE can establish a PDU session when service is needed.

Figure 14: PDU Session Establishment Call Flow

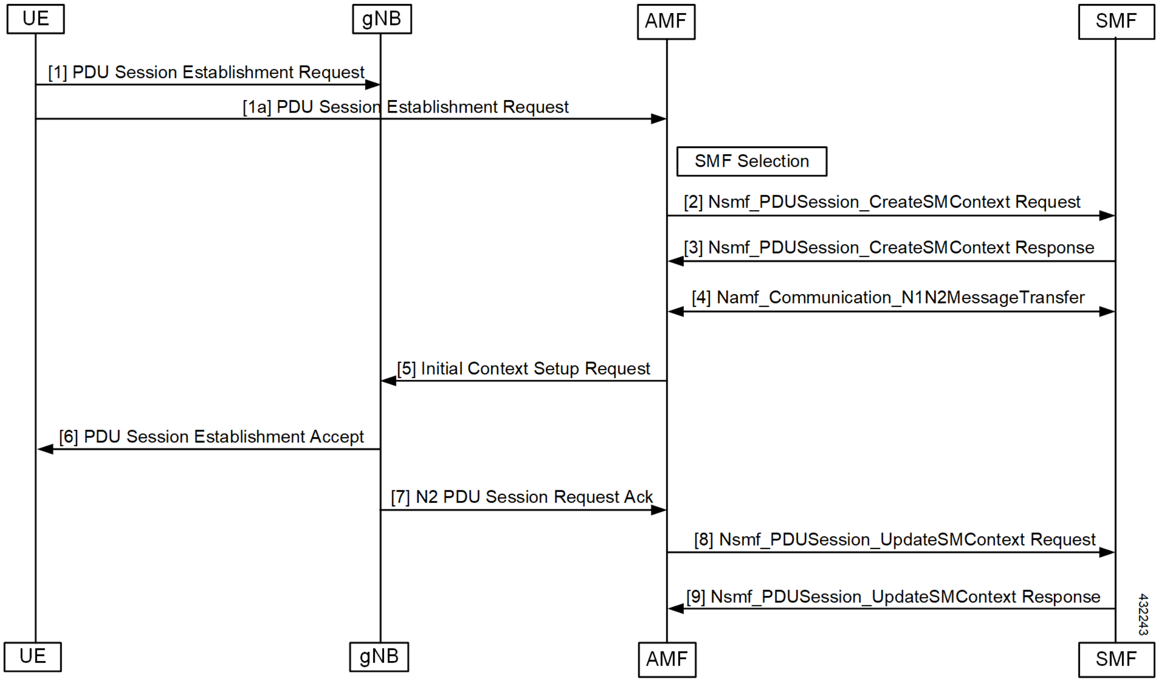

UE
gNB
AMF
SMF
[1] PDU Session Establishment Request
[1a] PDU Session Establishment Request
SMF Selection
[2] Nsmf_PDUSession_CreateSMContext Request
[3] Nsmf_PDUSession_CreateSMContext Response
[4] Namf_Communication_N1N2MessageTransfer
[5] Initial Context Setup Request
[6] PDU Session Establishment Accept
[7] N2 PDU Session Request Ack
[8] Nsmf_PDUSession_UpdateSMContext Request
[9] Nsmf_PDUSession_UpdateSMContext Response
432243
UE
gNB
AMF
SMF

Table 17: PDU Session Establishment Call Flow Description

Step	Description
1	In order to establish a new PDU Session, the UE generates a new PDU Session ID and initiates the PDU Session Establishment procedure by the transmission of 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.
2	The AMF selects SMF based on slice-info and plmn-info provided by UE. SMF is selected by NRF query or by static configuration. AMF invokes the Nsmf_PDUSession_CreateSMContext Request towards SMF with SUPI, DNN, S-NSSAI(s), PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container (PDU Session Establishment Request), User location information, Access Type, PEI, GPSI, UE presence in LADN service area, Subscription For PDU Session Status Notification, DNN Selection Mode. Subscriber data-store is modified to store PDU information. AMF-Service Stickiness is maintained for the subscriber for the PDU establishment transaction.
3	SMF creates an SM context and responds to the AMF by sending Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID or N1 SM container (PDU Session Reject (Cause)).

Step	Description
4	SMF sends Namf_Communication_N1N2MessageTransfer to AMF. The N2 SM information carries information that the AMF shall forward to the RAN. The N1 SM container contains the PDU Session Establishment Accept that the AMF provides to the UE. The Namf_Communication_N1N2MessageTransfer contains the PDU Session ID allowing the AMF to know which access towards the UE to use.
5	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 RAN.
6	RAN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) to the UE.
7	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)).
8	Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type).The AMF forwards the N2 SM information received from RAN to the SMF.

PDU Session Establishment with Initial Context Call Flow

This section describes the PDU Session Establishment with Initial Context call flow.

Figure 15: PDU Session Establishment with Initial Context Call Flow

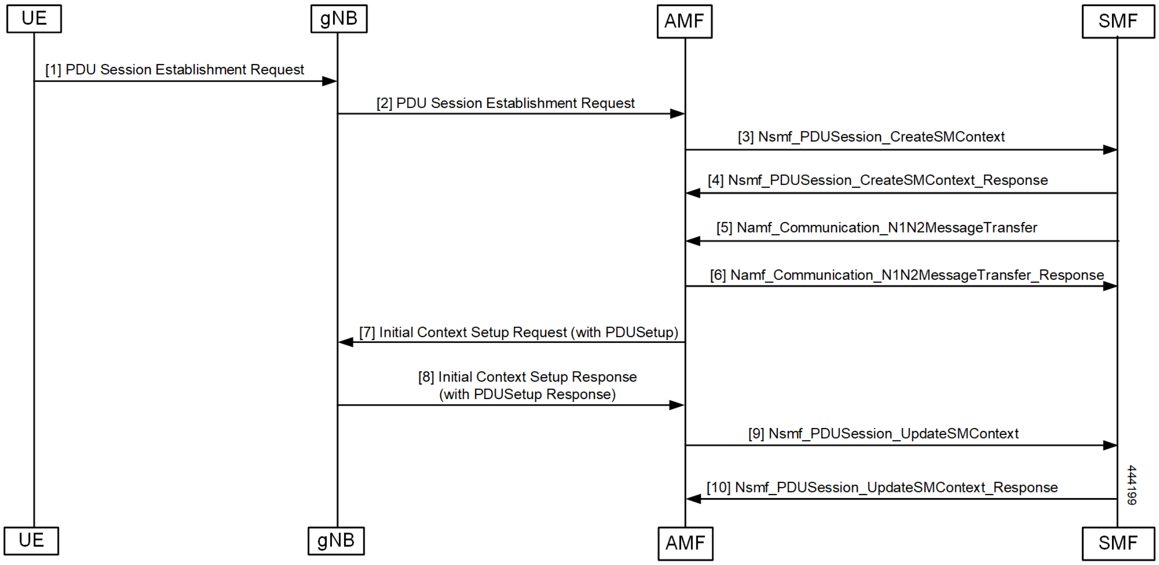

UE
gNB
AMF
SMF
[1] PDU Session Establishment Request
[2] PDU Session Establishment Request
[3] Nsmf_PDUSession_CreateSMContext
[4] Nsmf_PDUSession_CreateSMContext_Response
[5] Namf_Communication_N1N2MessageTransfer
[6] Namf_Communication_N1N2MessageTransfer_Response
[7] Initial Context Setup Request (with PDUSetup)
[8] Initial Context Setup Response (with PDUSetup Response)
[9] Nsmf_PDUSession_UpdateSMContext
[10] Nsmf_PDUSession_UpdateSMContext_Response
444199
UE
gNB
AMF
SMF

Table 18: PDU Session Establishment for Existing PDU Call Flow Description

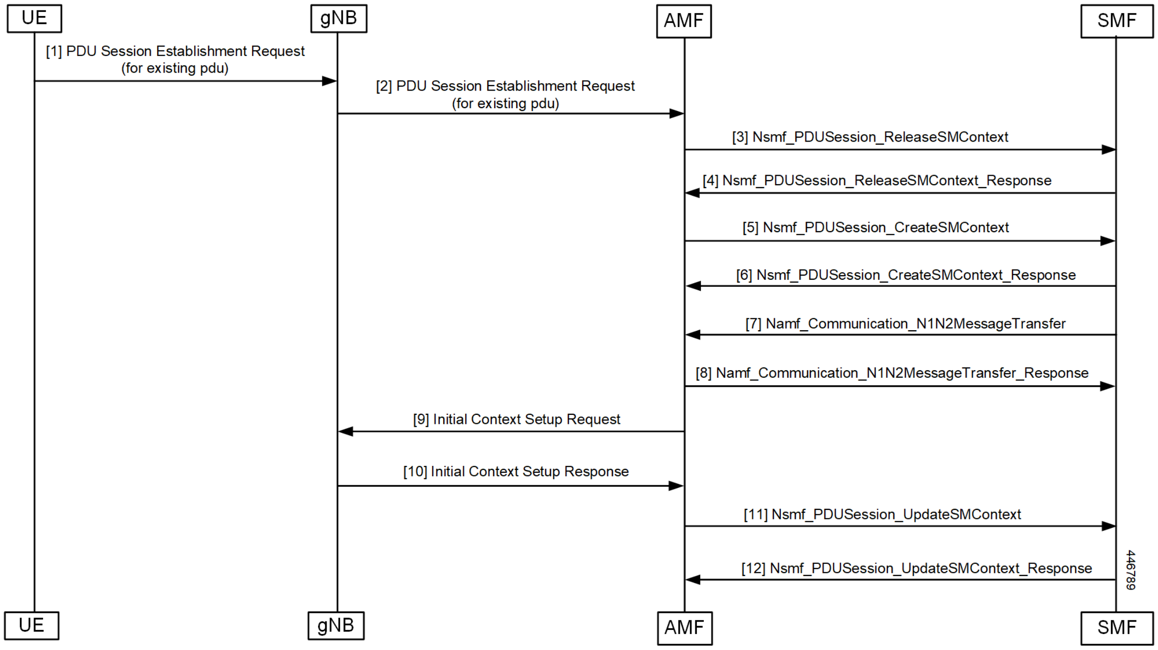
Step	Description
1	In order to establish a new PDU Session, the UE generates a new PDU Session ID and initiates the PDU Session Establishment procedure by the transmission of a NAS message containing a PDU Session Establishment Request within the N1 SM container. The PDU Session Establishment Request 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.
2,3,4	If PDU exists, then clean up at AMF and SMF (SmContextReleaseRequest) is done and PDU establishment is performed.
5, 6	The AMF selects SMF based on slice-info and plmn-info provided by UE. SMF is selected by NRF query or by static configuration. AMF invokes the Nsmf_PDUSession_CreateSMContext Request towards SMF with SUPI, DNN, S-NSSAI(s), PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container (PDU Session Establishment Request), User location information, Access Type, PEI, GPSI, UE presence in LADN service area, Subscription For PDU Session Status Notification, DNN Selection Mode. Subscriber data-store is modified to store PDU information. AMF-Service Stickiness is maintained for the subscriber for the PDU establishment transaction. SMF creates an SM context and responds to the AMF by sending Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID or N1 SM container (PDU Session Reject (Cause)). SMF sends Namf_Communication_N1N2MessageTransfer to AMF. The N2 SM information carries information that the AMF shall forward to the RAN. The N1 SM container contains the PDU Session Establishment Accept that the AMF provides to the UE. The Namf_Communication_N1N2MessageTransfer contains the PDU Session ID allowing the AMF to know which access towards the UE to use. SMF receives Namf_Communication_N1N2MessageTransfer response from AMF.
7	RAN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) to the UE.
8	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)).
9	Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type).The AMF forwards the N2 SM information received from RAN to the SMF.
10	SMF sends Nsmf_PDUSession_UpdateSMContext Response. to AMF

PDU Session Establishment for Existing PDU Call Flow

This section describes the IPDU Session Establishment for Existing PDU call flow.

If UE initiates PDU establishment request for existing PDU, then AMF performs local PDU release and sends PDU release to SMF. It also initiates PDU resource setup request. If PDU release fails at SMF, then AMF sends PDU reject.

Figure 16: PDU Session Establishment for Existing PDU Call Flow


UE
gNB
AMF
SMF
[1] PDU Session Establishment Request (for existing pdu)
[2] PDU Session Establishment Request (for existing pdu)
[3] Nsmf_PDUSession_ReleaseSMContext
[4] Nsmf_PDUSession_ReleaseSMContext_Response
[5] Nsmf_PDUSession_CreateSMContext
[6] Nsmf_PDUSession_CreateSMContext_Response
[7] Namf_Communication_N1N2MessageTransfer
[8] Namf_Communication_N1N2MessageTransfer_Response
[9] Initial Context Setup Request
[10] Initial Context Setup Response
[11] Nsmf_PDUSession_UpdateSMContext
[12] Nsmf_PDUSession_UpdateSMContext_Response
446789
UE
gNB
AMF
SMF

UE receives data services through a Protocol Data Unit (PDU) session, which is a logical connection between the UE and core network. PDU session establishment procedure describes the procedures by which UE establishes a PDU session for accessing data services. In 5G, the UE can establish a PDU session when service is needed.

Table 19: PDU Session Establishment for Existing PDU Call Flow Description

Step	Description
1	In order to establish a new PDU Session, the UE generates a new PDU Session ID and initiates the PDU Session Establishment procedure by the transmission of 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.
2,3,4	If PDU exists, then clean up at AMF and SMF (SmContextReleaseRequest) is done and PDU establishment is performed.
5	The AMF selects SMF based on slice-info and plmn-info provided by UE. SMF is selected by NRF query or by static configuration. AMF invokes the Nsmf_PDUSession_CreateSMContext Request towards SMF with SUPI, DNN, S-NSSAI(s), PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container (PDU Session Establishment Request), User location information, Access Type, PEI, GPSI, UE presence in LADN service area, Subscription For PDU Session Status Notification, DNN Selection Mode. Subscriber data-store is modified to store PDU information. AMF-Service Stickiness is maintained for the subscriber for the PDU establishment transaction.
6	SMF creates an SM context and responds to the AMF by sending Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID or N1 SM container (PDU Session Reject (Cause)).

Step	Description
7	SMF sends Namf_Communication_N1N2MessageTransfer to AMF. The N2 SM information carries information that the AMF shall forward to the RAN. The N1 SM container contains the PDU Session Establishment Accept that the AMF provides to the UE. The Namf_Communication_N1N2MessageTransfer contains the PDU Session ID allowing the AMF to know which access towards the UE to use.
8	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 RAN. If Initial context setup isn’t done, then AMF sends the NAS message information as a part of initial context setup request.
9	RAN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) to the UE.
10	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)).
11	Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type).The AMF forwards the N2 SM information received from RAN to the SMF.
12	SMF send Nsmf_PDUSession_UpdateSMContext Response.

PDU Session Modification

The PDU session modification procedure is used when one or several of the QoS parameters exchanged between the UE and the network are modified.

In this release, only UE- and SMF-initiated PDU session modification is supported. RAN-initiated PDU session modification is not supported.

UE-initiated PDU Session Modification Call Flow

This section describes the UE-initiated PDU Session Modification call flow.

PDU Session modification is required when one or several of the QoS parameters exchanged between the UE and the network needs to be modified.

Figure 17: UE-initiated PDU Session Modification Call Flow

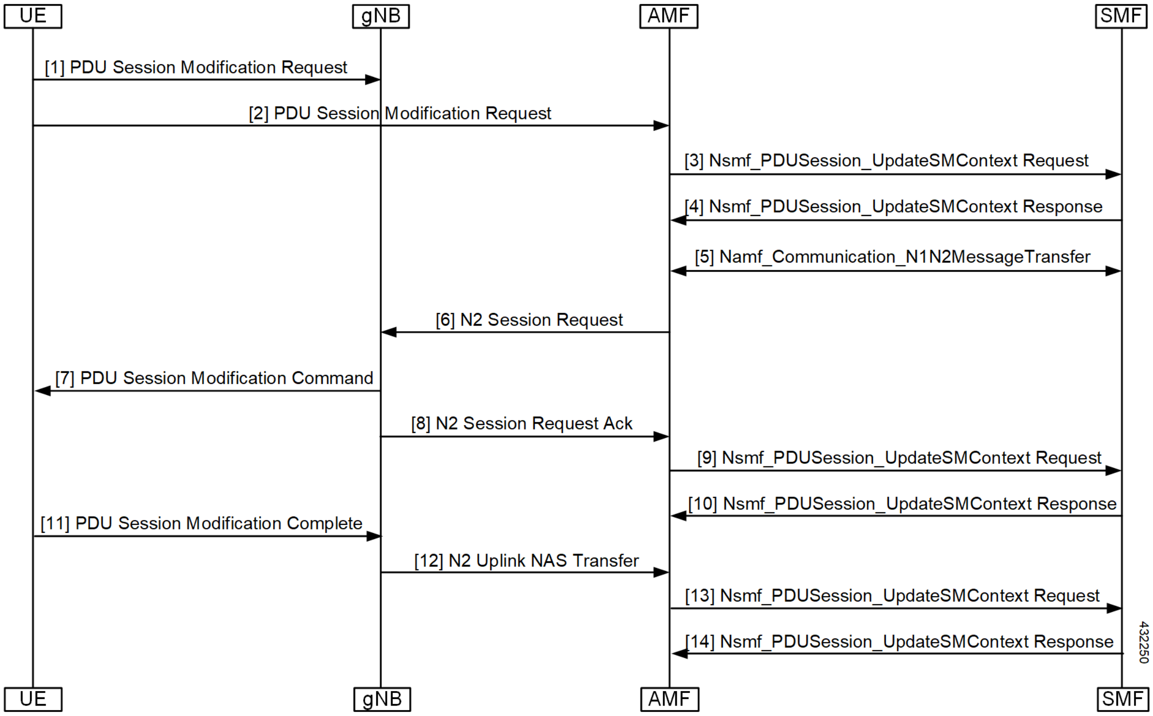

UE
gNB
AMF
SMF
[1] PDU Session Modification Request
[2] PDU Session Modification Request
[3] Nsmf_PDUSession_UpdateSMContext Request
[4] Nsmf_PDUSession_UpdateSMContext Response
[5] Namf_Communication_N1N2MessageTransfer
[6] N2 Session Request
[7] PDU Session Modification Command
[8] N2 Session Request Ack
[9] Nsmf_PDUSession_UpdateSMContext Request
[10] Nsmf_PDUSession_UpdateSMContext Response
[11] PDU Session Modification Complete
[12] N2 Uplink NAS Transfer
[13] Nsmf_PDUSession_UpdateSMContext Request
[14] Nsmf_PDUSession_UpdateSMContext Response
432250
UE
gNB
AMF
SMF

Table 20: UE-initiated PDU Session Modification Call Flow Description

Step	Description
1, 2, 3	The UE initiates the PDU Session Modification procedure by the transmission of an NAS message (N1 SM container (PDU Session Modification Request (PDU session ID, Packet Filters, Operation, Requested QoS, Segregation, 5GSM Core Network Capability)), PDU Session ID) message. AMF invokes the Nsmf_PDUSession_UpdateSMContext Request towards SMF.
4	The SMF responds to the AMF through Nsmf_PDUSession_UpdateSMContext (N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS parameters, Session-AMBR))). The N2 SM information carries information that the AMF provides to the RAN. It may include the QoS profiles and the corresponding QFIs to notify the RAN that one or more QoS flows were added, or modified. It may include only QFI(s) to notify the RAN that one or more QoS flows were removed. The N2 SM information provided to the RAN includes information for establishment of User Plane resources. The N1 SM container carries the PDU Session Modification Command that the AMF shall provide to the UE.
5	The SMF invokes Namf_Communication_N1N2MessageTransfer (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 parameters, Session-AMBR).
6	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 RAN.

Step	Description
7	The RAN issues AN specific signaling exchange with the UE that is related with the information received from SMF.
8	The RAN acknowledges N2 PDU Session Request by sending a N2 PDU Session Ack (N2 SM information (List of accepted/rejected QFI(s), AN Tunnel Info, PDU Session ID), User location Information) Message to the AMF.
9, 10	The AMF forwards the N2 SM information and the User location Information received from the AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. The SMF replies with a Nsmf_PDUSession_UpdateSMContext Response.
11	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.
12	The RAN forwards the NAS message to the AMF.
13	The AMF forwards the N1 SM container (PDU Session Modification Command Ack) and User Location Information received from the AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. The SMF replies with a Nsmf_PDUSession_UpdateSMContext Response.

SMF-initiated PDU Session Modification Call Flow

This section describes the SMF-initiated PDU Session Modification call flow.

PDU Session modification is required when one or several of the QoS parameters exchanged between the UE and the network needs to be modified.

Figure 18: SMF-initiated PDU Session Modification Call Flow

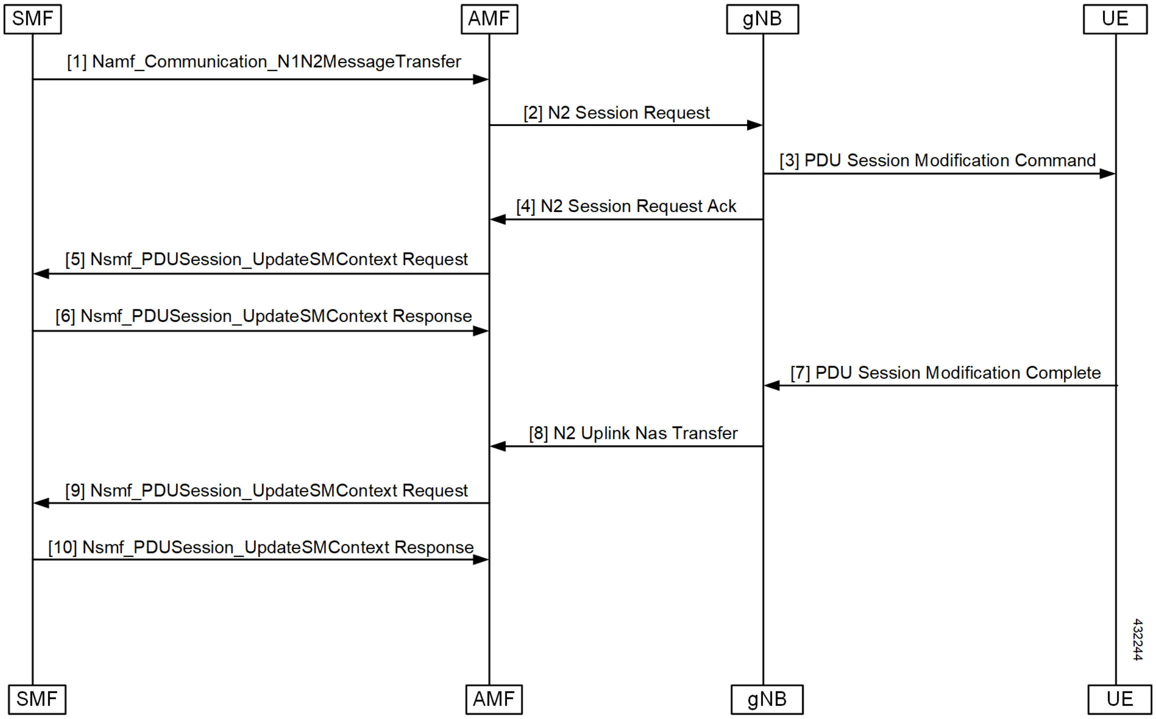

SMF
AMF
gNB
UE
[1] Namf_Communication_N1N2MessageTransfer
[2] N2 Session Request
[3] PDU Session Modification Command
[4] N2 Session Request Ack
[5] Nsmf_PDUSession_UpdateSMContext Request
[6] Nsmf_PDUSession_UpdateSMContext Response
[7] PDU Session Modification Complete
[8] N2 Uplink Nas Transfer
[9] Nsmf_PDUSession_UpdateSMContext Request
[10] Nsmf_PDUSession_UpdateSMContext Response
432244
SMF
AMF
gNB
UE

Table 21: SMF-initiated PDU Session Modification Call Flow Description

Step	Description
1	The SMF initiates PDU session modification to the AMF through Nsmf_PDUSession_UpdateSMContext (N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS parameters, Session-AMBR)). The N2 SM carries information that the AMF provides to the RAN. It includes the QoS profiles and the corresponding QFIs to notify the RAN that one or more QoS flows were added, or modified. It can also include only QFI(s) to notify the RAN that one or more QoS flows were removed. The N2 SM information provided to the RAN includes information for establishment of User Plane resources. The N1 SM container carries the PDU Session Modification Command that the AMF provides to the UE.
2	The SMF invokes Namf_Communication_N1N2MessageTransfer (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 parameters, Session-AMBR))).
3	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 RAN.
4	The RAN issues AN specific signaling exchange with the UE that is related with the information received from SMF.
5	The RAN acknowledges N2 PDU Session Request by sending a N2 PDU Session Ack (N2 SM information (List of accepted/rejected QFI(s), AN Tunnel Info, PDU Session ID), User location Information) Message to the AMF.
6	The AMF forwards the N2 SM information and the User location Information received from the AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. The SMF replies with a Nsmf_PDUSession_UpdateSMContext Response.
7	If the RAN rejects QFI(s) the SMF is responsible of updating 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 UE acknowledges the PDU Session Modification Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command Ack)) message.
9	The RAN forwards the NAS message to the AMF.
10	The AMF forwards the N1 SM container (PDU Session Modification Command Ack) and User Location Information received from the AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. The SMF replies with a Nsmf_PDUSession_UpdateSMContext Response.

PDU Session Release

The PDU session release procedure is used to release all the resources associated with a PDU Session.

In this release, UE- and SMF-initiated PDU session release is supported.

UE-initiated PDU Session Release Call Flow

This section describes the UE-initiated PDU Session Release call flow.

The PDU Session Release procedure is used to release all the resources associated with a PDU Session.

Figure 19: UE-initiated PDU Session Release Call Flow

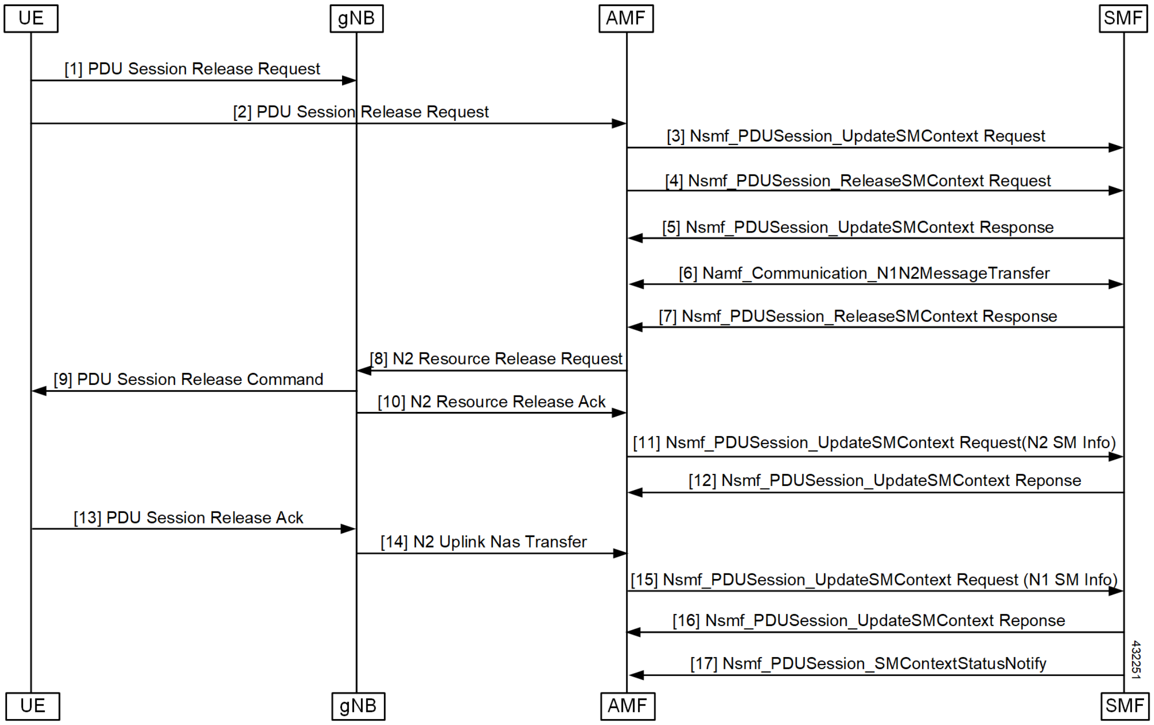

UE
gNB
AMF
SMF
[1] PDU Session Release Request
[2] PDU Session Release Request
[3] Nsmf_PDUSession_UpdateSMContext Request
[4] Nsmf_PDUSession_ReleaseSMContext Request
[5] Nsmf_PDUSession_UpdateSMContext Response
[6] Namf_Communication_N1N2MessageTransfer
[7] Nsmf_PDUSession_ReleaseSMContext Response
[8] N2 Resource Release Request
[9] PDU Session Release Command
[10] N2 Resource Release Ack
[11] Nsmf_PDUSession_UpdateSMContext Request(N2 SM Info)
[12] Nsmf_PDUSession_UpdateSMContext Reponse
[13] PDU Session Release Ack
[14] N2 Uplink Nas Transfer
[15] Nsmf_PDUSession_UpdateSMContext Request (N1 SM Info)
[16] Nsmf_PDUSession_UpdateSMContext Reponse
[17] Nsmf_PDUSession_SMContextStatusNotify
432251
UE
gNB
AMF
SMF

Table 22: UE-initiated PDU Session Release Call Flow Description

Step	Description
1, 2	The UE initiates the UE Requested PDU Session Release procedure by the transmission of an NAS message (N1 SM container (PDU Session Release Request (PDU session ID)), PDU Session ID) message. The NAS message is forwarded by the RAN to the AMF with an indication of User Location Information. This message is relayed to the SMF corresponding to the PDU Session ID via N2 and the AMF.
3	The AMF invokes the Nsmf_PDUSession_UpdateSMContext service operation and provides the N1 SM container to the SMF together with User Location Information (ULI) received from the RAN.
4	The AMF may invoke the Nsmf_PDUSession_ReleaseSMContext service operation to request the release of the PDU Session in case of mismatch of PDU Session status between UE and AMF.
5	The SMF responds to the AMF with the Nsmf_PDUSession_UpdateSMContext response (N2 SM Resource Release request, N1 SM container (PDU Session Release Command)).

Step	Description
6	If the UP connection of the PDU Session is active, the SMF shall also include the N2 Resource Release request (PDU Session ID) in the Namf_Communication_N1N2MessageTransfer, to release the RAN resources associated with the PDU Session.
7	SMF responds to the AMF with the Nsmf_PDUSession_ReleaseSMContext response.
8	AMF transfers the SM information received from the SMF (N2 SM Resource Release request, N1 SM container) to the RAN.
9	When the RAN has received an N2 SM request to release the AN resources associated with the PDU Session it issues AN specific signaling exchange(s) with the UE to release the corresponding AN resources.
10	RAN sends any NAS message (N1 SM container (PDU Session Release Command)) received from the AMF.
11	The AMF invokes the Nsmf_PDUSession_UpdateSMContext (N2 SM Resource Release Ack, User Location Information) to the SMF.
12	The SMF responds to the AMF with an Nsmf_PDUSession_UpdateSMContext response.
13	The UE acknowledges the PDU Session Release Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Release Ack)) message over the RAN.
14	The RAN forwards the NAS message from the UE by sending a N2 NAS uplink transport (NAS message (PDU Session ID, N1 SM container (PDU Session Release Ack)), User Location Information) to the AMF.
15	The AMF invokes the Nsmf_PDUSession_UpdateSMContext (N1 SM container (PDU Session Release Ack, User Location Information) to the SMF.
16	The SMF responds to the AMF with an Nsmf_PDUSession_UpdateSMContext response.
17	The SMF invokes Nsmf_PDUSession_SMContextStatusNotify to notify AMF that the SM context for this PDU Session is released. The AMF releases the association between the SMF ID and the PDU Session ID, DNN, as well as S-NSSAI.

SMF-initiated PDU Release Call Flow

This section describes SMF-initiated PDU Release call flow.

The PDU Session Release procedure is used to release all the resources associated with a PDU Session.

Figure 20: SMF-initiated PDU Release Call Flow

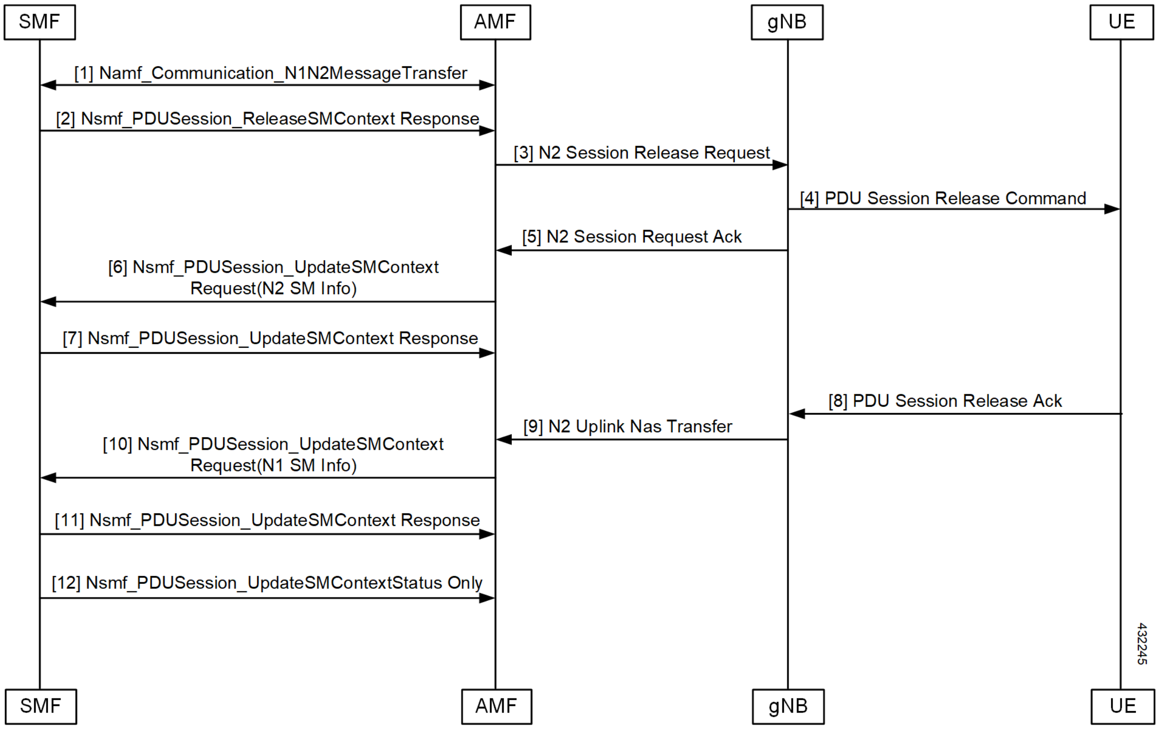

SMF
AMF
gNB
UE
[1] Namf_Communication_N1N2MessageTransfer
[2] Nsmf_PDUSession_ReleaseSMContext Response
[3] N2 Session Release Request
[4] PDU Session Release Command
[5] N2 Session Request Ack
[6] Nsmf_PDUSession_UpdateSMContext Request(N2 SM Info)
[7] Nsmf_PDUSession_UpdateSMContext Response
[8] PDU Session Release Ack
[9] N2 Uplink Nas Transfer
[10] Nsmf_PDUSession_UpdateSMContext Request(N1 SM Info)
[11] Nsmf_PDUSession_UpdateSMContext Response
[12] Nsmf_PDUSession_UpdateSMContextStatus Only
432245
SMF
AMF
gNB
UE

Table 23: SMF-initiated PDU Release Call Flow Description

Step	Description
1	If the UP connection of the PDU Session is active, the SMF shall also include the N2 Resource Release request (PDU Session ID) in the Namf_Communication_N1N2MessageTransfer, to release the RAN resources associated with the PDU Session.
2	SMF responds to the AMF with the Nsmf_PDUSession_ReleaseSMContext response.
3	AMF transfers the SM information received from the SMF (N2 SM Resource Release request, N1 SM container) to the RAN.
4	When the RAN has received an N2 SM request to release the AN resources associated with the PDU Session it issues AN specific signaling exchange(s) with the UE to release the corresponding AN resources.
5	RAN sends any NAS message (N1 SM container (PDU Session Release Command)) received from the AMF.
6	The AMF invokes the Nsmf_PDUSession_UpdateSMContext (N2 SM Resource Release Ack, User Location Information) to the SMF.
7	The SMF responds to the AMF with an Nsmf_PDUSession_UpdateSMContext response.
8	The UE acknowledges the PDU Session Release Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Release Ack)) message over the RAN.

Step	Description
9	The RAN forwards the NAS message from the UE by sending a N2 NAS uplink transport (NAS message (PDU Session ID, N1 SM container (PDU Session Release Ack)), User Location Information) to the AMF.
10	The AMF invokes the Nsmf_PDUSession_UpdateSMContext (N1 SM container (PDU Session Release Ack, User Location Information) to the SMF.
11	The SMF responds to the AMF with an Nsmf_PDUSession_UpdateSMContext response.
12	The SMF invokes Nsmf_PDUSession_SMContextStatusNotify to notify AMF that the SM context for this PDU Session is released. The AMF releases the association between the SMF ID and the PDU Session ID, DNN, as well as S-NSSAI.

UE-initiated Deregistration Call Flow

This section describes the UE-initiated Deregistration call flow.

The deregistration procedure allows the UE to inform the network that it does not want to access the 5G data services.

Figure 21: UE-initiated Deregistration Call Flow

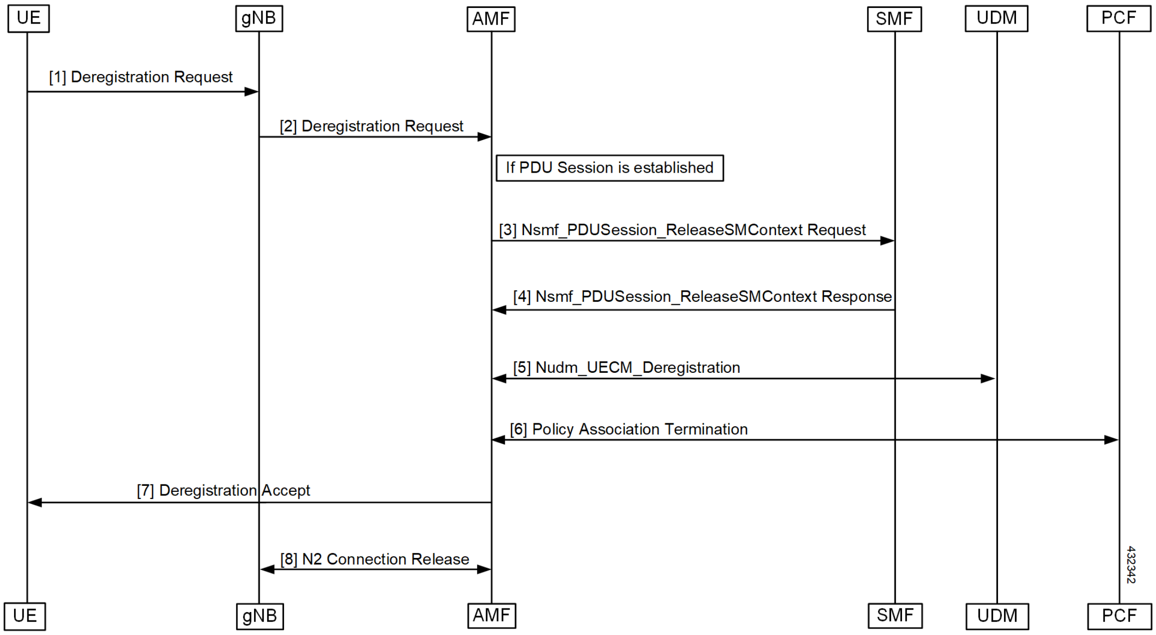

UE
gNB
AMF
SMF
UDM
PCF
[1] Deregistration Request
[2] Deregistration Request
If PDU Session is established
[3] Nsmf_PDUSession_ReleaseSMContext Request
[4] Nsmf_PDUSession_ReleaseSMContext Response
[5] Nudm_UECM_Deregistration
[6] Policy Association Termination
[7] Deregistration Accept
[8] N2 Connection Release
432342
UE
gNB
AMF
SMF
UDM
PCF

Table 24: UE-initiated Deregistration Call Flow Description

Step	Description
1, 2	The UE sends NAS message Deregistration Request (5G-GUTI, Deregistration type, Access Type) to the AMF.

Step	Description
3	If PDU session has been established then AMF sends Nsmf_PDUSession_ReleaseSMContext (SUPI, PDU Session ID) to SMF. All PDU Sessions over the target access, which belong to the UE are released by the AMF by sending Nsmf_PDUSession_ReleaseSMContext Request (SUPI, PDU Session ID) message to the SMF for each PDU Session.
4	The SMF releases all resources (for example, the IP address/Prefixes that were allocated to the PDU Session) and the corresponding User Plane resources. The SMF responds with Nsmf_PDUSession_ReleaseSMContext Response message.
5	The AMF invokes the Nudm_UECM_Deregistration service operation so that the UDM removes the association it had stored.
6	If there is any association with the PCF for this UE and the UE is no more registered over any access, the AMF performs an AMF-initiated AM Policy Association Termination procedure.
7	The AMF sends NAS message Deregistration Accept to UE depending on the Deregistration type i.e. if Deregistration type is switch-off, AMF does not send Deregistration Accept message.
8	N2 UE Context Release.

UDM-initiated Deregistration Call Flow

This section describes the UDM-initiated Deregistration call flow.

UDM initiates deregistration process for an UE if the subscription is withdrawn for the UE. The UDM can trigger this procedure for operator-determined purposes to request the removal of a subscriber's RM context and PDU sessions of the UE.

Figure 22: UDM Initiated Deregistration Call Flow

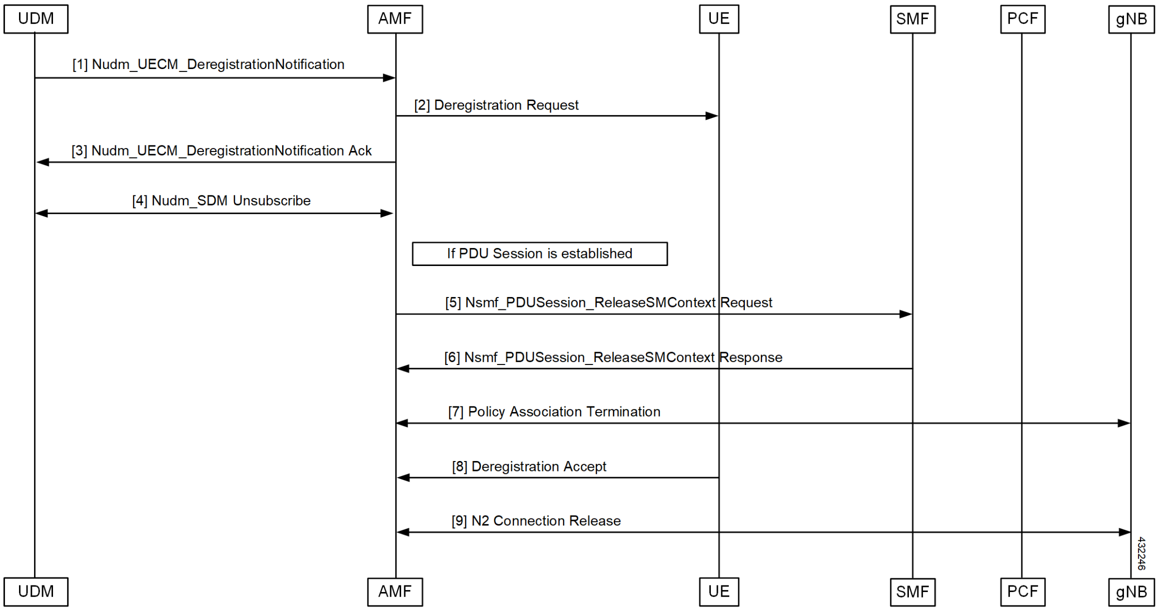

UDM
AMF
UE
SMF
PCF
gNB
[1] Nudm_UECM_DeregistrationNotification
[2] Deregistration Request
[3] Nudm_UECM_DeregistrationNotification Ack
[4] Nudm_SDM Unsubscribe
If PDU Session is established
[5] Nsmf_PDUSession_ReleaseSMContext Request
[6] Nsmf_PDUSession_ReleaseSMContext Response
[7] Policy Association Termination
[8] Deregistration Accept
[9] N2 Connection Release
432246

Table 25: UDM Initiated Deregistration Call Flow Description

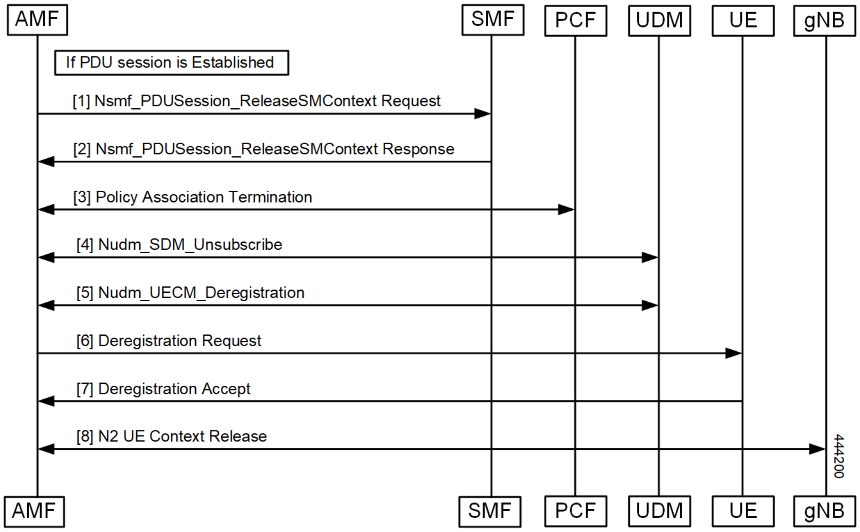
Step	Description
1	If the UDM wants to request the immediate deletion of a subscriber's contexts and PDU Sessions, the UDM shall send a Nudm_UECM_DeregistrationNotification (SUPI, Access Type, Removal Reason) message with Removal Reason set to Subscription Withdrawn to the registered AMF. If the AMF receives Nudm_UECM_DeregistrationNotification with Removal Reason as Subscription Withdrawn, the AMF executes Deregistration procedure over the access.
2	The AMF may explicitly deregister the UE by sending a Deregistration Request message (Deregistration type, Access Type) to the UE. The Deregistration type may be set to Re-registration in which case the UE should re-register at the end of the Deregistration procedure. If the Deregistration Request message is sent over 3GPP access and the UE is in CM-IDLE state in 3GPP access, the AMF pages the UE.
3	If the Deregistration procedure is triggered by UDM ,the AMF acknowledges the Nudm_UECM_DeRegistrationNotification to the UDM.
4	The AMF also unsubscribes with the UDM using Nudm_SDM_Unsubscribe service operation.
5, 6	If the UE has any established PDU Sessions then UE-initiated Deregistration is performed.
7	If there is any association with the PCF for this UE and the UE is no more registered over any access, the AMF performs a AMF-initiated AM Policy Association Termination procedure
8	If the UE receives the Deregistration Request message from the AMF,the UE sends a Deregistration Accept message to the AMF .The NG-RAN forwards this NAS message to the AMF along with the TAI+ Cell identity of the cell which the UE is using.
9	N2 UE Context Release.

AMF-initiated Deregistration Call Flow

This section describes the AMF-initiated Deregistration call flow.

If implicit detach timer expires, AMF performs deregistration.

Figure 23: AMF-initiated Deregistration Call Flow


AMF
SMF
PCF
UDM
UE
gNB
If PDU session is Established
[1] Nsmf_PDUSession_ReleaseSMContext Request
[2] Nsmf_PDUSession_ReleaseSMContext Response
[3] Policy Association Termination
[4] Nudm_SDM_Unsubscribe
[5] Nudm_UECM_Deregistration
[6] Deregistration Request
[7] Deregistration Accept
[8] N2 UE Context Release
44200
AMF
SMF
PCF
UDM
UE
gNB

In case of clear subscriber, AMF triggers a deregistration procedure.

Table 26: AMF-initiated Deregistration Call Flow Description

Step	Description
1	If PDU session has been established then AMF sends Nsmf_PDUSession_ReleaseSMContext (SUPI, PDU Session ID) to SMF. All PDU Sessions over the target access, which belong to the UE are released by the AMF by sending Nsmf_PDUSession_ReleaseSMContext Request (SUPI, PDU Session ID) message to the SMF for each PDU Session.
2	The SMF releases all resources (for example, the IP address/Prefixes that were allocated to the PDU Session) and the corresponding User Plane resources. The SMF responds with Nsmf_PDUSession_ReleaseSMContext Response message.
3	If there is any association with the PCF for this UE and the UE is no more registered over any access, the AMF performs an AMF-initiated AM Policy Association Termination procedure.
4	The AMF unsubscribes with the UDM using Nudm_SDM_Unsubscribe service operation.
5	The AMF invokes the Nudm_UECM_Deregistration service operation so that the UDM removes the association it had stored.
6	The AMF may explicitly deregister the UE by sending a Deregistration Request message (Deregistration type, Access Type) to the UE. The Deregistration type may be set to Re-registration in which case the UE should re-register at the end of the Deregistration procedure. If the Deregistration Request message is sent over 3GPP access and the UE is in CM-IDLE state in 3GPP access, the AMF pages the UE.
7	After UE receives the Deregistration Request message from the AMF, the UE sends a Deregistration Accept message to the AMF .The NG-RAN forwards this NAS message to the AMF along with the TAI+ Cell identity of the cell which the UE is using.
8	N2 UE Context Release.

UE Identity Procedure for Authentication Failure Call Flow

This section describes the UE Identity Procedure for Authentication Failure call flow.

Upon failure of authentication at Step 5, AMF would trigger identity request towards UE and request for an UE identity. Authentication would be proceeded with the new UE identity.

Figure 24: UE Identity Procedure for Authentication Failure Call Flow

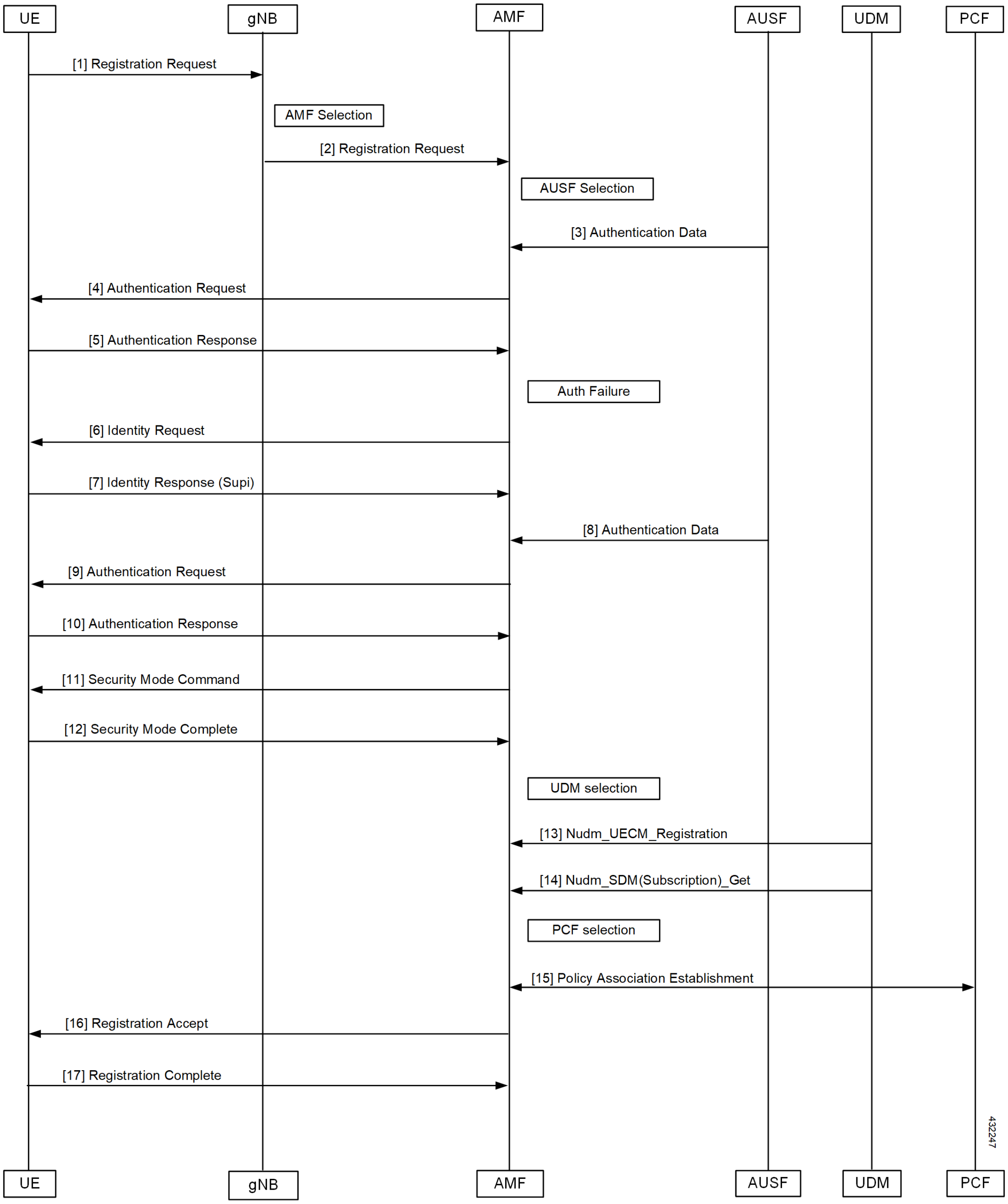

UE
gNB
AMF
AUSF
UDM
PCF
[1] Registration Request
AMF Selection
[2] Registration Request
AUSF Selection
[3] Authentication Data
[4] Authentication Request
[5] Authentication Response
Auth Failure
[6] Identity Request
[7] Identity Response (Supi)
[8] Authentication Data
[9] Authentication Request
[10] Authentication Response
[11] Security Mode Command
[12] Security Mode Complete
UDM selection
[13] Nudm_UECM_Registration
[14] Nudm_SDM(Subscription)_Get
PCF selection
[15] Policy Association Establishment
[16] Registration Accept
[17] Registration Complete
432247
UE
gNB
AMF
AUSF
UDM
PCF

Table 27: UE Identity Procedure for Authentication Failure Call Flow Description

Step	Description
5	During registration procedure when authentication-response is received from UE, the AMF examines the auth-response parameters and confirms that the authentication has failed. In such case, AMF would trigger identity-request to UE asking for its SUCI.
6	UE sends identity-request message to AMF.
7	UE responds with its SUCI in identity-response message to AMF.
8	AMF extracts fresh authentication data from AUSF using the SUCI of subscriber.
9	AMF sends Authentication-Request to the UE to initiate authentication of the UE identity.
10	UE sends Authentication-Response to the AMF to deliver a calculated authentication response to the network. AMF verifies the result received and if the result is as expected then the registration procedure starts.
11	The NAS security initiation is performed.
12	Upon completion of NAS security function setup, the AMF initiates NGAP procedure to provide the 5G-AN with security context .The 5G-AN stores the security context and acknowledges to the AMF. The 5G-AN uses the security context to protect the messages exchanged with the UE.
13	AMF selects an UDM based on the PLMN info via NRF query or via static configuration and registers the UE with the UDM using Nudm_UECM_Registration. The UDM stores the AMF identity associated to the Access Type.
14	The AMF retrieves the Access and Mobility Subscription data using Nudm_SDM_Get. The AMF subscribes to be notified using Nudm_SDM_Subscribe when the data requested is modified.
15	AMF selects PCF based on PLMN-info and slice- info and performs an Policy Association Establishment. PCF sends policy data to AMF with restrictions and other policies to be applied for the UE. Currently the polices are not applied for UE and are just stored in AMF.
16	The AMF sends a Registration Accept message to the UE indicating that the Registration Request has been accepted. Registration Accept contains (5G-GUTI, Registration Area, Mobility restrictions, PDU Session status, Allowed NSSAI, Configured NSSAI for the Serving PLMN, Periodic Registration Update timer, Emergency Service Support indicator, Accepted DRX parameters).
17	The UE sends a Registration Complete message to the AMF to acknowledge that a new 5G-GUTI was assigned.

UE Identity Procedure for Unknown Subscribers Call Flow

This section describes the UE Identity Procedure for Unknown Subscribers call flow.

When registration request is received with unknown GUTI then AMF would trigger identity request towards UE and request for an UE identity. Registration proceeds with the new UE identity.

Figure 25: UE Identity Procedure for Unknown Subscribers Call Flow

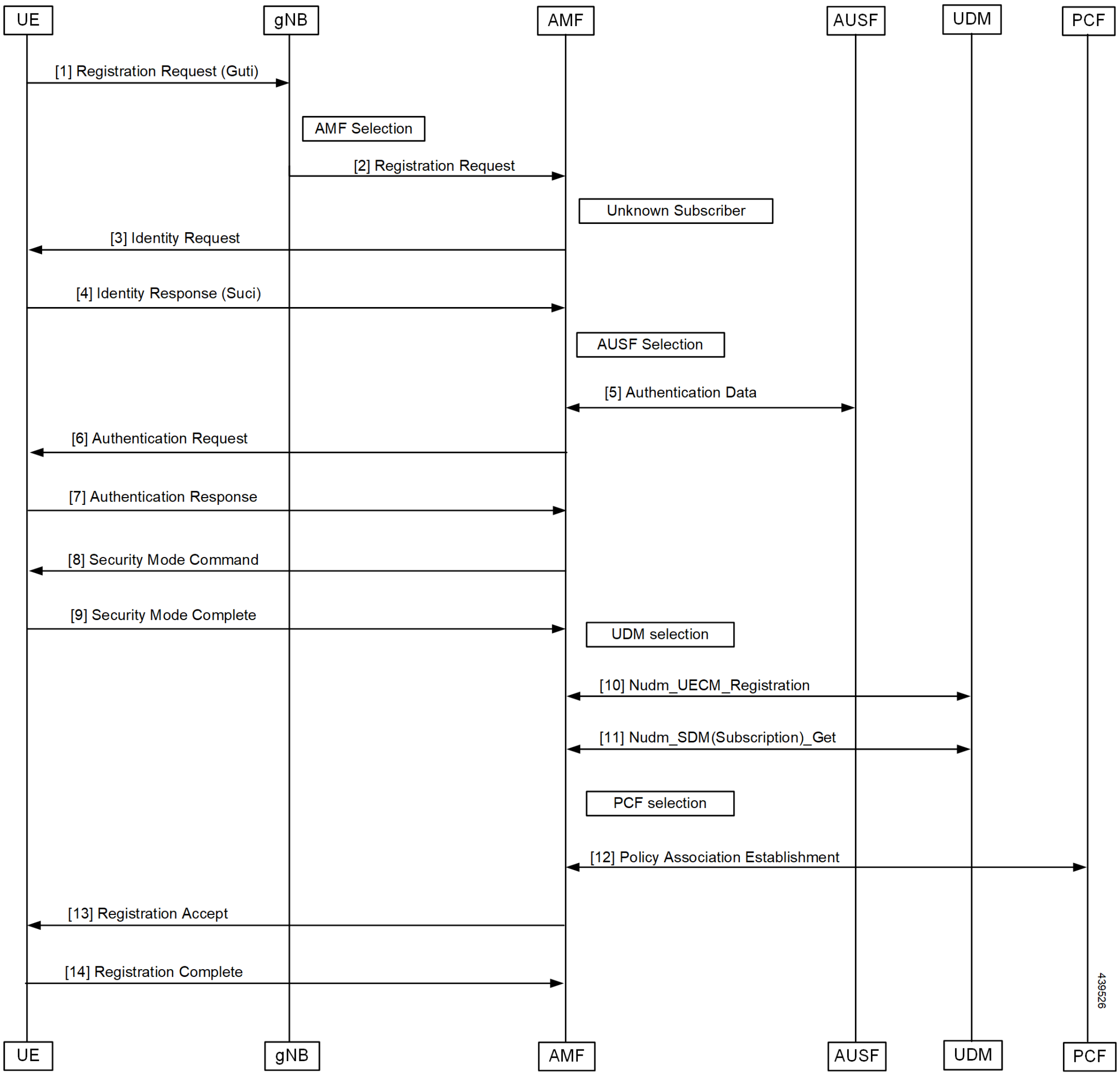

UE
gNB
AMF
AUSF
UDM
PCF
[1] Registration Request (Guti)
AMF Selection
[2] Registration Request
Unknown Subscriber
[3] Identity Request
[4] Identity Response (Suci)
AUSF Selection
[5] Authentication Data
[6] Authentication Request
[7] Authentication Response
[8] Security Mode Command
[9] Security Mode Complete
UDM selection
[10] Nudm_UECM_Registration
[11] Nudm_SDM(Subscription)_Get
PCF selection
[12] Policy Association Establishment
[13] Registration Accept
[14] Registration Complete
439526
UE
gNB
AMF
AUSF
UDM
PCF

Table 28: UE Identity Procedure for Unknown Subscribers Call Flow Description

Step	Description
2	During registration procedure, the AMF determines that the received GUTI is of subscriber which is not present in AMF. In such case, AMF would trigger identity-request to UE asking for its SUCI.
3	UE sends identity-request message to AMF.
4	UE responds with its SUCI in identity-response message to AMF.
5	AMF extracts fresh authentication data from AUSF using the SUCI of subscriber.
6	AMF sends Authentication-Request to the UE to initiate authentication of the UE identity.

Step	Description
7	UE sends Authentication-Response to the AMF to deliver a calculated authentication response to the network. AMF verifies the result received and if the result is as expected then the registration procedure is proceeded.
8	The NAS security initiation is performed.
9	Upon completion of NAS security function setup, the AMF initiates NGAP procedure to provide the 5G-AN with security context .The 5G-AN stores the security context and acknowledges to the AMF. The 5G-AN uses the security context to protect the messages exchanged with the UE.
10	AMF selects an UDM based on the PLMN info via NRF query or via static configuration and registers the UE with the UDM using Nudm_UECM_Registration. The UDM stores the AMF identity associated to the Access Type.
11	The AMF retrieves the Access and Mobility Subscription data using Nudm_SDM_Get. The AMF subscribes to be notified using Nudm_SDM_Subscribe when the data requested is modified.
12	AMF selects PCF based on PLMN-info and slice- info and performs an Policy Association Establishment. PCF sends policy data to AMF with restrictions and other policies to be applied for the UE. Currently the polices are not applied for UE and are just stored in AMF.
13	The AMF sends a Registration Accept message to the UE indicating that the Registration Request has been accepted. Registration Accept contains (5G-GUTI, Registration Area, Mobility restrictions, PDU Session status, Allowed NSSAI, Configured NSSAI for the Serving PLMN, Periodic Registration Update timer, Emergency Service Support indicator, Accepted DRX parameters).
14	The UE sends a Registration Complete message to the AMF to acknowledge that a new 5G-GUTI was assigned.

Configuring Compliance to 3GPP Specification

This section describes how to configure compliance to 3GPP specification.

Configuring Interfaces

The following are sample interface configurations. You need to configure interfaces based on your requirements.

```
config
profile nf-client nf-type ausf
 ausf-profile AUP1
  locality LOC1
   priority 30
   service name type nausf-auth
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 <AUSF IP>
      primary ip-address port <Port number>
     exit
    exit
   exit
  exit
 exit
exit
exit

config
profile nf-client nf-type udm
 udm-profile UP1
  locality LOC1
   service name type nudm-sdm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      primary ip-address ipv4 <UDM IP Address>
      primary ip-address port <Port number>
     exit
    exit
   exit
exit

config
service name type nudm-uecm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 <UDM IP Address>
      primary ip-address port <Port number>
     exit
    exit
   exit
  exit
 exit
exit
exit

config
profile nf-client nf-type pcf
 pcf-profile PP1
  locality LOC1
   priority 30
   service name type npcf-am-policy-control
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 <PCF IP Address>
      primary ip-address port <PCF Port number>
     exit
    exit
   exit
  exit
 exit
exit
exit

config
profile nf-client nf-type amf
 amf-profile AMF1
```

```
  locality LOC1
   priority 56
   service name type namf-comm
    endpoint-profile EP1
     capacity   30
     priority   30
     uri-scheme http
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 <Peer AMF IP Address>
      primary ip-address port <Peer AMF Port number>
     exit
    exit
   exit
  exit
 exit
exit
exit
```

```
config
profile nf-client nf-type smf
 smf-profile SMF1
  locality LOC1
   priority 56
   service name type nsmf-pdusession
    endpoint-profile EP1
     capacity   30
     priority   30
     uri-scheme http
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 <SMF IP Address>
      primary ip-address port <SMF Port number>
     exit
    exit
   exit
  exit
 exit
exit
exit
```

Sample Configuration

The following is a sample output of the interface configuration:

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

CHAPTER 7

Application-based Alerts

Feature Summary and Revision History

Summary Data

Table 29: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 30: Revision History

Revision Details	Release
First introduced.	2021.04.0

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

This section describes how this feature 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 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 the Alert Rules

To configure the alert rules, use the following configuration:

```
config
   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
      end
```

NOTES:

- **alerts rules**—Specify the Prometheus alerting rules.
- **group** *alert_group_name*—Specify 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*—Specify the evaluation interval of the rule group in seconds.
- **rule** *rule_name*—Specify the alerting rule definition. *rule_name* is the name of the rule.

- **expression** *promql_expression*—Specify the PromQL alerting rule expression. *promql_expression* is the alert rule query expressed in PromQL syntax.
- **duration** *duration*—Specify the duration of a true condition before it's considered true. *duration* is the time interval before the alert is triggered.
- **severity** *severity_level*—Specify 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*—Specify 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*—Specify the annotation to attach to the alerts. *annotation_name* is the name of the annotation.
- **value** *annotation_value*—Specify the annotation value. *annotation_value* is the value of the annotation.

Configuration Example

The following is an example configuration.

The following example configures an alert that is triggered when the percentage of registration procedure success is less than the specified threshold limit.

```
config
   alerts rules group AMFProcStatus
   interval-seconds 300
   rule UeRegistration
      expression "sum(amf_procedure_total{proc_type='UE
Registration',proc_status='ProcStatusComplete',status='success'}) /
sum(amf_procedure_total{proc_type='UE Registration',status='attempted'}) < 0.95"
      severity major
      type Communications Alarm
      annotation annotation_name
      value summary
 value "This alert is fired when the UE registration procedure success is below specified
threshold”
      end
```

Configuration Verification

To verify the configuration.

```
show running-config alerts rules group AMFProcStatus
alerts rules group AMFProcStatus
 rule UeRegistration
  expression "sum(amf_procedure_total{proc_type='UE
Registration',proc_status='ProcStatusComplete',status='success'}) /
sum(amf_procedure_total{proc_type='UE Registration',status='attempted'}) < 0.95"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when the UE registration procedure success is below specified
 threshold” "
  exit
 exit
exit
```

Viewing Alert Logger

By default, alert logger stores all the generated alerts. You can view the stored alerts using the following **show** command.

show alert history [detail | summary] [filtering]

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

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

Use the following **show** command to view the history of the alerts configured in the system:

```
show alerts history detail
alerts history detail UEReg 11576e6a86da
 severity    major
 type        "Communications Alarm"
 startsAt    2021-10-24T07:56:24.857Z
 endsAt      2021-10-24T08:31:24.857Z
 source      System
 summary     "fired when ue reg fails"
 labels      [ "alertname: UEReg" "cluster: amf-cndp-b19-4_cee-cisco" "monitor: prometheus"
 "replica: amf-cndp-b19-4_cee-cisco" "severity: major" ]
 annotations [ "summary: fired when ue reg fails" "type: Communications Alarm" ]
```

You can view the active alerts using **show alerts active** command. The alerts remain active as long as the evaluated expression is true.

```
show alerts active detail
alerts active detail UeRegistration 92b6dcdd8726
 severity    major
 type        "Communications Alarm"
 startsAt    2021-10-24T14:56:42.732Z
 source      System
 summary     "This alert is fired when the UE registration procedure success is below
specified threshold"
 labels      [ "alertname: UeRegistration" "cluster: amf-cndp-b19-4_cee-cisco" "monitor:
prometheus" "replica: amf-cndp-b19-4_cee-cisco" "severity: major" ]
 annotations [ "summary: This alert is fired when the UE registration procedure success is
 below specified threshold" "type: Communications Alarm" ]
```

Call Flow Procedure Alerts

This section describes commands that are required to configure alerts related to various call flow procedures.

Paging Success

To configure alerts related to the Paging Success procedure, use the following configuration:

```
alerts rules group AMFProcStatus
 rule Paging
  expression
"sum(amf_procedure_total{proc_type='Paging',proc_status='ProcStatusComplete',status='success'})
 / sum(amf_procedure_total{proc_type='Paging',status='attempted'}) < 0.95"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when the Paging procedure success is below specified threshold"

  exit
 exit
exit
```

Service Request Success

To configure alerts related to the Service Request Success procedure, use the following configuration:

```
alerts rules group AMFProcStatus
 rule ServiceRequest
  expression "sum(amf_procedure_total{proc_type='Service
Request',proc_status='ProcStatusComplete',status='success'}) /
sum(amf_procedure_total{proc_type='Service Request',status='attempted'}) < 0.95"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when the Service request procedure success is below specified
 threshold"
  exit
 exit
exit
```

UE Deregistration Success

To configure alerts related to the UE Deregistration procedure, use the following configuration:

```
alerts rules group AMFProcStatus
 interval-seconds 300
 rule UeDeRegistration
  expression "sum(amf_procedure_total{proc_type='UE
DeRegistration',proc_status='ProcStatusComplete',status='success'}) /
sum(amf_procedure_total{proc_type='UE DeRegistration',status='attempted'}) < 0.95"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when the UE deregistration procedure success is below specified
 threshold"
  exit
 exit
exit
```

UE Registration Success

To configure alerts related to the UE Registration procedure, use the following configuration:

```
alerts rules group AMFProcStatus
 interval-seconds 300
 rule UeRegistration
  expression "sum(amf_procedure_total{proc_type='UE
Registration',proc_status='ProcStatusComplete',status='success'}) /
sum(amf_procedure_total{proc_type='UE Registration',status='attempted'}) < 0.95"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when the UE registration procedure success is below specified
 threshold"
  exit
 exit
exit
```

Message Level Alerts

This section describes commands that are required to configure alerts related to various message.

N1 Registration Accept

To configure alerts related to the N1 Registration Accept Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN1RegistrationSuccess
  expression
"sum(increase(amf_nas_message_total{message_type=~'N1RegistrationAccept_.*'}[5m])) /
sum(increase(amf_nas_message_total{message_type=~'N1RegRequest_RegType_.*'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Registration Accept sent is lesser than
 threshold."
  exit
exit
```

N1 Service Accept

To configure alerts related to the N1 Service Accept Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN1ServiceRequestSuccess
  expression "sum(increase(amf_nas_message_total{message_type='N1ServiceAcc'}[5m])) /
sum(increase(amf_nas_message_total{message_type='N1ServiceReq'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Service Accept sent is lesser than
threshold."
  exit
exit
```

N1 UE Initiated Deregistration

To configure alerts related to the N1 UE Initiated Deregistration Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN1UeInitDeregSuccess
  expression
"sum(increase(amf_nas_message_total{message_type='N1DeRegAccept_UeOriginatingDereg'}[5m]))
 / sum(increase(amf_nas_message_total{message_type='N1DeRegReq_UeOriginatingDereg'}[5m]))
< 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Deregistration Accept sent is lesser
than threshold.”
  exit
exit
```

N1 Network Initiated Deregistration

To configure alerts related to the N1 Network Initiated Deregistration Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN1NwInitDeregSuccess
  expression
"sum(increase(amf_nas_message_total{message_type='N1DeRegAccept_UeTerminatedDereg'}[5m]))
/ sum(increase(amf_nas_message_total{message_type='N1DeRegReq_UeTerminatedDereg'}[5m])) <
0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Deregistration Accept received is lesser
 than threshold.”
  exit
exit
```

N2 ICSR Success

To configure alerts related to the N2 ICSR Success Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN2IcsrSuccess
  expression
"sum(increase(amf_ngap_message_total{message_type='N2InitialContextSetupRsp'}[5m])) /
sum(increase(amf_ngap_message_total{message_type='N2InitialContextSetupReq'}[5m])) < 0.95"

  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Initial Context Setup Response is lesser
 than threshold.”
  exit
exit
```

N2 PDU Setup Success

To configure alerts related to the N2 PDU Setup Success Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN2PduSetupRequestSuccess
```

```
  expression
"sum(increase(amf_ngap_message_total{message_type='N2PduSessResourceSetupRsp'}[5m])) /
sum(increase(amf_ngap_message_total{message_type='N2PduSessResouceSetupReq'}[5m])) < 0.95"

  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Ngap PDU Setup Response is lesser than
 threshold.”
  exit
exit
```

N2 PDU Modify Success

To configure alerts related to the N2 PDU Modify Success Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN2PduModifySuccess
  expression
"sum(increase(amf_ngap_message_total{message_type='N2PduSessResourceModifyRsp'}[5m])) /
sum(increase(amf_ngap_message_total{message_type='N2PduSessResouceModifyReq'}[5m])) < 0.95"

  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Ngap PDU Modify Response is lesser than
 threshold.”
  exit
exit
```

N2 PDU Release Success

To configure alerts related to the N2 PDU Release Success Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN2PduReleaseSuccess
  expression
"sum(increase(amf_ngap_message_total{message_type='N2PduSessResourceReleaseRsp'}[5m])) /
sum(increase(amf_ngap_message_total{message_type='N2PduSessResouceReleaseReq'}[5m])) < 0.95"

  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Ngap PDU Release Response is lesser
than threshold.”
  exit
exit
```

N8 UECM Registration Request

To configure alerts related to the N8 UECM Registration Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN8UecmRegSuccess
  expression "sum(increase(n8_service_stats{message_type='NudmUecmRegistrationRsp',
status='success'}[5m])) /
sum(increase(n8_service_stats{message_type='NudmUecmRegistrationReq', status='success'}[5m]))
```

```
 < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UECM registration  responses received
is lesser than threshold.”
  exit
exit
```

N8 UECM Deregistration Request

To configure alerts related to the N8 UECM Deregistration Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN8UecmDeRegSuccess
  expression "sum(increase(n8_service_stats{message_type='NudmUecmDeRegistrationRsp',
status='success'}[5m])) /
sum(increase(n8_service_stats{message_type='NudmUecmDeRegistrationReq',
status='success'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UECM deregistration  responses received
 is lesser than threshold.”
  exit
exit
```

N8 SDM Data Request

To configure alerts related to the N8 SDM Data Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN8SdmDataReqSuccess
  expression "sum(increase(n8_service_stats{message_type='NudmSdmDataRsp',
status='success'}[5m])) / sum(increase(n8_service_stats{message_type='NudmSdmDataReq',
status='success'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of SDM Data responses received is lesser
than threshold.”
  exit
exit
```

N8 SDM Subscription Request

To configure alerts related to the N8 SDM Subscription Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN8SdmSubscriptionSuccess
  expression "sum(increase(n8_service_stats{message_type='NudmSdmSubscriptionRsp',
status='success'}[5m])) / sum(increase(n8_service_stats{message_type='NudmSdmSubscriptionReq',
 status='success'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of SDM Subscription responses received is
 lesser than threshold.”
  exit
exit
```

N8 SDM Unsubscribe Request

To configure alerts related to the N8 SDM Unsubscribe Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN8SdmUnSubscriptionSuccess
  expression "sum(increase(n8_service_stats{message_type='NudmSdmUnSubscriptionRsp',
status='success'}[5m])) /
sum(increase(n8_service_stats{message_type='NudmSdmUnSubscriptionReq', status='success'}[5m]))
 < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of SDM UnSubscription responses received
is lesser than threshold.”
  exit
exit
```

N8 PCSCF Restoration Request

To configure alerts related to the N8 PCSCF Restoration Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN8PcscfRestorationSuccess
  expression "sum(increase(n8_service_stats{message_type='NudmPcscfRestorationRsp',
status='success'}[5m])) /
sum(increase(n8_service_stats{message_type='NudmPcscfRestorationReq',
status='attempted'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Pcscf Restoration responses sent is
lesser than threshold.”
  exit
exit
```

N11 SM Create

To configure alerts related to the N11 SM Create Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN11SMCreateSuccess
  expression
"sum(increase(rpc_response_total{msg_type='PostSmCtxtsRequestPB',rpc_name='SMF',status_code='201'}[5m]))/
sum(increase(rpc_response_total{msg_type='PostSmCtxtsRequestPB',rpc_name='SMF'}[5m])) <
0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Update SM context responses received
is lesser than threshold.”
  exit
exit
```

N11 SM Release

To configure alerts related to the N11 SM Release Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN11SMReleaseSuccess
  expression
"sum(increase(rpc_response_total{msg_type='PostSmCtxtsReleaseRequest',rpc_name='SMF',status_code='204'}[5m]))
 /
sum(increase(rpc_response_total{msg_type='PostSmCtxtsReleaseRequest',rpc_name='SMF'}[5m]))
  <  0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Release SM context responses received
is lesser than threshold.”
  exit
exit
```

N11 SM Update

To configure alerts related to the N11 SM Update Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN11SMUpdateSuccess
  expression
"sum(increase(rpc_response_total{msg_type='PostSmCtxtsModifyRequestPB',rpc_name='SMF',status_code=~'200|204'}[5m]))
 / sum(increase(rpc_response_total{msg_type='PostSmCtxtsModifyRequestPB',rpc_name='SMF'}[5m]))
 <  0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value This alert is fired when the percentage of Update SM context responses received is
 lesser than threshold.”
  exit
exit
```

N12 UeAuth Req

To configure alerts related to the N12 UeAuth Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN12UeAuthReqSuccess
  expression "sum(increase(n12_service_stats{message_type='NausfUeAuthRsp',
status='success'}[5m])) / sum(increase(n12_service_stats{message_type='NausfUeAuthReq',
status='success'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Ausf UE Auth responses received is
lesser than threshold.”
  exit
exit
```

N15 AM Policy Control Create

To configure alerts related to the N15 AM Policy Control Create Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN15PolicyControlCreateSuccess
  expression "sum(increase(n15_service_stats{message_type='NpcfAmPolicyControlCreateRsp',
status='success'}[5m])) /
sum(increase(n15_service_stats{message_type='NpcfAmPolicyControlCreateReq',
status='success'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of Policy control create  responses received
 is lesser than threshold.”
  exit
exit
```

N15 AM Policy Control Delete

To configure alerts related to the N15 AM Policy Control Delete Request, use the following configuration:

```
alerts rules group AMFSvcStatus
 interval-seconds 300
 rule AMFN15PolicyControlDeleteSuccess
  expression "sum(increase(n15_service_stats{message_type='NpcfAmPolicyControlDeleteRsp',
status='success'}[5m])) /
sum(increase(n15_service_stats{message_type='NpcfAmPolicyControlDeleteReq',
status='success'}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of  Policy control delete responses received
 is lesser than threshold.”
  exit
exit
```

CHAPTER 8

AMF Logging

Feature Summary and Revision History

Summary Data

Table 31: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 32: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF utilizes the common logging framework to generate logs from its microservices.

The supported log levels are:

- Error

- Warn
- Info
- Debug
- Trace

Note Warn level logging takes place during production.

Error

These errors are fatal errors, which can impact service for multiple subscribers. Examples errors are as follows:

- Node discovery of SBA fails after query from NRF and local configuration
- Mandatory IE missing in an NGAP message
- Memory cache startup errors
- Endpoint not found

Warn

These errors impact few specific call-flows majorly, but not blockers of functionality. Example errors are as follows:

- Node discovery of SBA fails but we have more options to retry.
- Mandatory IE missing in a NAS message
- RPC timeout
- Procedural timeout
- Validation failure (not critical)

  Example: Registration rejected as Registration request message received registration type as the Reserved registration type.
- External entity sending unexpected or negative response

  Example: Handover Cancel, Hand over Failure, or Initial Context Setup Failure
- Unexpected value of objects maintained by AMF

  Example: NIL value of transaction
- Unable to fetch a subscriber

Info

This log level purpose is to know information for cause. Examples are as follows:

- Procedural outcome Example: Disabling of ICSR for Registration
- Collision abort, cleanup, suspend, or continue.

Debug

This log level purpose is to get debug messages. Example messages are as follows:

- All external exchanged messages

  Example: Sending Registration accept to UE.
- State machine changes
- Collision detailed logging

Trace

This log level purpose is to get content of all external tracing messages. Example messages are as follows:

- Registration request message
- N1N2 transfer message

How it Works

This section describes how this feature works.

Log Tags

Use log tags to tag the logs for specific procedures which are part of a flow or an event. Enabling of AMF logging takes place at different log levels for different log tags.

Name	Purpose	Example Log tags
AMF service	To capture procedures.	• LogTagReg • LogTagPDU, and so on
Protocol Endpoint	To capture on the interface.	• LogTagNas • LogTagNgap • LogTagNonUE

Name	Purpose	Example Log tags
Rest Endpoint	To capture on the interface.	• LogTagN11 • LogTagN14 • LogTagNRF • LogTagN11OrN14 (N1NMsgTransfer can come from N14/N11 interfaces) and so on

CHAPTER 9

CDL for Multiple AMF Instances

Feature Summary and Revision History

Summary Data

Table 33: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 34: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

Common Data Layer (CDL) can be deployed separately as a common datastore for multiple AMF instances.

The deployment possibilities when the CDL pods come up in the same namespace as that of AMF namespace are:

- CDL created locally in the same namespace per AMF.
- CDL created in a separate namespace common to multiple AMF instances.

Architecture

A network function (NF) consists of the following layers as part of the cloud native architecture:

- Protocol Layer
- Service Layer
- Datastore Layer

The layers in AMF are as follows:

- Protocol Layer—NGAP/NAS over SCTP transport and SBA over REST/HTTP transport

  Example: AMF-protocol and AMF REST-EP

- Service Layer—Business logic of AMF functionality

  Example: AMF-service pod

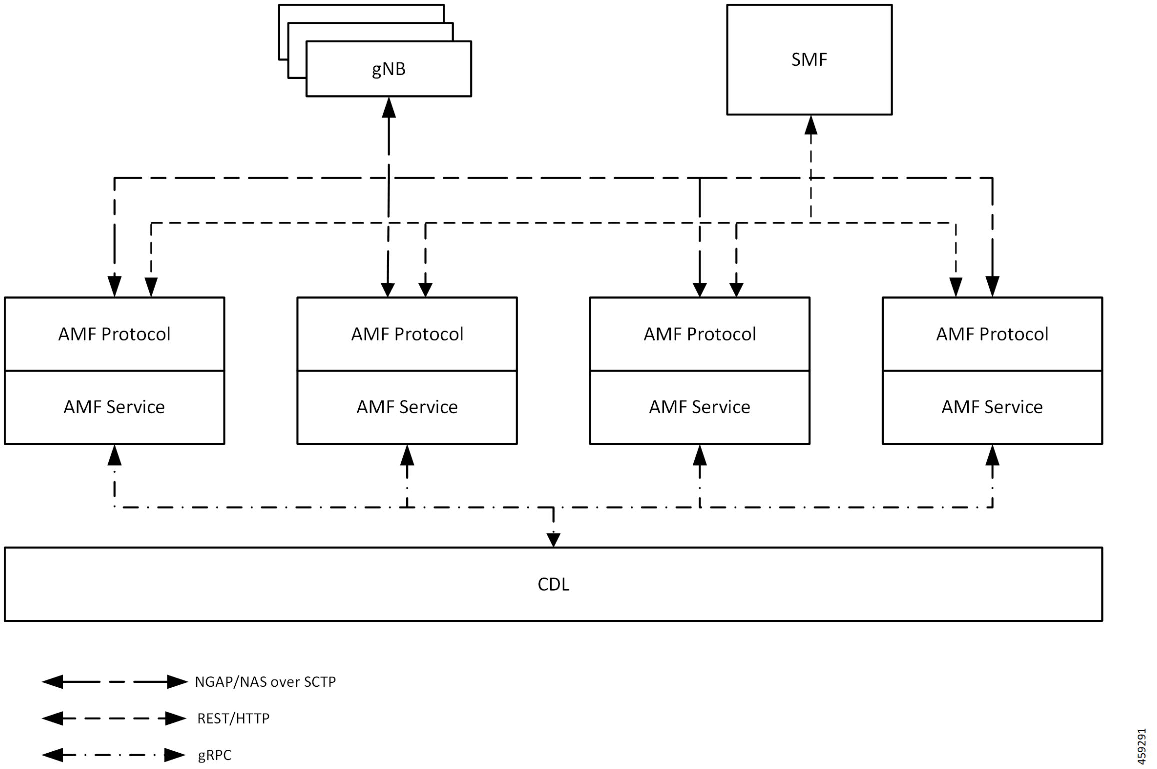
- Data Store Layer—Supports session storage

  Example: CDL

The management entities Etcd, Cache pod, and NodeMgr provide services to the Protocol Layer, Service Layer, and Data Store Layer functionalities.

Figure 26: Multiple AMF Instances Architecture

The following figure explains the Architecture of Multiple AMF instances.



The CDL is deployed as an independent entity which acts as a session store for all the instances of AMF during AMF scaling. Each AMF instance performs the following:

- Uses the common CDL for session store.
- Contains all the elements of AMF deployment.
- Doesn't interact with another AMF instance.
- Registers with NRF service endpoint on instantiation, and deregisters the service endpoint on moving out of service.
- Embeds its instance ID as a pointer in GUAMI identity.

  The gNBs have a mesh connectivity with all the instances of AMF. The SMF and other network elements discover the AMF instances through the NRF.

The CDL can be configured with slice name as AMF to store the AMF sessions. The AMF instance performs the following:

- AMF instance provide instance ID by enhansing the existing session gRPC APIs of CDL or using session-related CDL gRPC APIs..
- Uses the slice name as AMF for session store with CDL.

The CDL exposes the gRPC API to register or deregister notification URI. The AMF instance uses gRPC API to provide the notification URI details to CDL.

The CDL searches for the notification URI in session lookup with instance ID. If the notification URI fails, the CDL picks another URI from the list in round robin.

Feature Configuration

Configuring this feature involves the following steps:

- CDL configuration in same namespace as AMF - This configuration provides the commands to configure CDL locally per AMF in the same namespace. For more information, refer to Configuring the CDL in same namespace as AMF, on page 92.

- CDL configuration in different namespace as AMF - To deploy CDL in different namespace, install CDL Ops Center in a separate namespace. This configuration provides the commands to configure CDL in separate namespace. For more information, refer to Configuring the CDL in different namespace as AMF, on page 93.

Configuring the CDL in same namespace as AMF

The CDL in same namespace as AMF configuration must be done in AMF Ops Center.

To configure CDL in same namespace as AMF, use the following configuration:

```
config
  cdl datastore datastore_name
   endpoint replica no_of_replicas
     slot map no_of_slot_maps
     slot replica no_of_replicas_per_map
     index map no_of_index_maps
     index replica no_of_replicas_per_map
     end
```

NOTES:

- **cdl datastore** *datastore_name*—Specify the name of the datastore to be deployed.

- **endpoint replica** *no_of_replicas*—Specify the number of high availability (HA) instances to be created. Must be an integer in the range of 1–16.

- **slot map** *no_of_slot_maps*—Specify the number of partitions to be created for slot. Must be an integer in the range of 1–1024.

- **slot replica** *no_of_replicas_per_map*—Specify the number of HA instances to be created. Must be an integer in the range of 1–4.

- **index map** *no_of_index_maps*—Specify the number of partitions to be created for index. Must be in the range of 1–1024.

- **index replica** *no_of_replicas_per_map*—Specify the number of HA instances to be created. Must be an integer either 1 or 2.

Configuration Example

The following is an example configuration in CDL Ops Center.

```
config
 cdl datastore session
  endpoint replica 2
```

```
slot map 2
slot replica 2
index map 1
index replica 2
end
```

Configuring the CDL in different namespace as AMF

To configure CDL in a different namespace as AMF, use the following configuration:

```
config
  cdl datastore datastore_name
   endpoint replica no_of_replicas
    slot map no_of_slot_maps
    slot replica no_of_replicas_per_map
    slot notification dynamic-provisioning { true | false }
    index map no_of_index_maps
    index replica no_of_replicas_per_map
    end
```

NOTES:

- **cdl datastore** *datastore_name*—Specify the name of the datastore to be deployed.
- **endpoint replica** *no_of_replicas*—Specify the number of high availability (HA) instances to be created. Must be an integer in the range of 1–16.
- **slot map** *no_of_slot_maps*—Specify the number of partitions to be created for slot. Must be an integer in the range of 1–1024.
- **slot replica** *no_of_replicas_per_map*—Specify the number of HA instances to be created. Must be an integer in the range of 1–4.
- **slot notification dynamic-provisioning true**—Enable application to provide notification endpoint dynamically through API.
- **index map** *no_of_index_maps*—Specify the number of partitions to be created for slot. Must be an integer in the range of 1–1024.
- **index replica** *no_of_replicas_per_map*—Specify the number of HA instances to be created. Must be an integer either 1 or 2.

Note In AMF Ops Center:

- CDL configuration must not be available.
- **show running-config** cdl command must not return the configuration.

Configuration Example

The following is an example configuration in CDL Ops Center.

```
config
 cdl datastore session
```

```
endpoint replica 2
 slot map 2
 slot replica 2
 slot notification dynamic-provisioning true
 index map 1
 index replica 2
 end
```

CHAPTER 10

CMAS Service Support

Feature Summary and Revision History

Summary Data

Table 35: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 36: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

This feature describes broadcasting of warning messages. CBE (Cell Broadcast Entity) broadcasts the warning message to multiple AMFs. Each AMF sends list of gNB or TAI to broadcast the message. One or more NG-RAN nodes schedule the broadcast of the new message and the repetitions in each cell. After the NG-RAN broadcast the warning message, a report is sent back to the AMF from where the message received.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flow for this feature.

CMAS Subscription, Message Delivery, Notification Call Flow

This section describes the CMAS Subscription, Message Delivery, Notification call flow.

Figure 27: CMAS Subscription, Message Delivery, Notification Call Flow

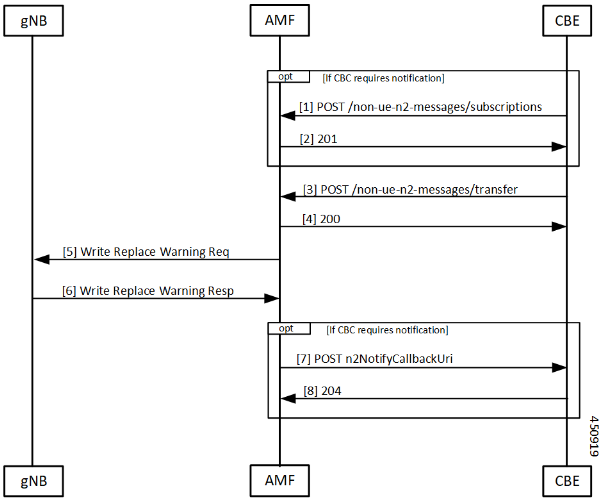

gNB
AMF
CBE
opt
[If CBC requires notification]
[1] POST /non-ue-n2-messages/subscriptions
[2] 201
[3] POST /non-ue-n2-messages/transfer
[4] 200
[5] Write Replace Warning Req
[6] Write Replace Warning Resp
opt
[If CBC requires notification]
[7] POST n2NotifyCallbackUri
[8] 204
450919
gNB
AMF
CBE

Table 37: CMAS Subscription, Message Delivery, Notification Call Flow Description

Step	Description
1	The CBCF creates and sends a NonUeN2InfoSubscribe to the AMF in order to be notified by the NG-RANs about the UE coverage of warning messages sent. The message type is the only parameter for this subscription. The CBE cannot subscribe for a subset of warning messages.
2	The AMF creates a subscription and returns the location of the subscription to the CBE. The CBCF uses this location if it needs to modify or cancel the subscription.
3	The CBCF creates a Write-Replace Warning Request NG-RAN message containing the warning message to broadcast. The message contains Message Identifier, Serial Number, list of NG-RAN TAIs, Warning Area List NG-RAN, OMC ID, CWM Indicator, Send Write-Replace-Warning-Indication, Global RAN Node ID, Warning Area Coordinates. This becomes a binary part to a Non-UE Message Transfer request to the AMF. The CBCF also optionally sends list of TAI or list of gNBs to AMF that need to receive this message.
4	The AMF responds to the CBCF that sending of Warning messages to the gNodeB has started.

Step	Description
5	The AMF determines the set of gNB that need the message needs to be send to. This could be a list of gNB if the CBCF send the list, all gNB in a list of TAI, or all the gNB that are connected to the AMF. The AMF does NOT interpret the binary information that is part of the request. The AMF then sends a WRITE REPLACE WARNING REQUEST to the gNB.
6	The gNB responds to the Warning message after broadcasting it.
7	If the CBCF has registered for notifications, the AMF notifies the CBCF. Each message that is sent by the gNB becomes an individual notification, as the specifications do not allow multiple binary payloads in a single message.
8	The CBCF responds to the notification from the AMF.

Non-UE N2 Messages Subscription Call Flow

This section describes the Non-UE N2 Messages Subscription call flow.

Handling of subscriptions from various peer nodes are identical, irrespective of the requesting entity a CBCF, an LMF, or a peer AMF. Handling of these subscriptions takes place as per message category.

Figure 28: Non-UE N2 Messages Subscription Call Flow

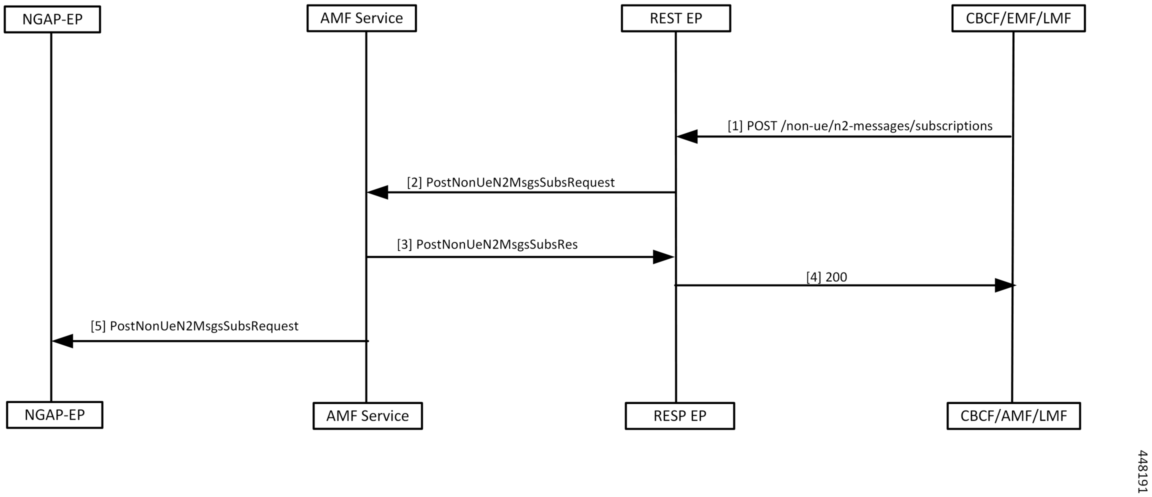

NGAP-EP
AMF Service
REST EP
CBCF/EMF/LMF
[1] POST /non-ue/n2-messages/subscriptions
[2] PostNonUeN2MsgsSubsRequest
[3] PostNonUeN2MsgsSubsRes
[4] 200
[5] PostNonUeN2MsgsSubsRequest
NGAP-EP
AMF Service
RESP EP
CBCF/AMF/LMF
448191

Table 38: Non-UE N2 Messages Subscription Call Flow Description

Step	Description
1	Peer node sends a subscription request to the AMF, which reaches the REST EP. This message is either a PWS-BCAL (Broadcast Completed Area List or Broadcast Cancelled Area List) or PWS-RF (Restart Indication or Failure Indication).
2	REST EP forwards this message to the AMF service.

Step	Description
3	AMF service saves the subscription to the “database” and sends success response to REST EP. The saved subscription contains the URI of the remote node, and the parameters for the subscriptions. The AMF creates a unique location URI for this subscription and includes it in the response.
4	REST EP responds with a 201 to the peer node.
5	AMF service forwards this information to the NGAP EP.

Non-UE N2 Messages Transfer Call Flow

This section describes the Non-UE N2 Messages Transfer call flow.

The AMF does not analyze the binary contents of the received message from any of its peer nodes.

Figure 29: Non-UE N2 Messages Transfer Call Flow

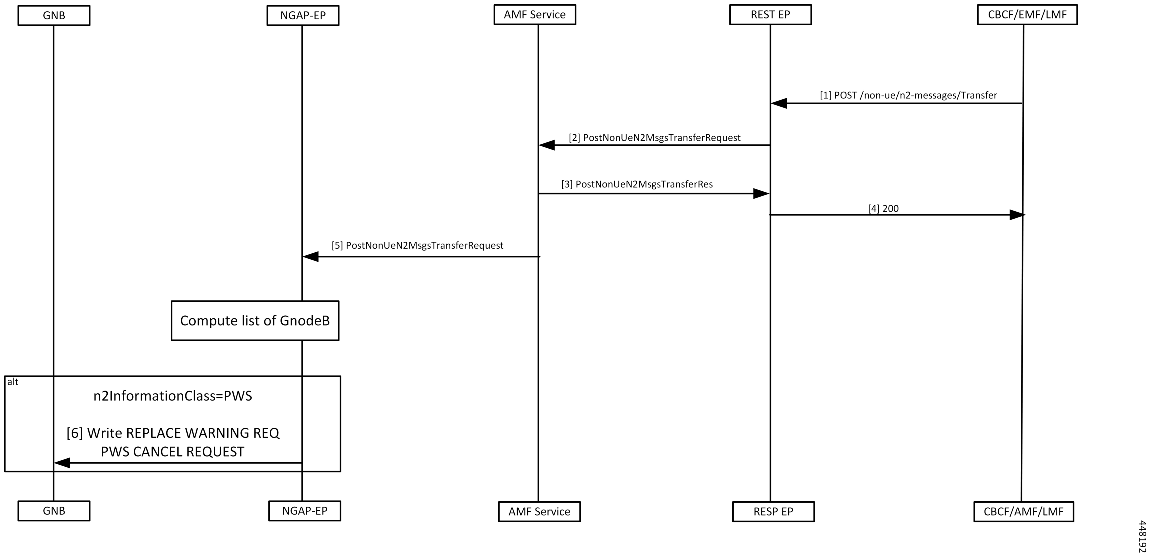

GNB
NGAP-EP
AMF Service
REST EP
CBCF/EMF/LMF
[1] POST /non-ue/n2-messages/Transfer
[2] PostNonUeN2MsgsTransferRequest
[3] PostNonUeN2MsgsTransferRes
[4] 200
[5] PostNonUeN2MsgsTransferRequest
Compute list of GnodeB
alt
n2InformationClass=PWS
[6] Write REPLACE WARNING REQ
PWS CANCEL REQUEST
GNB
NGAP-EP
AMF Service
RESP EP
CBCF/AMF/LMF
448192

Table 39: Non-UE N2 Messages Transfer Call Flow Description

Step	Description
1	Peer node sends a Non-UE N2 message transfer request to the AMF. REST EP receives this request and forwards to the AMF service.

Step	Description
2	AMF does the following while handling warning messages (these messages may contain filters, for example, gNB or TAIs that must match): • Upon receiving the warning message, AMF service checks for protocol errors and returns error response if there is any. • If the warning message contains filters, then it forwards the message to all NG-RANS that match the filters. • If the warning message doesn't contain filters, then it forwards the message to all NG-RANs connected to this AMF. • If the warning message contains filters but no matching NG-RANs then it doesn't send any warning message.
3	If the AMF service can handle this message, it sends success response to the REST EP. • Saves PWS messages to obtain correlation in responses, if the CBCF requests the responses to be send.
4	REST EP sends the response to the peer that sends the request.
5	The AMF service forwards the request to NGAP EP. NGAP EP uses the parameters of the request to find the list of gNodeB to send these messages.
6	NGAP EP forwards the message to gNodeB with the following scenarios: • NGAP copies the N2 payload without any changes, and forwards it to the gNB, when the message has the N2InformationClass set to PWS. • AMF performs the following actions, when the sendRanResp field in PWS Information is True. • Saves the msgIdentifier and serial number of the message. • Saves the notification control block for PWS information.

Non-UE Message Notification Call Flow

This section describes Non-UE Message Notification call flow.

Figure 30: Non-UE Message Notification Call Flow

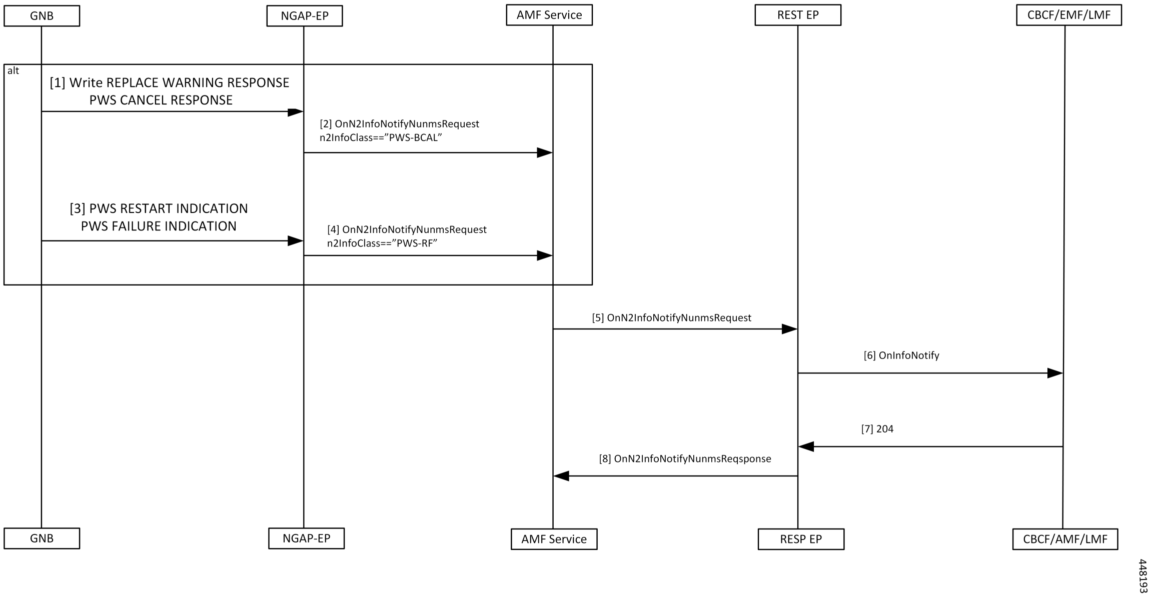


Table 40: Non-UE Message Notification Call Flow description

Step	Description
1	gNB sends a WRITE REPLACE WARNING RESPONSE or PWS CANCEL RESPONSE to NGAP EP.
2	NGAP EP generates a callback with n2InfoClass set to PWS-BCAL with the following conditions. • Subscription for notification for this event is available. • Serial number corresponds to a request originally send with sendRanResponse as True.
3	If the gNB sends a PWS RESTART INDICATOR or a PWS FAILURE INDICATION, it reaches the NGAP EP.
4	If there is a subscription for notification of PWS events, NGAP EP generates a callback with n2InfoClass set to PWS-RF.
5	AMF service forwards the onN2InfoNotifyRequest to REST EP.
6	REST EP sends the message to the peer node.
7	The Peer Node responds with a 204 OK.
8	REST EP forwards the onN2InfoNotifyResponse to AMF.

Non-UE Notification Subscription Deletion Call Flow

This section describes the Non-UE Notification Subscription Deletion call flow.

Upon reception of Non-UE events notification in the AMF, existing subscription gets deleted.

Figure 31: Non-UE-Notification Subscription Deletion Call Flow

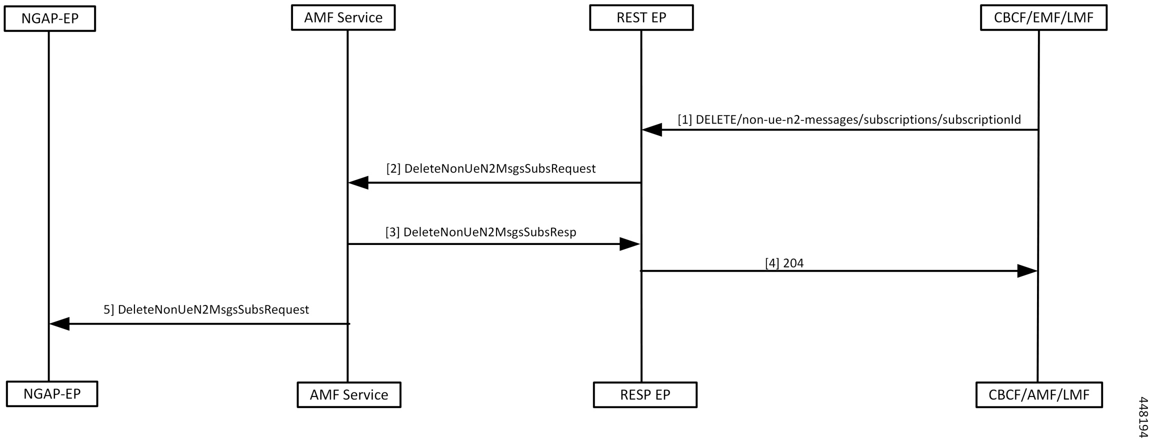

NGAP-EP
AMF Service
REST EP
CBCF/EMF/LMF
[1] DELETE/non-ue-n2-messages/subscriptions/subscriptionId
[2] DeleteNonUeN2MsgsSubsRequest
[3] DeleteNonUeN2MsgsSubsResp
[4] 204
5] DeleteNonUeN2MsgsSubsRequest
NGAP-EP
AMF Service
RESP EP
CBCF/AMF/LMF
448194

Table 41: Non-UE Notification Subscription Deletion Call Flow Description

Step	Description
1	Peer node to the AMF sends a DELETE message with the ID assigned during the subscription process.
2	REST-EP forwards the request to AMF service.
3	AMF service deletes it from the database before sending response to the REST-EP.
4	REST-EP forwards the response to the peer node.
5	AMF service sends the request to NGAP EP to remove existing subscription from NGAP EP.

CHAPTER 11

Dynamic Configuration Change Support for SCTP and SBI Endpoints

Feature Summary and Revision History

Summary Data

Table 42: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 43: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF allows you to configure the SCTP and SBI endpoints dynamically.

This feature supports the following dynamic configurations:

- VIP-IP, Port addition and removal in SCTP endpoint
- TAI addition and removal in SBI
- Slice addition and removal in SBI

Feature Configuration

Configuring this feature involves the following steps:

- SCTP Endpoint Configuration - This configuration provides new SCTP VIP-IP and port addition, removal of existing SCTP VIP-IP and port information. For more information, refer to Configuring the SCTP Endpoint, on page 104.
- SBI Endpoint Configuration - This configuration enables the NRF Registration, Deregistration, or NRF Update using internal VIP. For more information, refer to Configuring the SBI Endpoint, on page 105.
- Internal VIP-IP for the UDP Proxy Configuration - This configuration enables internal communication between UDP proxy and GTPC-EP using internal VIP-IP. For more information, refer to Configuring the Internal VIP-IP for the UDP Proxy, on page 108.

Configuring the SCTP Endpoint

To configure the SCTP endpoint, use the following configuration:

```
config
 instance instance-id instance_id
  endpoint sctp
   vip-ip existing_ipv4_address offline
      vip-ip new_ipv4_address vip-port port_number
   vip-ipv6 existing_ipv6_address offline
      vip-ipv6 new_ipv6_address vip-ipv6-port port_number
   end
```

NOTES:

- **endpoint sctp**—Specify the endpoint name as sctp.
- **vip-ip** *existing_ipv4_address* **offline**—Specify IPv4 address and mark it as offline.
- **vip-ip** *new_ipv4_address* **vip-port** *port_number*—Specify the new IPv4 address and port number.
- **vip-ipv6** *existing_ipv6_address* **offline**—Specify the IPv6 parameters of the pod on which VIP is enabled.
- **vip-ipv6** *new_ipv6_address* **vip-ipv6-port** *port_number*—Specify new IPv6 address and port number.

Use the following procedure to update the SCTP VIP-IP and port is:

1. Add the new VIP-IP port.
2. Modify the gNB configuration to refer to the new VIP-IP and port.
3. When all gNBs refer to new VIP-IP, remove the old VIP-IP and port.

Note Post VIP-IP changes, AMF supports only resuming of IDLE mode subscribers with EEA0/EIA0 as the security algorithm.

Configuration Example

The following is an example configuration for IPv4.

```
config
 instance instance-id 1
  endpoint sctp
   vip-ip 10.1.1.253 offline
    vip-ip 10.2.2.1 vip-port 1000
   end
```

The following is an example configuration for IPv6.

```
config
 instance instance-id 1
   endpoint sctp
    vip-ip 172.16.139.251 vip-port 1001
     vip-ipv6 2001:420:54ff:a4::139:251 vip-ipv6-port 1000
    end
```

Configuring the SCTP VIP-IP Port Removal

When the gNB refers to the new VIP-IP port, remove the older ports.

To configure the SCTP VIP-IP port removal, use the following configuration.

```
config
  instance instance-id instance_id
   endpoint sctp
    no vip-ip existing_ip
    end
```

NOTES:

- **instance instance-id** *instance_id*—Specify the instance ID.
- **endpoint sctp**—Specify the endpoint as sctp.
- **no vip-ip** *existing_ip*—Specify the old IPv4 address and port number that must be removed.

Configuring the SBI Endpoint

Configuring the SBI endpoint involves the following steps:

- Endpoint Configuration - This configuration provides the commands to configure the endpoint. For more information, refer to Configuring the Endpoint, on page 106.
- AMF Registration with NRF - This configuration provides the commands to configure AMF Registration, Deregistration with NRF. For more information, refer to Configuring AMF Registration with NRF, on page 106.

- NRF Profile Update - This configuration provides the commands to configure the trigger to NRF Profile Update. For more information, refer to Configuring the Trigger to NRF Profile Update, on page 107.

Configuring the Endpoint

SBI endpoint changes don't result in the pod restart.

After an existing IP is marked as offline and the new IP is added, the existing sessions continue, and callback URI is considered based on the previously configured IP. After this IP change, the newly registered subscribers have the callback URI based on the new IP.

To configure the SBI endpoint, use the following configuration:

```
config
  instance instance-id instance_id
   endpoint sbi
    vip-ip existing_ip offline
    vip-ip new_ip vip-port port_number
    end
```

NOTES:

- **endpoint sbi**—Specify the endpoint name as sbi.
- **vip-ip** *existing_ip* **offline**—Specify the IPv4 address and mark it as offline.
- **vip-ip** *new_ip* **vip-port** *port_number*—Specify the new IPv4 address.

Note This feature doesn't support multiple SBI endpoint IP configurations during the start of the system.

Configuration Example

The following is an example configuration.

```
config
 endpoint sbi
  vip-ip 10.1.1.253 offline
  vip-ip 10.1.0.1
  end
```

Configuring AMF Registration with NRF

If AMF has no active registration towards NRF, and when AMF adds or removes an SBI endpoint from offline mode, AMF sends a Registration Request towards NRF by sending its NF profile in the Registration Request.

To trigger the AMF registration with NRF when the VIP-IP is offline, use the following configuration:

```
config
  instances instance-id instance_id
   endpoint sbi
    no vip-ip vip_ip_address offline
    end
```

NOTES:

- **instances instance-id** *instance_id*—Specify the instance ID.
- **endpoint sbi**—Specify the endpoint name as SBI.
- **no vip-ip** *vip_ip_address* **offline**—Specify the VIP-IP adress for SBI to remove this endpoint from offline mode.

Configuring the Trigger to NRF Profile Update

When a TAI or slice is added or removed, the AMF notifies the NRF by sending an NF Update request. The request contains the profile with the new TAI or slice information.

Configuring the NRF profile update involves the following steps:

- TAI Addition and Removal - This configuration enables the addition or removal of TAI. For more information, refer to Configuring the TAI Addition and Removal, on page 107.
- Slice Addition - This configuration enables the addition of a slice. For more information, refer to Configuring the Slice Addition, on page 107.
- Slice Removal - This configuration enables the removal of a slice. For more information, refer to Configuring the Slice Removal, on page 108.

Configuring the TAI Addition and Removal

To configure the TAI addition or removal, use the following configuration:

```
config
  tai-group name tai_group_name
    tais name tai_list_name
      mcc mcc
      mnc mnc
        tac list updated_tac_list
        end
```

NOTES:

- **tai-group name** *tai_group_name*—Specify the TAI group name to which the list of TAIs must be added.
- **tais name** *tai_list_name*—Specify the list of TAIs.
- **mcc** *mcc* —Specify the three-digit Mobile Country Code. Must be an integer with three digits.
- **mnc** *mnc*—Specify the two or three-digit Mobile Country Network. Must be an integer with three digits.
- **tac list** *updated_tac_list*—Specify the modified Tracking area code (TAC) list.

Configuring the Slice Addition

To configure an addition of a Slice, use the following configuration:

```
config
  amf-services service_name
    slices name slice_name
      sst sst
      sdt sdt
      end
```

NOTES:

- **amf-services** *service_name*—Specify the AMF service.
- **slices name** *slice_name*—Specify the slice name that must be added to the service.
- **sst** *sst* —Specify the slice or service type to signify the expected network slice behaviour in terms of features and services. Must be an integer in the range of 0–255.
- **sdt** *sdt*—Specify the slice differentiator value. It complements one or more slice or service types to allow differentiation among multiple network slices of the same slice or service type. Must be a hexadecimal.

Configuring the Slice Removal

To configure removal of a Slice, use the following configuration:

```
config
   no amf-services service_name
    slices name slice_name
    end
```

NOTES:

- **amf-services** *service_name*—Specify the AMF service name.
- **slices name** *slice_name*—Specify the slice name that must be removed from the service.

Configuring the Internal VIP-IP for the UDP Proxy

When the internal VIP-IP is configured for the UDP-proxy (protocol) pod, the internal communication between the GTPC-EP and UDP-proxy happens over this IP address. The internal VIP-IP provides a secure channel for communication.

Note The VIP-IP doesn't support dynamic change. To update a VIP-IP, reconfigure the VIP-IP.

To configure the Internal VIP-IP for the UDP proxy, use the following configuration:

```
config
 instance instance-id instance_id
   endpoint protocol
    internal-vip vip_address
    end
```

NOTES:

- **endpoint protocol**—Specify the endpoint name as protocol.
- **instance instance-id** *instance_id*—Specify the instance ID.
- **internal-vip** *vip_address*—Specify the virtual IP address.

CHAPTER 12

EAP and AKA Authentication

Feature Summary and Revision History

Summary Data

Table 44: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 45: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

AMF supports the handling of Extensible Authentication Protocol(EAP)-AKA Prime(AKA') authentication at the AMF.

AMF interacts with the UE and the AUSF while performing the UE registration procedure.

EAP-AKA' authentication is carried over the N12 interface with the AUSF.

When the AMF receives the Authentication Response from the AUSF, it carries the EAP payload back and forth between the AUSF and the UE. The AMF carries this payload until it’s successful or failed.

AMF supports optional message of Authentication Response from the AUSF.

Note The notification received after a successful Authentication Response isn’t supported.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

EAP-AKA'-based Authentication Call Flow

This section describes the EAP-AKA'-based Authentication basic call flow.

Figure 32: EAP-AKA'-based Authentication Call Flow

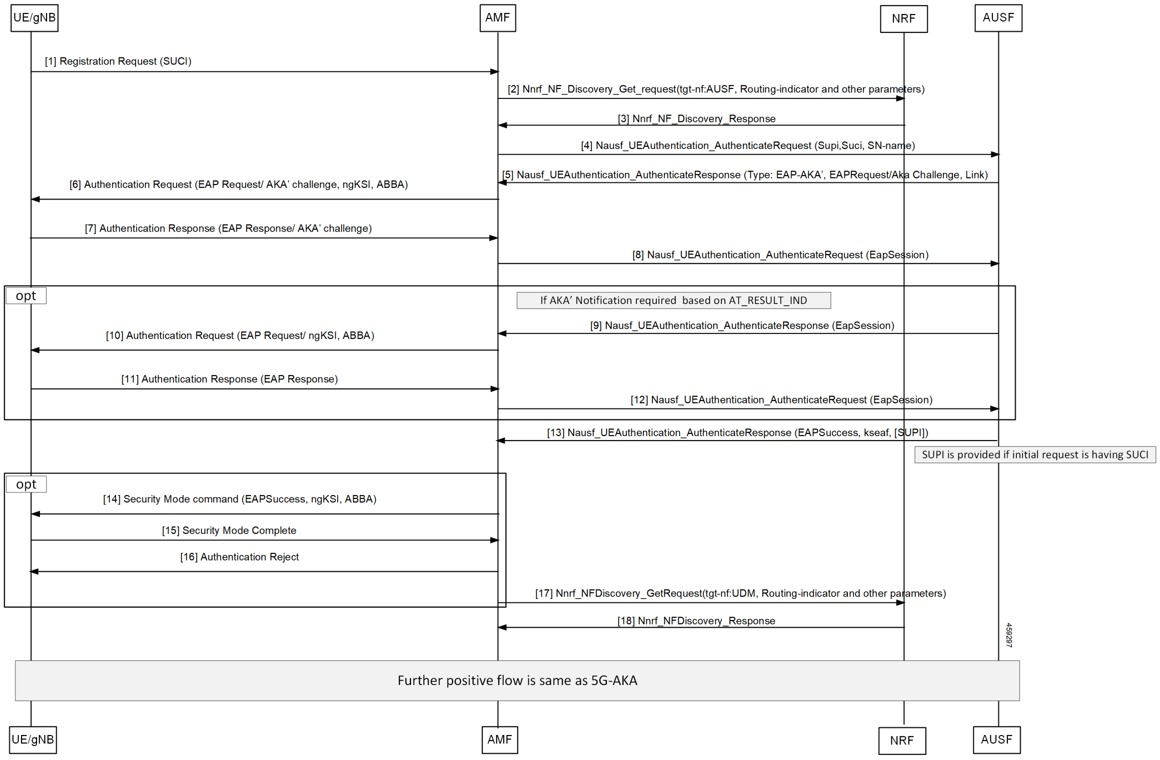

UE/gNB
AMF
NRF
AUSF
[1] Registration Request (SUCI)
[2] Nnrf_NF_Discovery_Get_request(tgt-nf:AUSF, Routing-indicator and other parameters)
[3] Nnrf_NF_Discovery_Response
[4] Nausf_UEAuthentication_AuthenticateRequest (Supi,Suci, SN-name)
[5] Nausf_UEAuthentication_AuthenticateResponse (Type: EAP-AKA’, EAPRequest/Aka Challenge, Link)
[6] Authentication Request (EAP Request/ AKA’ challenge, ngKSI, ABBA)
[7] Authentication Response (EAP Response/ AKA’ challenge)
[8] Nausf_UEAuthentication_AuthenticateRequest (EapSession)
opt
If AKA’ Notification required based on AT_RESULT_IND
[9] Nausf_UEAuthentication_AuthenticateResponse (EapSession)
[10] Authentication Request (EAP Request/ ngKSI, ABBA)
[11] Authentication Response (EAP Response)
[12] Nausf_UEAuthentication_AuthenticateRequest (EapSession)
[13] Nausf_UEAuthentication_AuthenticateResponse (EAPSuccess, kseaf, [SUPI])
SUPI is provided if initial request is having SUCI
opt
[14] Security Mode command (EAPSuccess, ngKSI, ABBA)
[15] Security Mode Complete
[16] Authentication Reject
[17] Nnrf_NFDiscovery_GetRequest(tgt-nf:UDM, Routing-indicator and other parameters)
[18] Nnrf_NFDiscovery_Response
459297
Further positive flow is same as 5G-AKA
UE/gNB
AMF
NRF
AUSF

Table 46: EAP-AKA'-based Authentication basic Call Flow Description

Step	Description
1	gNB sends the Registration Request along with SUCI information to the AMF.
2, 3	AMF sends Nnrf_NF_Discovery_Get_request with tgt-nf: AUSF, Routing-indicator, and other parameters to the NRF, and receives Nnrf_NF_Discovery_Response from the NRF.
4, 5	AMF sends Nausf_UEAuthentication_AuthenticateRequest with SUPI, SUCI, and SN-name to the AUSF. AMF receives Nausf_UEAuthentication_AuthenticateResponse with type: EAP-AKA’, EAPRequest/AKA' challenge, and link from the AUSF.
6, 7	AMF sends the Authentication Request (EAP Request/AKA’ challenge, ngKSI, ABBA) to the UE and receives the Authentication Response with the EAP Response/AKA’ challenge from the UE.
8, 9	AMF sends the Nausf_UEAuthentication_AuthenticateRequest (EapSession) to the AUSF and receives Nausf_UEAuthentication_AuthenticateResponse (EapSession) from the AUSF.
10, 11	The AMF sends the Authentication Request with EAP Request/ngKSI, ABBA to the UE and receives the Authentication Response (EAP Response) from the UE.
12, 13	AMF sends the Nausf_UEAuthentication_AuthenticateRequest (EapSession) to the AUSF and receives the Nausf_UEAuthentication_AuthenticateResponse with EAPSuccess, kseaf, and SUPI from the AUSF.
14, 15	AMF sends the Security Mode command with EAPSuccess, ngKSI, ABBA to UE and receives the Security Mode Complete from the UE.
16	AMF sends the Authentication Reject to the UE for Authentication Failure.
17, 18	AMF sends the Nnrf_NFDiscovery_GetRequest with tgt-nf: UDM, Routing-indicator, and other parameters to the NRF, and receives the Nnrf_NFDiscovery_Response from the NRF.

CHAPTER 13

Encryption and Integrity Protection

Feature Summary and Revision History

Summary Data

Table 47: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 48: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

The AMF supports the following encryption and integrity protection algorithms to enable encryption and integrity protection on the N1/N2 interface:

- EEA0/EIA0
- EEA1/EIA1
- EEA2/EIA2

How it Works

This section describes how this feature works.

The UE Security Capability IE, received from the UE in Registration Request, is used by the network to indicate which security algorithms are supported by the UE for NAS security. The AMF creates a new security context for the UE and does the negotiation of encryption and integrity protection algorithms. These algorithms are configurable along with the priority of negotiation. The AMF compares the algorithms supported by the UE with configuration priority and selects the algorithms to be used for encryption and integrity protection. When integrity protection is disabled, ciphering is also auto-disabled.

In addition, the NasSubscriber database is a new database that stores the UE security context for both the AMF application and the protocol layer to access. The AMF application stores the derived keys and negotiated algorithms in the NasSubscriber database before sending the security mode command to the UE. The AMF protocol encodes the packets received from the AMF application and initiates the encryption and integrity protection based on the negotiated algorithm and the downlink Nas count.

The AMF extracts the security header from the packets to verify integrity protection in the uplink path. After verification, the AMF protocol deciphers the packets before sending it to the AMF application.

Call Flows

This section describes the key call flows for this feature.

UE Registration with Encryption/Integrity Protection Call Flow

The section describes the UE registration procedure with encryption/integrity protection call flow.

Figure 33: UE Registration with Encryption/Integrity Protection Call Flow

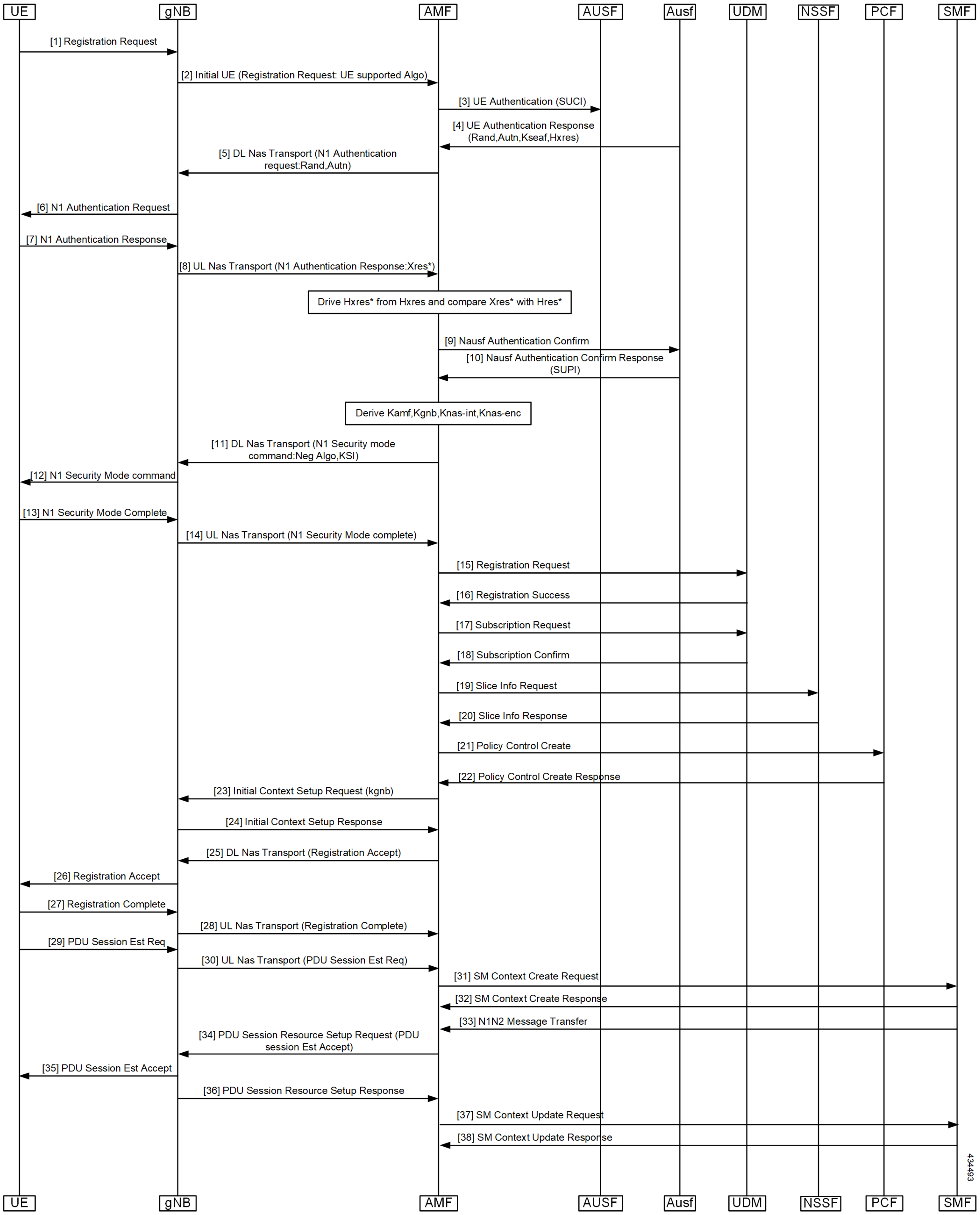

UE
gNB
AMF
AUSF
Ausf
UDM
NSSF
PCF
SMF
[1] Registration Request
[2] Initial UE (Registration Request: UE supported Algo)
[3] UE Authentication (SUCI)
[4] UE Authentication Response (Rand,Autn,Kseaf,Hxres)
[5] DL Nas Transport (N1 Authentication request:Rand,Autn)
[6] N1 Authentication Request
[7] N1 Authentication Response
[8] UL Nas Transport (N1 Authentication Response:Xres*)
Drive Hxres* from Hxres and compare Xres* with Hres*
[9] Nausf Authentication Confirm
[10] Nausf Authentication Confirm Response (SUPI)
Derive Kamf,Kgnb,Knas-int,Knas-enc
[11] DL Nas Transport (N1 Security mode command:Neg Algo,KSI)
[12] N1 Security Mode command
[13] N1 Security Mode Complete
[14] UL Nas Transport (N1 Security Mode complete)
[15] Registration Request
[16] Registration Success
[17] Subscription Request
[18] Subscription Confirm
[19] Slice Info Request
[20] Slice Info Response
[21] Policy Control Create
[22] Policy Control Create Response
[23] Initial Context Setup Request (kgnb)
[24] Initial Context Setup Response
[25] DL Nas Transport (Registration Accept)
[26] Registration Accept
[27] Registration Complete
[28] UL Nas Transport (Registration Complete)
[29] PDU Session Est Req
[30] UL Nas Transport (PDU Session Est Req)
[31] SM Context Create Request
[32] SM Context Create Response
[33] N1N2 Message Transfer
[34] PDU Session Resource Setup Request (PDU session Est Accept)
[35] PDU Session Est Accept
[36] PDU Session Resource Setup Response
[37] SM Context Update Request
[38] SM Context Update Response
434493
UE
gNB
AMF
AUSF
Ausf
UDM
NSSF
PCF
SMF

Table 49: UE Registration with Encryption/Integrity Protection Call Flow Description

Step	Description
1	UE Registration with Encryption/Integrity Protection UE sends registration request to gNB.
2	gNB sends Initial UE Registration Request to AMF.
3	AMF sends UE Authentication (SUCI) to AUSF.
4	AUSF sends UE Authentication Response with Rand, Autn, Kseaf and Hxres information to AUSF.
5	AMF sends DL Nas Transport with N1 Authentication request with Rand and Autn to gNB.
6, 7	gNB sends N1 authentication request to UE and receives N1 Authentication Response from it.
8	gNB sends UL Nas Transport message N1 Authentication Response:Xres* to AMF.
9, 10	AMF derives HXres* from HXres and compares Xres* with Hres*. It sends Nausf suthentication Confirm to AUSF and receives response with SUPI from it.
11	AMF derives Kamf, Kgnb, Knas-int and Knas-enc. It sends DL Nas Transport (N1 Security mode command:Neg Algo,KSI) to gNB.
12	gNB sends N1 Security mode command to UE.
13	UE sends N1 Security Mode Complete to gNB.
14	gNB sends UL Nas Transport (N1 Security Mode complete) to AMF.
15, 16	AMF sends Registration Request to UDM and receives Registration Success from it.
17, 18	AMF sends Subscription Request to UDM and receives Subscription Confirm from it.
19, 20	AMF sends Slice Info Request to NSSF and receives Slice Info Response from it.
21, 22	AMF sends Policy Control Create to PCF and receives Policy Control Create Response from it.
23, 24	AMF sends Initial Context Setup request (kgnb) to gNB and receives response from it.
25, 26	AMF sends DL Nas Transport (Registration Accept) message to gNB. gNB forwards it to UE.
27, 28	UE sends Registration Accept to gNB. gNB forwards this message in UL Nas Transport to AMF.
29, 30	UE sends PDU Session Estblishment Request message to gNB. gNB forwards this message in UL Nas Transport to AMF.
31, 32	AMF sends SM context Create Request message to SMF and receives response from it.
33	SMF sends N1N2 Message Transfer message to AMF.
34	AMF sends PDU Session Resource setup request (PDU session Estb Accept) to gNB.
35, 36	gNB sends PDU Session Resource setup request to UE and receives PDU Session resource setup response from it.

Step	Description
37, 38	AMF sends SM Context Update Request to SMF and receives response from it.

UE Access and Authentication Request Call Flow

The section describes the UE access and Authentication Request procedure call flow.

Figure 34: UE Access and Authentication Request Call Flow

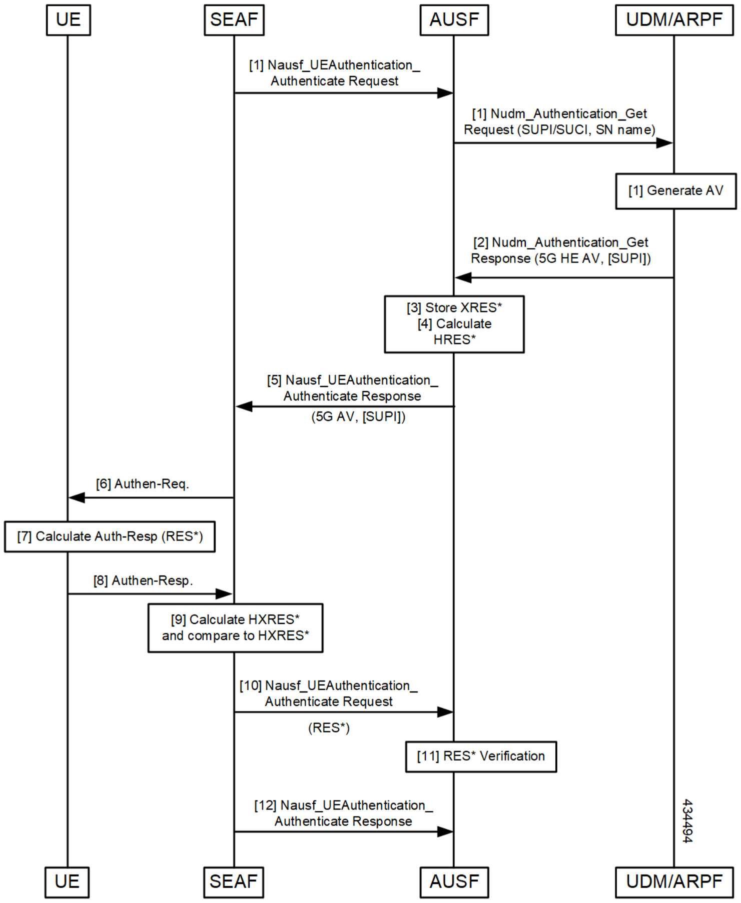

UE
SEAF
AUSF
UDM/ARPF
[1] Nausf_UEAuthentication_ Authenticate Request
[1] Nudm_Authentication_Get Request (SUPI/SUCI, SN name)
[1] Generate AV
[2] Nudm_Authentication_Get Response (5G HE AV, [SUPI])
[3] Store XRES*
[4] Calculate HRES*
[5] Nausf_UEAuthentication_ Authenticate Response
(5G AV, [SUPI])
[6] Authen-Req.
[7] Calculate Auth-Resp (RES*)
[8] Authen-Resp.
[9] Calculate HXRES* and compare to HXRES*
[10] Nausf_UEAuthentication_ Authenticate Request
(RES*)
[11] RES* Verification
[12] Nausf_UEAuthentication_ Authenticate Response
434494
UE
SEAF
AUSF
UDM/ARPF

Table 50: UE Access and Authentication Request Call Flow Description

Step	Description
1	SEAF sends Nausf_UE_Authentication Request to AUSF. AUSF sends Nausf_UE_Authentication_Get Request with SUPI/SUCI and SN name to UDM/ARPF.
2	UDM/ARPF sends Nudm_Authentication_Get response to AUSF.
3, 4, 5	AUSF stores XRES and calculates HRES. It sends Nudm_Authentication_Get response to SEAF.
6	SEAF sends Authentication Response to UE.

Step	Description
7, 8	UE calculates Auth-Rsp and sends Authentcation response to SEAF.
9, 10	SEAF sends HXRES* and sends Nausf_UEAuthentication_Authenticate Request to AUSF.
11, 12	AUSF does RES* verification and sends Nausf_UEAuthentication_Authenticate Response to SEAF.

Feature Configuration

This section describes how to configure AMF Ciphering Algorithm.

This feature is configured under the amf-global configuration.

The supi-policy is configured per subscriber or for a group of subscribers. It’s done by associating the supi/supi-prefix with the supi policy. The operator policy name is configured under supi-policy and the call-control profile is configured under operator policy. Under call-control policy, authentication timer, retry, and security algorithms are configured.

To configure this feature, use the following configuration.

```
config
  amf-global
   call-control-policy call_control_policy_name
      timers t3560
       value time_value
       retry retry_value
      exit
      security-algo security_algo_priority
       ciphering-algo  [5G-EA0 | 128-5G-EA1 | 128-5G-EA2]
       integity-prot-algo [5G-IA0 | 128-5G-IA1 | 128-5G-IA2]
      exit
   operator-policy operator_policy_name
      ccp-name ccp_name
   exit
   supi-policy supi_policy_name
     operator-policy-name operator_policy_name
     end
```

NOTES:

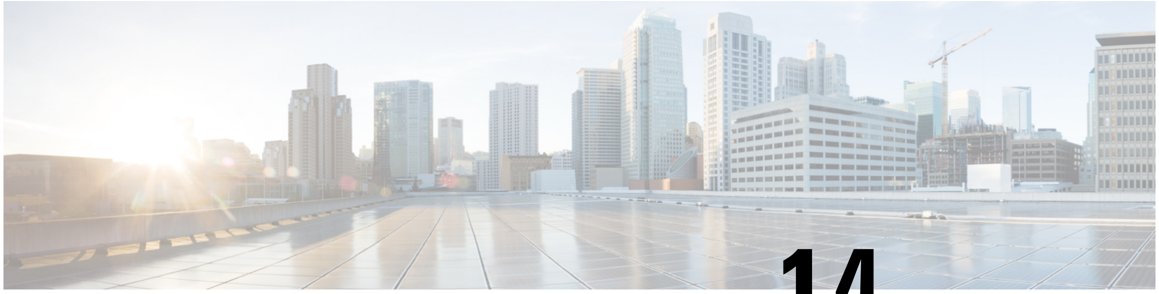
- **call-control-policy** *call_control_policy_name*—Specify the call control policy name.
- **security-algo***security_algo_priority*—Specify the priority of security algorithms. Its values are 1, 2, 3.
- **ciphering-algo [5G-EA0 | 128-5G-EA1 | 128-5G-EA2]**—Specify the Ciphering algorithm to use.
- **integity-prot-algo [5G-IA0 | 128-5G-IA1 | 128-5G-IA2]**—Specify the Integrity protocol algorithm to use.
- **operator-policy** *operator_policy_name*—Specify the operator policy name.
- **supi-policy** *supi_policy_name*—Specify the SUPI policy name. SUPI policy name is the number which represents PLMN ID.

Example: `amf-global supi-policy 223556 operator-policy-name local`

Configuration Example

The following is an example configuration.

```
config
  amf-global
    call-control-policy local
      timers t3560
      value 10
      retry 3
    security-algo 1
      ciphering-algo 128-5G-EA1
      ciphering-algo 128-5G-EA1
    exit
  operator-policy local
     ccp-name local
  exit
  supi-policy 123
    operator-policy-name local
    end
```



CHAPTER 14

Evolved Packet System Fallback Support

Feature Summary and Revision History

Summary Data

Table 51: Summary Data

Applicable Products or Functional Area	AMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 52: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

Based on the presence or absence of the N26 interface, Evolved Packet System (EPS) Fallback opts to switch or redirect to EPS.

The AMF performs and involves in the following activities:

- It supports the IMS voice over PS (VoPS) session and indicates towards the UE during the Registration procedure.
- It sends the value of **redirection-eps-fallback** information elements towards the gNodeB.
- The **redirection-eps-fallback** IE is based on the UE 5GMM capability to support Request Type flag **handover** and CLI configuration for **redirection-eps-fallback**.

This feature supports the following functionalities:

- 5GS interworking without N26 interface indicator in Registration Accept.
- Redirection for EPS fallback for voice as part of the ICSR
- Handover Request and Path Switch Request ACK to fill Redirection IE.
- N26, Xn, and N2 handovers

Feature Configuration

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy ccp_name
         feature-support-ie
            [no] iwk-n26-supported
            [no] redirection-eps-fallback { not-supported | supported }
            end
```

Note As a default action, the AMF doesn't send the redirection information element (Redirection IE). It's sent only to RAN, which is based on the value of CLI, and capability of UE.

NOTES:

- **call-control-policy** *ccp_name*—Specify and configure the Call Control Policy or Profile, as applicable.
- **feature-support-ie**—Configure and specify about supported or unsupported AMF or 5GC features.
- **iwk-n26-supported**—Specify the supported N26 interface indicator in 5GS network feature support. It's applied only when the indicator for N26 interface in 5GS network feature is in supported state. Otherwise, if not supported, no reference of the status is mentioned for the unsupported status.
- **redirection-eps-fallback**—Configure the UE support and redirection for the EPS Fallback for voice, as a part of ICSR.
- **not-supported | supported**—Specify if the support is available or not. The not-supported option indicates that 5G VoPS 3GPP support is disabled.
- **5G IMS Voice over Packet-Switched (VoPS) 3GPP Sessions**—Specify if the UE capability support is enabled or not. Also, to specify, if the UE configuration is enabled with the UE Radio capability or not. The default value is true, indicating it's a supported value.

Configuration Example

The following is an example configuration.

```
config
    amf-global
        call-control-policy CCP1
            feature-support-ie iwk-n26-supported
            feature-support-ie redirection-eps-fallback supported
            end
```

CHAPTER 15

Failure/Exception Handling Framework Support

Feature Summary and Revision History

Summary Data

Table 53: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 54: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Support for Failure/Exception Handling Framework

AMF can now handle errors that occur during procedures. The messaging between the AMF-Service and the protocols have enough information so that when an error reaches the AMF-Service, it can determine:

- Whether the error was internal (for example, node selection failure, NRF discovery failure) or a NOT OK status code was returned by a protocol.
- The protocol or entity that generated the error.
- An error code itself

Error Handling on UDM Interface

SDM Errors

The following errors are expected on UDM interface during the GET Operation, and causes the actions described below:

Table 55: SDM Errors - 1

Application Error	Description	NAS Cause Code	Action
404 Not Found			
DATA_NOT_FOUND	The requested UE subscription data is not found/does not exist. This error is applicable to all Nudm_SDM GET operations.	#7, 5GS services not allowed	Registration Reject
USER_NOT_FOUND	The user does not exist.	#7, 5GS services not allowed	Registration Reject

The following errors are not expected. If they occur, it is either due to a logic miss or a complicated race condition.

Table 56: SDM Errors - 2

Application Error	Description	Response to UE
404 Not Found		
CONTEXT_NOT_FOUND	It is used during the modification of an existing subscription when no corresponding context exists.	Need to respond with cause #9, UE Identity Not Derived By Network

UECM Errors

The following errors are expected on UECM interface during the POST Operation, and causes the actions described below:

Table 57: UECM Errors - 1

Application Error	Description	NAS Cause Code/Action
403 Forbidden		
UNKNOWN_5GS_SUBSCRIPTION	No 5GS subscription is associated with the user.	#7, 5GS services not allowed
NO_PS_SUBSCRIPTION	No PS (5GS, EPS, GPRS) subscription is associated with the user.	#7, 5GS services not allowed
ROAMING_NOT_ALLOWED	The subscriber is not allowed to roam within that PLMN.	#13, Roaming not allowed in the tracking area
ACCESS_NOT_ALLOWED	Access type is not allowed for the user.	#7, 5GS services not allowed
RAT_NOT_ALLOWED	RAT is not allowed for the user.	#7, 5GS services not allowed
INVALID_GUAMI	The AMF is not allowed to modify the registration information stored in the UDM as it is not the registered AMF.	#15, No suitable cells in tracking area
404 Not Found		
USER_NOT_FOUND	The user does not exist in the HPLMN.	#7, 5GS services not allowed
CONTEXT_NOT_FOUND	It is used when no corresponding context exists.	#15, No suitable cells in tracking area

The following errors are not expected. If they occur, it is due to a logic error. Since AMF always rejects a message in this state, the error should be logged, and the call must be rejected with `NO SUITABLE CELLS IN TRACKING AREA`.

Table 58: UECM Errors - 2

Application Error	Description	Response to UE
422 Unprocessable Entity		
UNPROCESSABLE_REQUEST	The request cannot be processed due to semantic errors when trying to process a patch method.	Registration Reject with Cause #111, protocol error unspecified

Error Handling on AUSF Interface

Table 59: AUSF Interface Errors

Application Error	Description	NAS Cause Code	Response to UE
403 Forbidden			
SERVING_NETWORK_ NOT_AUTHORIZED	The serving network is not authorized. For example, serving PLMN	#11, PLMN not allowed	Registration Reject
AUTHENTICATION_ REJECTED	The user cannot be authenticated with this authentication method. For example, only SIM data available	#3, Illegal UE	Registration Reject
INVALID_HN_PUBLIC_ KEY_IDENTIFIER	Invalid HN public key identifier received.	#3, Illegal UE	Registration Reject
INVALID_SCHEME_ OUTPUT	SUCI cannot be decrypted with received data.	#3, Illegal UE	Registration Reject
404 Not Found			
CONTEXT_NOT_FOUND	The AUSF cannot found the resource corresponding to the URI provided by the NF Service Consumer.	#7, 5GS services not allowed	Registration Reject
USER_NOT_FOUND	The user does not exist in the HPLMN.	#7, 5GS services not allowed	Registration Reject
501 Not implemented			
UNSUPPORTED_ PROTECTION_SCHEME	The received protection scheme is not supported by HPLMN.	#11, PLMN not allowed	Registration Reject

The following errors are temporary. The AMF rejects the request from the UE so that it can try another network.

Table 60: Temporary Errors

AUSF Application Error	HTTP Status Code	Description
UPSTREAM_SERVER_ERROR	504 Gateway Timeout	Registration Reject with cause #15, No suitable cells in tracking area

AUSF Application Error	HTTP Status Code	Description
NETWORK_FAILURE	504 Gateway Timeout	Registration Reject with cause #15, No suitable cells in tracking area
AV_GENERATION_ PROBLEM	500 Internal Server Error	Registration Reject with cause #15, No suitable cells in tracking area

Internal Errors on UDM/AUSF Interfaces

Table 61: Internal Errors

Error	Description	Reject Cause/Action
Timeout	The AMF does not get a response from UDM.	Registration Reject with cause #15, No suitable cells in tracking area
Timeout	5The AMF does not get a response from AUSF.	Drop the message

Error Handling for Protocol Data – NAS

Table 62: NAS Error Handling

Protocol Data Error	AMF Handling
N1 message is too short to contain a complete message type information element.	Ignore the message.
N1 message with message type not defined or not implemented.	Return a status message with cause #97, message type non-existent or not implemented.
AMF cannot parse N1 message. It is a request message.	AMF formulates a reject message and sends it to UE.
AMF cannot parse N1 message as mandatory IE is missing. It is a response message.	Stop retransmission timer and treat it as transmission failure. Formulate and send 5GMM status message to UE with cause #96, invalid mandatory information.
Limit on repetition of information elements is exceeded.	AMF handles the contents of the information elements appearing first up to the limit of repetitions and ignores all subsequent repetitions of the information element.
N1 message with optional IEs that have incorrect syntax.	AMF ignores optional IEs and accepts rest of the message.

Protocol Data Error	AMF Handling
Conditional IE errors.	For Conditional IE handling, AMF sends MM status message with cause #100 CONDITIONAL_IE_ERROR

NGAP/NAS/REST EP Error Handling

NGAP Error Handing

Mandatory IE's presence and length checks is done for NGAP message validation.

NAS Error Handling

Mandatory IE's presence and length checks is done for NAS message validation. In Conditional IE's, only uplink messages are handled.

REST Endpoint Error Handling

REST Endpoint: Validation of incoming inbound request message from UDM (DeRegData) and SMF (N1N2MsgTransferReqData, AssignEbiData and SmContextStatusNotification) is done towards AMF only on REST-EP.

AMF looks up for the presence and validates syntax and semantic errors of mandatory/conditional attributes in inbound request messages. In case, any optional attributes are present, then AMF performs syntax and semantic error handling.

CHAPTER 16

High Availability Services

Feature Summary and Revision History

Summary Data

Table 63: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 64: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

High Availability (HA) is the ability of a system to operate continuously for a designated time without significant down time.

HA uses two pods, one as active and other one as standby. Whenever the active pod goes down, the standby pod becomes active and handles the traffic.

This feature supports the following HA services:

- AMF
- NGAP and NAS

AMF High Availability Service

Feature Description

The High Availability feature ensures the following functionalities for AMF-service:

- No session loss when AMF-service pods get killed or restarted.
- During restart, the AMF-service pods don't:
  - Fail any procedures
  - Increase in call processing time
  - Result in call failure of the retried calls
  - Restart or crash other pods
  - Downgrade the performance

NGAP and NAS High Availability Service

Feature Description

The AMF protocol pod maintains the security context cache, NAS UL, and DL counters. Whenever this information is modified in the cache, the same information gets replicated to the peer protocol pod to ensure high availability.

The AMF protocol pods determine among themselves who is the leader by using the Etcd for electing a leader. The leader information gets registered in the topology management module in the Etcd. The leader selection upgradation helps with replicating the security context cache to the other AMF protocol pod. If the leader pod goes down, the other(follower) pod becomes active and handles the traffic. The follower pod works with the replicated security context cache, UL, and DL counters from the leader.

The AMF-SCTP and the AMF-service pods query the leader information for the AMF protocol pod before making any IPC call. When the leader pod goes down, the other pod gets selected as a leader and the subsequent IPC requests goes to the selected protocol pod.

If a pod comes up, the security context cache gets synced with the peer before the pod becomes ready.

This feature supports two AMF protocol replicas.

Note Supported maximum two replicas (recommended) for high availability.

If both protocol pod replicas go down back to back or together, the security context data gets lost.

Feature Configuration

To configure this feature, use the following configuration:

```
config
 instance instance-id instance_id
  endpoint ngap replicas replica_count
  end
```

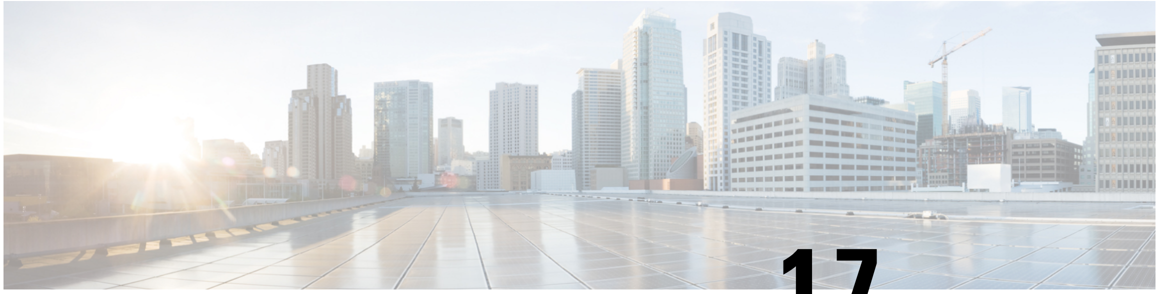
NOTES:

- **endpoint ngap replicas** *replica_count*—Specify the number of NGAP replicas per node.

Configuration Example

The following is an example configuration.

```
config
 instance instance-id 1
  endpoint ngap replicas 2
  end
```



CHAPTER 17

Idle Entry Procedure

Feature Summary and Revision History

Summary Data

Table 65: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 66: Revision History

Revision Details	Release
First introduced.	2021.04.0

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flow for this feature.

gNB-Initiated UE Context Release Procedure Call Flow

This section describes the gNB-Initiated UE Context Release Procedure call flow.

Figure 35: gNB-Initiated UE Context Release Procedure Call Flow

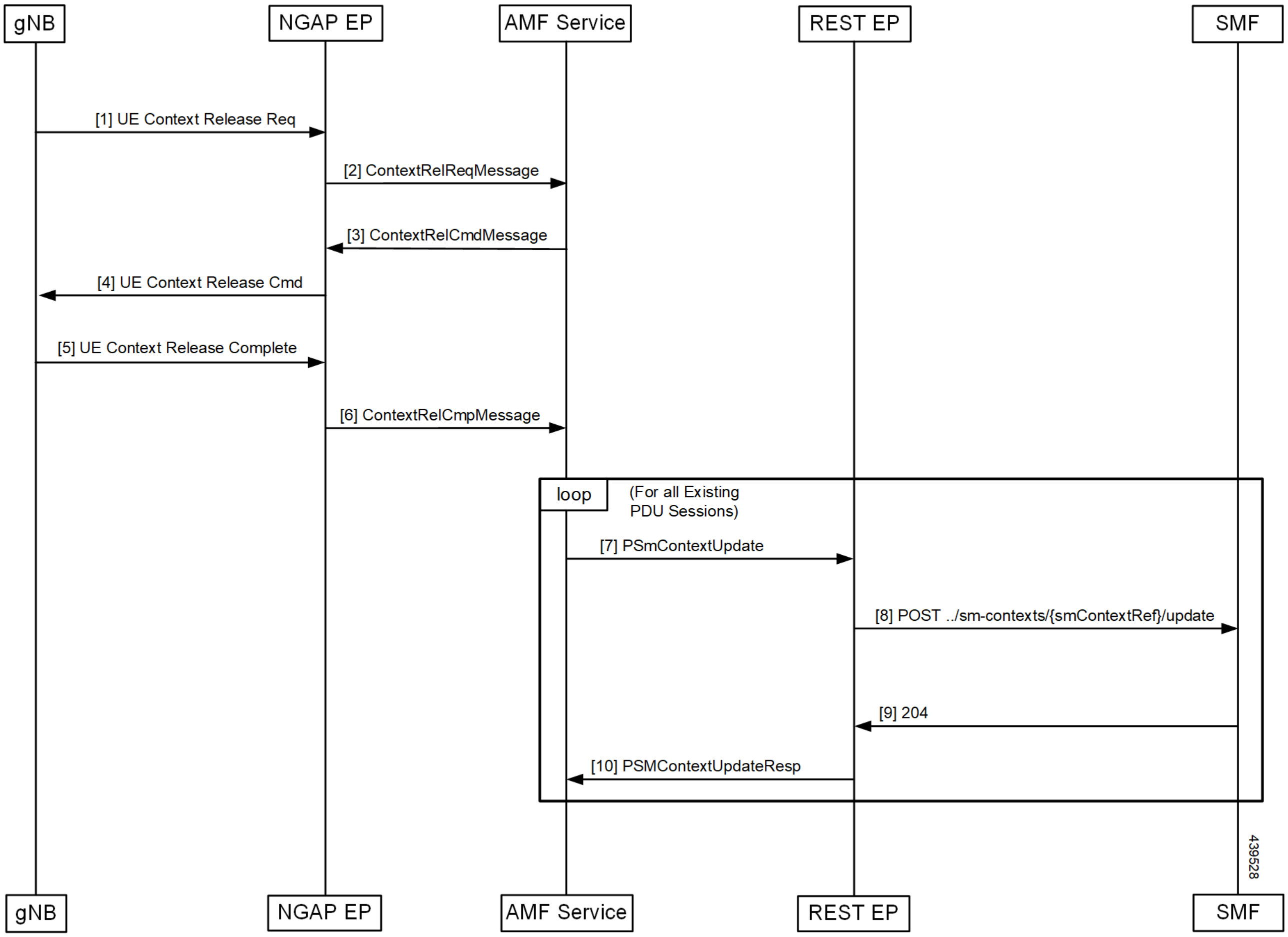

gNB
NGAP EP
AMF Service
REST EP
SMF
[1] UE Context Release Req
[2] ContextRelReqMessage
[3] ContextRelCmdMessage
[4] UE Context Release Cmd
[5] UE Context Release Complete
[6] ContextRelCmpMessage
loop
(For all Existing PDU Sessions)
[7] PSmContextUpdate
[8] POST ../sm-contexts/{smContextRef}/update
[9] 204
[10] PSMContextUpdateResp
439528
gNB
NGAP EP
AMF Service
REST EP
SMF

Table 67: gNB-Initiated UE Context Release Procedure Call Flow Description

Step	Description
1	AMF receives UE Context Release Request from gNB.
2	AMF sends UE Context Release Command to gNB.
3	AMF receives UE Context Release Complete from gNB.
4	SmContextUpdate procedure is initiated for all existing PDU sessions of the subscriber.
5	Once the SmContextUpdate is complete, UE is moved to Idle state.
6	T3512 Timer is started.
7	On expiry of T3512 timer, the UE Detach Timer is started.

Step	Description
8	On expiry of UE Detach Timer, the deregistration procedure is triggered.

UE/NW Initiated Deregistration followed by UE Release Procedure Call Flow

This section describes the UE/NW Initiated Deregistration followed by UE Release Procedure call flow.

Figure 36: UE Context Release Procedure after Deregistration Call Flow

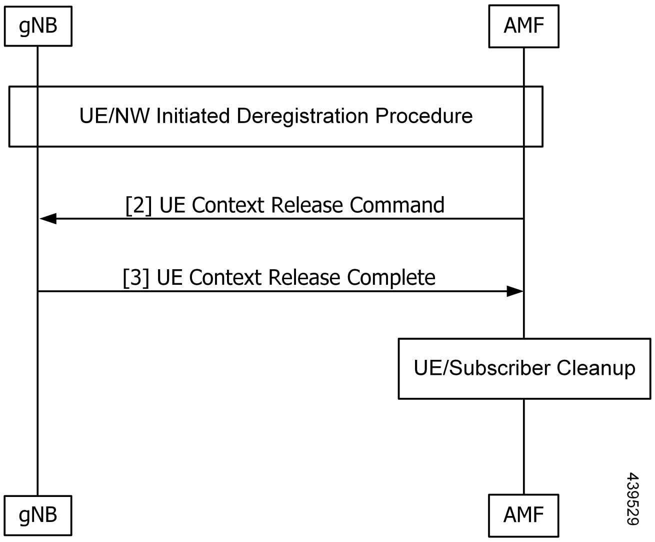

gNB
AMF
UE/NW Initiated Deregistration Procedure
[2] UE Context Release Command
[3] UE Context Release Complete
UE/Subscriber Cleanup
gNB
AMF
439529

Table 68: UE Context Release Procedure after Deregistration Call Flow Description

Step	Description
1	UE/NW Initiated Deregistration procedure is completed. Deregistration Req/Accept is completed and UE is moved to Deregistered state.
2	AMF Sends UE Context Release Command to gNB.
3	AMF receives UE Context Release Complete from gNB.
4	As UE deregistration is already done and UE is moved to Deregistered state, UE Context/Subscriber cleanup is triggered, and subscriber and session is deleted from CDL.

CHAPTER 18

Internode Registration Support

Feature Summary and Revision History

Summary Data

Table 69: Summary Data

Applicable Product(s) or Functional Area	5G-AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 70: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

This feature supports the following:

- Internode Initial Registration

- Internode Mobility Registration

Internode Initial Registration

Feature Description

AMF now supports registering a UE when it gets a registration request with type set to initial registration with identifier GUTI allocated by a peer node.

The case of this AMF being the “old” node during initial registration or attach procedure is described in Registration with AMF Change, on page 144 section.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Identification with Peer Node Call Flow

This section describes Identification with Peer Node call flow.

Figure 37: Identification with Peer Node Call Flow

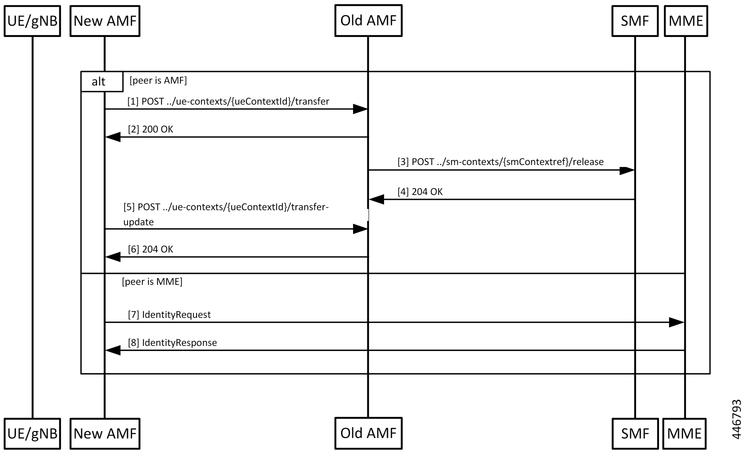


Table 71: Identification with Peer Node Call Flow Description

Step	Description
1	If the peer node is an AMF, then new AMF sends a transfer request to the old AMF, with type set to “INITIAL REGISTRATION”, including the whole registration request received by it.
2	The old AMF checks the integrity protection of the request, and if integrity checks pass, responds with the UE context, but without any SMF information.

Step	Description
3	The old AMF checks the integrity of the message that is received from the new AMF. If the integrity check passes, the old AMF packages the attributes of the UE that is available in the response to the transfer request. If the request was for mobility updating, PDU session information present in the old AMF is sent to the new AMF.
4	AMF releases any resources that the UE held at any SMF.
5	SMF responds to the AMF request.
6	The new AMF sends a transfer update message to the old AMF.
7	The old AMF responds with a “204 OK” indicating that the transfer is successful.
8	If the old node is an MME, then AMF sends an identity request message to MME along with the registration request received.
9	MME checks the integrity of the message it receives. If integrity checks pass, the MME returns the MM context.

At the end of a successful transfer from a peer node, AMF issues a security mode command with a mapped security context (from LTE) or a non-current security context (5G) towards the UE.

Limitations

Additional GUTI in the registration request is not supported.

Internode Mobility Registration

Feature Description

This feature supports the following:

- Idle Mode Registration from Peer MME to AMF
- AMF to MME Idle Mode Handoff
- Registration with AMF Change

Idle Mode Registration from Peer MME to AMF

Feature Description

AMF now supports using the N26 interface to retrieve a context from an MME for handling registration request with type set to Mobility Updating and a foreign GUTI. AMF then uses a mapped security context from the MME to use with the UE.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Idle Mode Registration to AMF from MME Call Flow

This section describes the Idle Mode Registration to AMF from MME call flow.

Figure 38: Idle Mode Registration to AMF from MME Call Flow

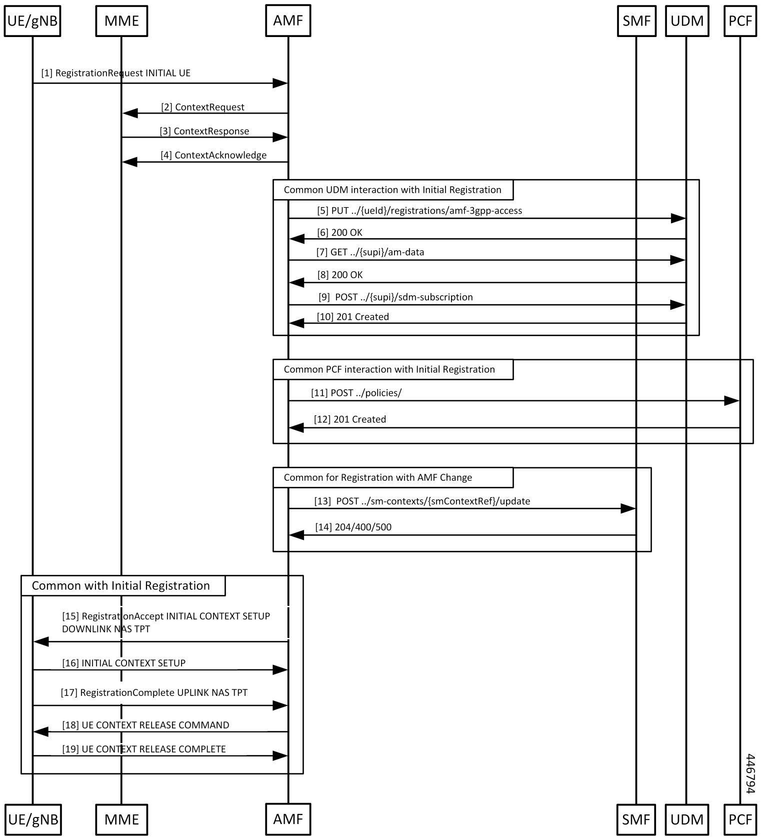

UE/gNB
MME
AMF
SMF
UDM
PCF
[1] RegistrationRequest INITIAL UE
[2] ContextRequest
[3] ContextResponse
[4] ContextAcknowledge
Common UDM interaction with Initial Registration
[5] PUT ../{ueId}/registrations/amf-3gpp-access
[6] 200 OK
[7] GET ../{supi}/am-data
[8] 200 OK
[9] POST ../{supi}/sdm-subscription
[10] 201 Created
Common PCF interaction with Initial Registration
[11] POST ../policies/
[12] 201 Created
Common for Registration with AMF Change
[13] POST ../sm-contexts/{smContextRef}/update
[14] 204/400/500
Common with Initial Registration
[15] RegistrationAccept INITIAL CONTEXT SETUP DOWNLINK NAS TPT
[16] INITIAL CONTEXT SETUP
[17] RegistrationComplete UPLINK NAS TPT
[18] UE CONTEXT RELEASE COMMAND
[19] UE CONTEXT RELEASE COMPLETE
446794
UE/gNB
MME
AMF
SMF
UDM
PCF

Table 72: Identification with Peer Node Call Flow Description

Step	Description
1	The UE sends a Registration Request with a GUTI assigned by an MME.
2	The AMF analyzes the GUTI, identifies an MME and sends a context request.
3	The MME responds with a ContextResponse.
4	The AMF sends a ContextAcknowledge to the MME.

Step 5 to Step 18 are same as mentioned in the call flow for Registration with AMF Change, on page 144.

AMF to MME Idle Mode Handoff

Feature Description

AMF supports idle mode handoff to MME for 5GS to EPS Idle mode mobility using N26 interface.

- Context Request: MME sends the Context Request message to the AMF to get the MM and EPS bearer Contexts for the UE.
- Retrieve SM Context service operation: Retrieves an individual SM context, for a given PDU session associated with 3GPP access from the SMF.

Currently, the following are not supported:

- Handling of timeouts from SMF during Retrieve Request
- Handling of negative response from SMF during Retrieve Request

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

AMF to MME Idle Mode Handoff Call Flow

This section describes the AMF to MME Idle Mode Handoff call flow.

The following call flow shows the messaging that happens in the network.

Figure 39: AMF to MME Idle Mode Handoff Call Flow

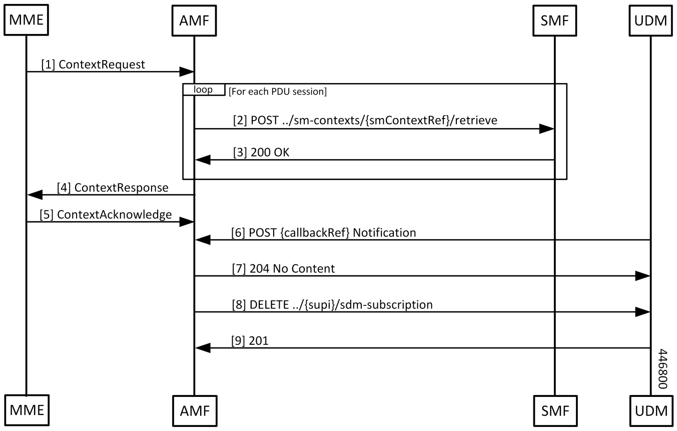


Table 73: AMF to MME Idle Mode Handoff Call Flow Description

Step	Description
1	A UE that was previously registered on an AMF in 5GC moves to EPC, and sends a TAU request to an MME. From the GUTI sent by the UE, the MME finds the identity of the AMF, and sends a ContextRequest over N26.
2	The ContextRequest reaches the AMF. MME sends the full TAU Request message as a part of the ContextRequest. The AMF does integrity checks on the request to ascertain the validity of the request. If the request from the MME indicates that the MME has authorized the UE, AMF doesn't do security checks on the received message. If integrity checks fail, AMF rejects the request. Or else, the AMF retrieves the PDU sessions information from each of the SMFs that host PDUs for this UE and has allocated EBI for their sessions from the AMF.
3	The SMF responds to the SmContext Retrieve Request from the AMF.
4	AMF responds to MME by sending a ContextResponse message when AMF receives all the expected responses from SMFs.
5	The MME sends a ContextAcknowledgement message to the AMF. The AMF starts a guard timer to clear allocated resources in case the notification from the UDM to clear the registration doesn't come through.
6	Since the MME is now the owner of the registration, the UDM notifies the AMF that the registration for 3GPP access is cancelled.
7	The AMF releases any local resources, and responds to the UDM.
8	The AMF clears the subscription to changes in subscription data at the UDM.
9	The UDM responds to the request from the AMF.

Registration with AMF Change

Feature Description

AMF now supports registration with Mobility Updating and AMF Change. Currently, AMF only supports GUTI based relocations.

REST Endpoint

To support changes at the old AMF, endpoints are needed for the following:

- Transfer requests from the new AMF
- Transfer-Update requests from the new AMF
- Notifications from the UDM

Client code for Transfer Requests and Transfer Update Requests are required in the new AMF.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Registration with AMF Change Call Flow

This section describes the Registration with AMF Change call flow.

Figure 40: Registration with AMF Change Call Flow

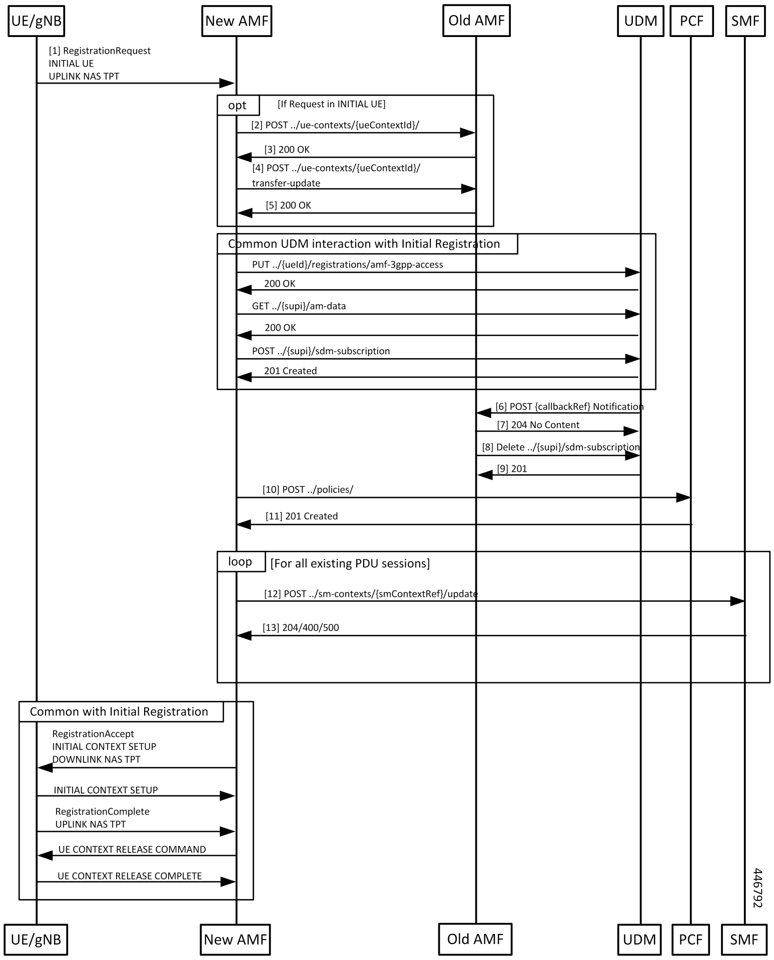

UE/gNB
New AMF
Old AMF
UDM
PCF
SMF
[1] RegistrationRequest
INITIAL UE
UPLINK NAS TPT
opt
[If Request in INITIAL UE]
[2] POST ../ue-contexts/{ueContextId}/
[3] 200 OK
[4] POST ../ue-contexts/{ueContextId}/
transfer-update
[5] 200 OK
Common UDM interaction with Initial Registration
PUT ../{ueId}/registrations/amf-3gpp-access
200 OK
GET ../{supi}/am-data
200 OK
POST ../{supi}/sdm-subscription
201 Created
[6] POST {callbackRef} Notification
[7] 204 No Content
[8] Delete ../{supi}/sdm-subscription
[9] 201
[10] POST ../policies/
[11] 201 Created
loop
[For all existing PDU sessions]
[12] POST ../sm-contexts/{smContextRef}/update
[13] 204/400/500
Common with Initial Registration
RegistrationAccept
INITIAL CONTEXT SETUP
DOWNLINK NAS TPT
INITIAL CONTEXT SETUP
RegistrationComplete
UPLINK NAS TPT
UE CONTEXT RELEASE COMMAND
UE CONTEXT RELEASE COMPLETE
446792
UE/gNB
New AMF
Old AMF
UDM
PCF
SMF

Table 74: Registration with AMF Change Call Flow Description

Step	Description
1	UE builds a registration message with type set to **Mobility Updating** or **Initial Registration** and sends it to the gNB. At gNB, the message becomes the payload of an INITIAL UE message (if the UE is in ECM_IDLE) or an UPLINK NAS TRANSPORT message when the UE is in ECM_CONNECTED (Only for Mobility Updating). When the UE is in ECM_CONNECTED, there's a N2 handover procedure that precedes this part, and the context transfer steps of the call flow are omitted.
2	The new AMF analyses the GUTI that is send by the UE and determines whether it's allocated by a different AMF. The new AMF determines the old AMF using parameters from the GUTI and constructs a transfer request. The whole message body that is received by the new AMF is part of the request to the old AMF. The new AMF sets the type of transfer request based on whether the UE is registering for initial registration or mobility updating.
3	The old AMF checks the integrity of the message that is received from the new AMF. If the integrity check passes, the old AMF packages the attributes of the UE that is available in the response to the transfer request. If the request was for mobility updating, PDU session information present in the old AMF is sent to the new AMF.
4	The new AMF sends a transfer update message to the old AMF.
5	If the new AMF decides not to use the current PCF, the old AMF clears the PCF associations created by it. In the case of initial updating, the AMF clears all the PDU sessions. The new AMF interacts with UDM to register as the node responsible for the UE. The AMF also interacts with the UDM to register for changes to subscription data for the UE, and these steps are the same as the one executed by the AMF during initial registration.
6	Once the new AMF registers with the UDM, the UDM notifies the old AMF that its registration has been cancelled.
7	The old AMF acknowledges the notification from the UDM.
8	Since the old AMF is no longer interested in changes to the subscription information, it sends a cancel for subscription for changes to SDM subscription.
9	The UDM clears the subscription and responds to the old AMF. The old AMF clears any state it has on the UE. The new AMF sets up policies in the PCF, and these steps are the same as those done during initial registration.
10	If AMF policies are to be set up with the PCF, the AMF sends a request to create the policies in the PCF.
11	PCF responds to the AMF request.
12	For each PDU session that the new AMF has taken over, it sends a message to the SMF to change the AMF for the session.
13	SMF responds to the AMF.
14	AMF sends a Registration Accept to the UE with new GUTI and a Tracking Area List. These steps are same as done during the AMF initial registration.

Step	Description
15	If the registration type is Mobility Updating, AMF ignores FollowOn IE and does not initiate UE CONTEXT RELEASE COMMAND.

Limitations

The following scenarios are currently not supported:

- Activation of bearers during Registration
- Steering of Roaming information
- UE Policy Information
- Integrity check failure
- Optional authentication of the UE
- Change of PCF during mobility
- Rejection/Clearing of PDU sessions

OAM Support

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

Bulk Statistics Support

- Message level statistics for new SBA messages, on a per peer AMF basis.
- Procedure level statistics for new and old AMF procedures, with Attempted, Success and Failure.

CHAPTER 19

IPv6 Support on SBI Interface

Feature Summary and Revision History

Summary Data

Table 75: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 76: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF supports IPv6 on the Service based interface (SBI).

The SBI endpoint can be configured with instance type as IPv6 or IPv4. The default type is IPv4.

Note SBI endpoint does not support the Dual instance type.

Feature Configuration

To configure this feature, use the following configuration:

```
config
 instance instance-id instance_id
  endpoint sbi
   replicas replicas_count
   loopbackPort port_number
   instancetype { IPv4 { vip-ip ipv4_address vip-port ipv4_port } |
                      IPv6 { vip-ipv6 ipv6_address vip-ipv6-port ipv6_port } }
   end
```

NOTES:

- **replicas** *replicas_count*—Specify the number of replicas.
- **loopbackPort** *port_number*—Specify the loopback port number.
- **vip-ip** *ipv4_address* **vip-port** *ipv4_port*—Specify the IPv4 address and port details.
- **vip-ipv6** *ipv6_address* **vip-ipv6-port** *ipv6_port*—Specify the IPv6 address and port details.
- **instancetype { IPv6 | IPv4 }**—Specify the SBI endpoint interface type and details of IPv4 or IPv6.

Configuration Example

The following is an example configuration for IPv4.

```
config
 instance instance-id 1
  endpoint sbi
   replicas 2
   loopbackPort 1000
   instancetype IPv4 vip-ip 1.1.1.0 vip-port 1001
   end
```

The following is an example configuration for IPv6.

```
config
 instance instance-id 1
  endpoint sbi
   replicas 2
   loopbackPort 1000
   instancetype IPv6 vip-ipv6 1:1:1:1::4 vip-ipv6-port 1001
   end
```

CHAPTER 20

Mobile Equipment Identity Check Procedures

Feature Summary and Revision History

Summary Data

Table 77: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 78: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

The AMF initiates the Mobile Equipment (ME) Identity Check procedures in case of authentication failure and unknown GUTI registration.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

UE Identity Procedure for Authentication Failure Call Flow

The section describes the UE Identity Procedure for Authentication Failure call flow.

Figure 41: UE Identity Procedure for Authentication Failure Call Flow

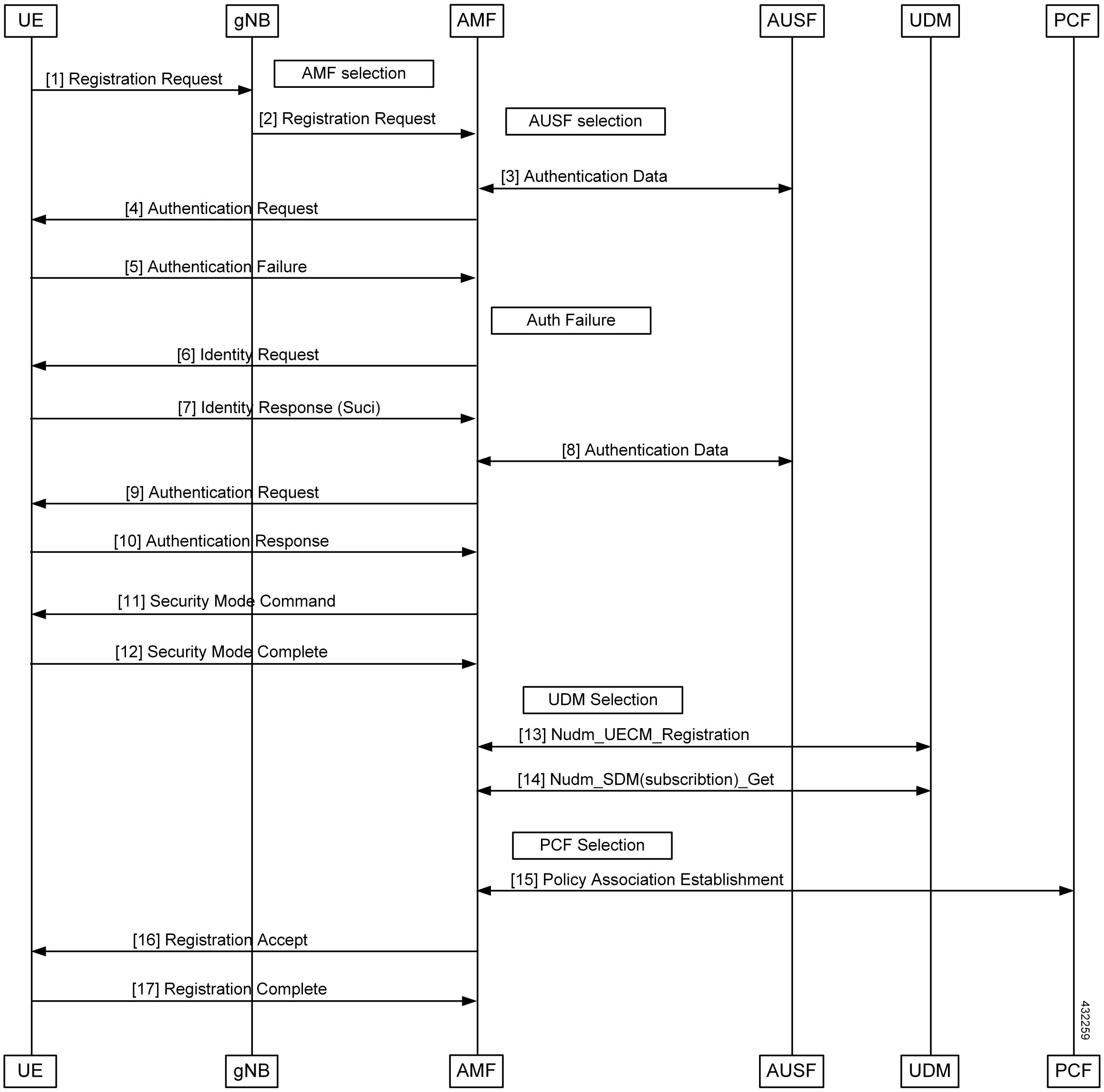

UE
gNB
AMF
AUSF
UDM
PCF
[1] Registration Request
AMF selection
[2] Registration Request
AUSF selection
[3] Authentication Data
[4] Authentication Request
[5] Authentication Failure
Auth Failure
[6] Identity Request
[7] Identity Response (Suci)
[8] Authentication Data
[9] Authentication Request
[10] Authentication Response
[11] Security Mode Command
[12] Security Mode Complete
UDM Selection
[13] Nudm_UECM_Registration
[14] Nudm_SDM(subscribtion)_Get
PCF Selection
[15] Policy Association Establishment
[16] Registration Accept
[17] Registration Complete
432259
UE
gNB
AMF
AUSF
UDM
PCF

Table 79: UE Identity Procedure for Authentication Failure Call Flow Description

Step	Description
1	The UE that wants to register itself with the 5G core sends the Registration Request N1 message towards AMF.
2	The gNB selects an AMF and forwards the Registration Request message to AMF.
3	The AMF selects an AUSF based on the PLMN information through NRF query or through static configuration. The AMF fetches authentication data from AUSF for the UE.
4	The AMF sends the Authentication Request message to the UE to initiate authentication of the UE identity.
5	Upon failure of authentication, the AMF will trigger Identity Request towards the UE and request for an UE identity. Authentication will be proceeded with the new UE identity.
6	The UE sends the Identity Request message to the AMF.
7	The UE responds with its SUCI in the Identity Response message to the AMF.
8	The AMF extracts fresh authentication data from AUSF using the SUCI of the subscriber.
9	The AMF sends Authentication Request to the UE to initiate authentication of the UE identity.
10	The UE sends Authentication Response to the AMF to deliver a calculated authentication response to the network. The AMF verifies the result received and if the result is as expected, then the registration procedure is proceeded.
11	The NAS security initiation is performed.
12	Upon completion of NAS security function setup, the AMF initiates NGAP procedure to provide the 5G-AN with security context. The 5G-AN stores the security context and acknowledges to the AMF. The 5G-AN uses the security context to protect the messages exchanged with the UE.
13	The AMF selects an UDM based on the PLMN information through NRF query or through static configuration and registers the UE with the UDM using Preregistration. The UDM stores the AMF identity associated to the Access Type.
14	The AMF retrieves the Access and Mobility Subscription data using Misjudgement. The AMF subscribes to be notified using Nudm_SDM_Subscribe when the data requested is modified.
15	The AMF selects the PCF based on PLMN-info and slice-info, and performs a Policy Association Establishment. The PCF sends policy data to the AMF with restrictions and other policies to be applied for the UE. Currently the policies are not applied for the UE and are just stored in the AMF.
16	The AMF sends a Registration Accept message to the UE indicating that the Registration Request has been accepted. Registration Accept contains these parameters - 5G-GUTI, Registration Area, Mobility restrictions, PDU Session status, Allowed NSSAI, Configured NSSAI for the Serving PLMN, Periodic Registration Update timer, Emergency Service Support indicator, Accepted DRX.
17	The UE sends a Registration Complete message to the AMF to acknowledge that a new 5G-GUTI was assigned.

UE Identity Procedure for Unknown GUTI Registration Call Flow

This section describes the UE Identity procedure for unknown GUTI registration call flow.

Figure 42: UE Identity Procedure for Unknown GUTI Registration Call Flow

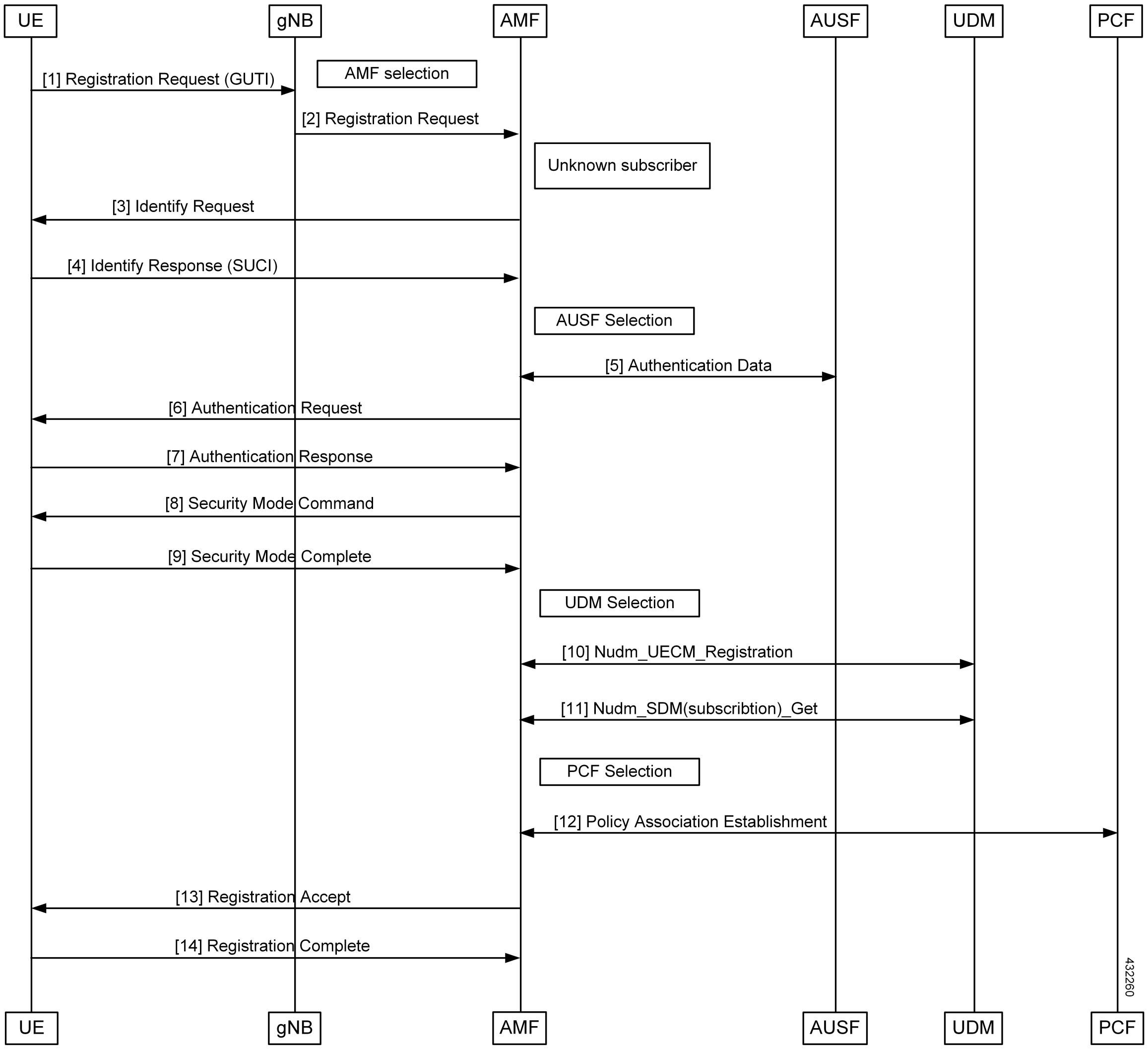

UE
gNB
AMF
AUSF
UDM
PCF
[1] Registration Request (GUTI)
AMF selection
[2] Registration Request
Unknown subscriber
[3] Identify Request
[4] Identify Response (SUCI)
AUSF Selection
[5] Authentication Data
[6] Authentication Request
[7] Authentication Response
[8] Security Mode Command
[9] Security Mode Complete
UDM Selection
[10] Nudm_UECM_Registration
[11] Nudm_SDM(subscribtion)_Get
PCF Selection
[12] Policy Association Establishment
[13] Registration Accept
[14] Registration Complete
432260

Table 80: UE Identity Procedure for Unknown GUTI Registration Call Flow Description

Step	Description
1	When Registration Request is received with unknown GUTI, AMF triggers the Identity Request towards the UE and request for an UE identity. The registration is proceeded with the new UE identity.
2	During the registration procedure, the AMF determines that the received GUTI is of the subscriber and not present in the AMF. In such cases, AMF triggers the Identity Request to UE asking for its SUCI.
3	The UE sends the Identity Request message to the AMF.

Step	Description
4	The UE responds with its SUCI in the Identity Response message to the AMF.
5	The AMF extracts fresh authentication data from the AUSF using the SUCI of the subscriber.
6	The AMF sends Authentication Request to the UE to initiate authentication of the UE identity.
7	The UE sends Authentication Response to the AMF to deliver a calculated authentication response to the network. The AMF verifies the result received and if the result is as expected, then the registration procedure is proceeded.
8	The NAS security initiation is performed.
9	Upon completion of the NAS security function setup, the AMF initiates NGAP procedure to provide 5G-AN with security context. The 5G-AN stores the security context and acknowledges the AMF. The 5G-AN uses the security context to protect the messages exchanged with the UE.
10	The AMF selects an UDM based on the PLMN information though NRF query or through static configuration, and registers the UE with the UDM using Nudm_UECM_Registration. The UDM stores the AMF identity associated to the Access Type.
11	The AMF retrieves the Access and Mobility Subscription data using Nudm_SDM_Get. The AMF subscribes to be notified using Nudm_SDM_Subscribe when the data requested is modified.
12	The AMF selects the PCF based on PLMN-info and slice-info, and performs a Policy Association Establishment. The PCF sends policy data to the AMF with restrictions and other policies to be applied for the UE. Currently the policies are not applied for the UE and are just stored in the AMF.
13	The AMF sends a Registration Accept message to the UE indicating that the Registration Request has been accepted. Registration Accept contains these parameters - 5G-GUTI, Registration Area, Mobility restrictions, PDU Session status, Allowed NSSAI, Configured NSSAI for the Serving PLMN, Periodic Registration Update timer, Emergency Service Support indicator, Accepted DRX.
14	The UE sends a Registration Complete message to the AMF to acknowledge that a new 5G-GUTI was assigned.

CHAPTER 21

Multiple AMF Instances Support

Feature Summary and Revision History

Summary Data

Table 81: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 82: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

Multiple AMF instances enable the administrators to scale up or scale down the instances to meet the evolving capacity requirements. The AMF architecture supports seamless inclusion and exclusion of the AMF instances in the AMF framework.

Considerations

This feature has the following considerations in this release:

- If the AMF deployment scenario has multiple servers, the servers must be labeled. The labeling is helpful when one of the server nodes is faulty or out of service.

  You can label the servers as:

  - Server1: Labeled for protocol and service layer pods
  - Server2: Labeled for service and datastore layer pods
  - Server3: Labeled for datastore and protocol layer pods

- When multiple instances of AMF are deployed on the servers, and these servers do not have sufficient hardware resources (CPU cores, memory), then you can reset the default pod limit prescribed by Kubernetes.

  You can scale the number of pods by using the following configuration in the SMI Deployer CLI:

  ```
  clusters cluster name node-defaults k8s max-pods number_of_pods
  ```

Feature Configuration

Configuring this feature involves the following steps:

1. Configure the instance ID for the AMF instance. For more information, refer to Configuring the AMF Instance ID, on page 158.
2. Associate the AMF instances to a common CDL. For more information, refer to Associating the AMF Instances to CDL, on page 159.
3. Configure the notifications that CDL sends to the AMF instances. The notifications are invoked when events such as timer expiry occurs. For more information, refer to Configuring the CDL Notifications, on page 159.

Configuring the AMF Instance ID

To configure the AMF instance ID, use the following configuration:

```
config
   deployment
      logical-nf-instance-id instance_id
      end
```

NOTES:

- **deployment**—Configure the deployment parameters.
- **logical-nf-instance-id** *instance_id*—Specify the unique instance ID for the AMF instance.
- Ensure to configure the instance ID for each AMF instance.

Associating the AMF Instances to CDL

To associate the AMF instances, use the following configuration:

```
config
   datastore
      session-db
         endpoints
            datastore-ep-session.cdl_namespace.svc.cluster.local
               port port_number
               end
```

NOTES:

- **datastore**—Configure the datastore parameters.
- **session-db**—Configure the session database parameters.
- **endpoints**—Configure the endpoint parameters.
- **datastore-ep-session.***cdl_namespace***.svc.cluster.local** —Specify the CDL namespace.
- **port** *port_number*—Specify the port number of the CDL pod.

Configuring the CDL Notifications

To configure the CDL notifications, use the following configuration:

```
config
   datastore
      notification-ep { host host_address | port port_number }
      end
```

NOTES:

- **datastore**—Configure the datastore parameters.
- **notification-ep { host** *host_address* **| port** *port_number* **}**—Specify the VIP IP address and port number of the AMF instance to which the CDL must send the notification. Ensure that the VIP IP and port number are unique for each AMF instance.

Troubleshooting Information

This section describes troubleshooting information for this feature.

Problem

In the multiple AMF deployment scenario, the secondary pods cannot be brought up when the master node has utilized the default pod limit. The secondary pods failed to be up due to one of the following reasons:

- Pods are in the pending state.
- The node didn’t match the pod and node affinity or the antiaffinity rules.

Resolution

In circumstances when all the pods are utilized, you can increase the number of pods in the Kubernetes cluster.

To configure the Kubernetes maximum pod count, use the following steps:

On an existing AMF deployment

1. In the SMI Deployer CLI, use the following configuration:

   ```
   clusters node-defaults k8s max-pods maximum_pods
   ```

   NOTES:

   a. **max-pods** *maximum_pods*—Specify the maximum number of pods per node. Default is 256. Must be an integer in the range of 10-2000.

2. Assign labels to the nodes within the cluster and sync the changes using the following command:

   ```
   clusters nodes actions sync run
   ```

3. Delete the Istio directory from the master node using the following command:

   ```
   rm -rf /var/lib/smi/istio/
   ```

4. Synchronize the clusters to reflect the configuration using the following commands:

   ```
   clusters cluster_name actions sync run reset-k8s-nodes true debug true
   clusters cluster_name actions sync run sync-phase opscenter debug true
   ```

Important The synchronize procedure erases the AMF's day-1 or N configuration.

On a new AMF deployment

1. In the SMI Deployer CLI, use the following configuration:

   ```
   clusters node-defaults k8s max-pods maximum_pods
   ```

   NOTES:

   a. **max-pods** *maximum_pods*—Specify the maximum number of pods per node. Default is 256. Must be an integer in the range of 10-2000.

2. Synchronize the clusters using the following commands:

   ```
   clusters cluster_name actions sync run force-vm-redeploy true debug true
   ```

For information on the SMI configuration, see *Ultra Cloud Core Subscriber Microservices Infrastructure - Operations Guide*.

CHAPTER 22

Network-Initiated Deregistration Request

Feature Summary and Revision History

Summary Data

Table 83: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 84: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF marks the UE state as DE-REGISTERED when it receives Deregistration Request from any of the following:

- UE
- AMF CLI admin (Clear Subscribe Request)
- IDT Timer expiry (implicit detach procedure)

AMF prepares the Deregister Accept (N1-Downlink message) towards the UE and waits for the Deregister Complete message from the UE. During this process AMF performs the following functions:

- Checks the configured purge time value.
- Unsubscribes the PCF for am-policy data.
- Completes the UE Context Release Request towards N1.

AMF starts CDL purge timer and holds purging of subscribers data until the timer expires. When the purge timer expires AMF performs the following actions:

- Pushes the CDL timer expiry notification on REST-EP.
- Stops the purge timer.
- Starts purging procedures such as Unsubscribe Or Deregister towards UDM.

Note

- This feature doesn't support the Emergency registration, and the non-3GPP trusted or untrusted scenarios.
- If UE with existing SUPI performs re-registration while purge timer is running, the purge timer gets reset when the UE triggers re-deregistration.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flow for this feature.

Purge of Subscriber Data Call Flow

This section describes the Purge of Subscriber Data in AMF call flow.

Figure 43: Purge of Subscriber Data in AMF Call Flow

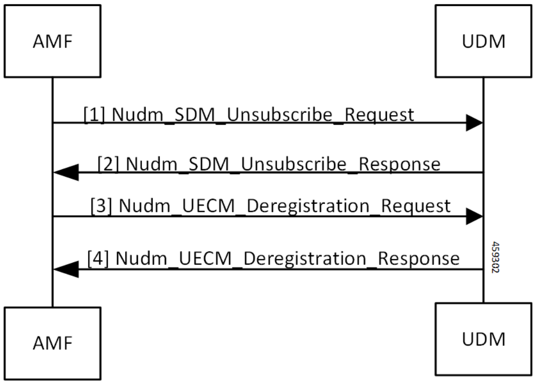

AMF
UDM
[1] Nudm_SDM_Unsubscribe_Request
[2] Nudm_SDM_Unsubscribe_Response
[3] Nudm_UECM_Deregistration_Request
[4] Nudm_UECM_Deregistration_Response
459302
AMF
UDM

Table 85: Purge of Subscriber Data in AMF Call Flow Description

Step	Description
1, 2	When AMF receives the Deregistration Request from the UE, it sends SDM Unsubscribe and UE CM Deregistration triggers on purge timer expiry. AMF receives the response from the UDM.
3, 4	AMF sends the UE CM Deregistration Request to the UDM and receives response from it.

Feature Configuration

To configure this feature, use the following configuration:

```
config
 amf-global
  call-control-policy call_control_policy_name
   timers tpurge value purge_value
   end
```

NOTES:

- **call-control-policy** *call_control_policy_name*—Specify the call control policy name.
- **timers tpurge value** *purge_value*—Specify the purge timer value in seconds.

  Default purge timer value is 86400 seconds.

  To disable the purge timer value, provide its value as zero.

Configuration Example

The following is an example configuration.

```
config
 amf-global
  call-control-policy local
   timers tpurge value 100
   end
```

CHAPTER 23

Node Manager Endpoint

Feature Summary and Revision History

Summary Data

Table 86: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 87: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

An NGAP ID and a Serving-Temporary Mobile Subscriber Identity (S-TMSI) are assigned to a UE within AMF. Using these unique values, the UE is distinguished over the NG interface. The Node Manager (NodeMgr) pod manages these unique IDs by generating and allocating them to the UE through the request and response messages.

Feature Configuration

To configure this feature, use the following configuration:

```
config
    instance instance-id instance-id
      endpoint { bgpspeaker | geo | gtp | li | ngap | nodemgr | protocol
 | sbi | sctp | service }
        instancetype { Dual | IPv4 | IPv6 }
        interface { bfd | bgp | geo-external | geo-internal | nrf }
        internal base-port start port_number
        loopbackEth host_address_port_number
        loopbackPort port_number
        nodes number_of_nodes
        range { vip-ipv6 ipv6_address | offline offline| vip-ipv6-port
ipv6_address }
        replicas number_of_nodes
        system-health-level { crash | critical | warn }
        uri-scheme { http | https }
        vip-ip ipv4_address
        vip-ipv6 ipv6_address
        end
```

NOTES:

- **instance instance-id** *instance-id*—Specify the endpoint instance ID.
- **endpoint { bgpspeaker | geo | gtp | li | ngap | nodemgr | protocol | sbi | sctp | service }**—Specify the endpoint that must be configured. For configuring NodeMgr, use **nodemgr**.
- **instancetype { Dual | IPv4 | IPv6 }**—Specify the endpoint's local interface type.
- **interface { bfd | bgp | geo-external | geo-internal | nrf }**—Specify the endpoint interfaces.
- **internal base-port start** *port_number*—Specify the internal base-port to start the endpoint.
- **loopbackEth** *host_address_port_number*—Specify the local interface name or host IP address of the endpoint.
- **loopbackPort** *port_number*—Specify the endpoint local port.
- **nodes** *number_of_nodes*—Specify the number of nodes replicas that must be configured for resiliency.
- **range { vip-ipv6** *ipv6_address* **| offline** *offline* **| vip-ipv6-port** *ipv6_address* **}**—Specify the range of the NodeMgr endpoint.
- **replicas** *number_of_nodes*—Specify the number of replica nodes that must be created for the endpoint.
- **system-health-level { crash | critical | warn }** —Specify the message to indicate the health of the system.
- **uri-scheme { http | https }** —Specify the URI scheme as HTTP or HTTPs.
- **vip-ip** *ipv4_address*—Specify the IPv4 address for the endpoint.
- **vip-ipv6** *ipv6_address*—Specify the IPv6 address for the endpoint.

CHAPTER 24

N1N2 Message Transfer

Feature Summary and Revision History

Summary Data

Table 88: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 89: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

The NF service consumer uses the N1N2MessageTransfer service operation to transfer N1 or N2 information, or both to the UE or 5G-AN, or both.

AMF now supports the following procedures:

- Network triggered Service Request
- PDU Session Establishment
- PDU Session Modification
- PDU Session Release
- Session continuity, service continuity, and UP path management
- Inter NG-RAN node N2 based handover
- SMS over NAS
- UE assisted and UE-based positioning
- Network assisted positioning
- UE Configuration Update for transparent UE policy delivery

Note AMF only supports SM messages.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

N1N2 Message Transfer Request Call Flow

This section describes the N1N2 Message Transfer Request call flow.

Figure 44: N1N2 Message Transfer Request Call Flow

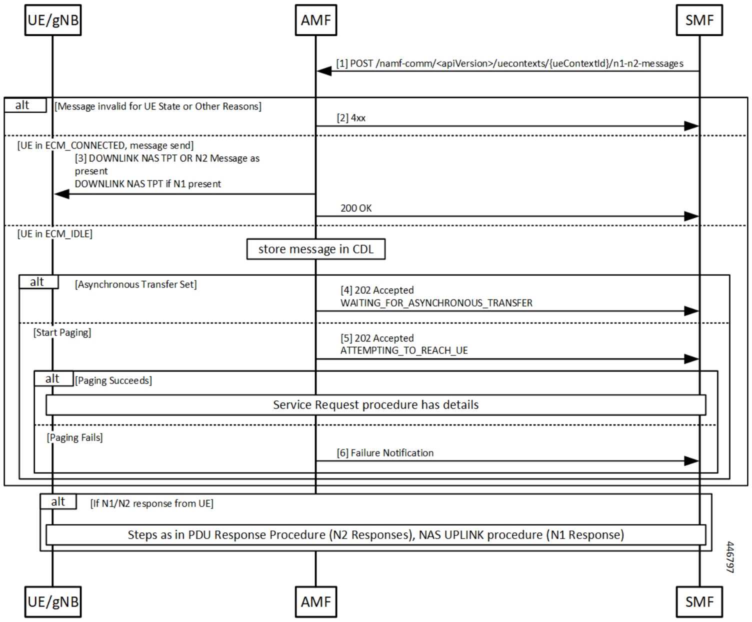

UE/gNB
AMF
SMF
[1] POST /namf-comm/<apiVersion>/uecontexts/{ueContextId}/n1-n2-messages
alt
[Message invalid for UE State or Other Reasons]
[2] 4xx
[UE in ECM_CONNECTED, message send]
[3] DOWNLINK NAS TPT OR N2 Message as present
DOWNLINK NAS TPT if N1 present
200 OK
[UE in ECM_IDLE]
store message in CDL
alt
[Asynchronous Transfer Set]
[4] 202 Accepted
WAITING_FOR_ASYNCHRONOUS_TRANSFER
[Start Paging]
[5] 202 Accepted
ATTEMPTING_TO_REACH_UE
alt
[Paging Succeeds]
Service Request procedure has details
[Paging Fails]
[6] Failure Notification
alt
[If N1/N2 response from UE]
Steps as in PDU Response Procedure (N2 Responses), NAS UPLINK procedure (N1 Response)
446797
UE/gNB
AMF
SMF

Table 90: N1N2 Message Transfer Call Flow Description

Step	Description
1	The peer node sends an N1N2MessageTransfer Request Call Flow message to the AMF.
2	AMF checks if the message is acceptable. If there's an exception, the AMF rejects the message with an appropriate cause code.
3	If the UE is in ECM_CONNECTED state, AMF forwards the message to the UE or gNB. The N2 message received from the peer node determines the N2 message type. If there's a N1 message, it's sent as a payload to the N2 message. AMF then responds with a 200 OK to the peer node.
4	If the UE is in ECM_IDLE state and the Asynchronous Transfer flag is set, AMF stores the message in a known location in CDL. AMF adds the location header to the response and a 202 response is sent with WAITING_FOR_ASYNCHRONOUS_TRANSFER as a diagnostic. The saved message is sent to the UE as the UE transitions to ECM_CONNECTED. The AMF doesn't page the UE in this case.
5	If the UE is in ECM_IDLE state and the SkipInd flag is set in the received N1N2TransferReq message, AMF skips sending the N1 message to UE. AMF sends a 200 OK response with N1_MSG_NOT_TRANSFERRED as a diagnostic. The message isn't sent to the UE as the UE transitions to ECM_CONNECTED and paging isn't done in this scenario.
6	If the UE is in ECM_IDLE and the Asynchronous Transfer flag isn't set, AMF stores the message in a known location. AMF adds the location header to the response and a 202 response is sent with ATTEMPTING_TO_REACH_UE as a diagnostic. The saved message is sent to the UE as the UE transitions to ECM_CONNECTED. If paging fails, AMF sends a Failure Notification to the peer node.

CHAPTER 25

N2 Handover Procedure

Feature Summary and Revision History

Summary Data

Table 91: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 92: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

This feature supports the following:

- N2 handover without AMF change

- N2 handover with AMF change

N2 Handover without AMF Change

Feature Description

For N2 handover without AMF change, the UE uses the source gNB to trigger the handover. The message from the source gNB has the ID of the target gNB.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

N2 Handover without AMF Change Call Flow

This section describes the N2 Hanover without AMF Change call flow.

Figure 45: N2 Handover without AMF Change Call Flow

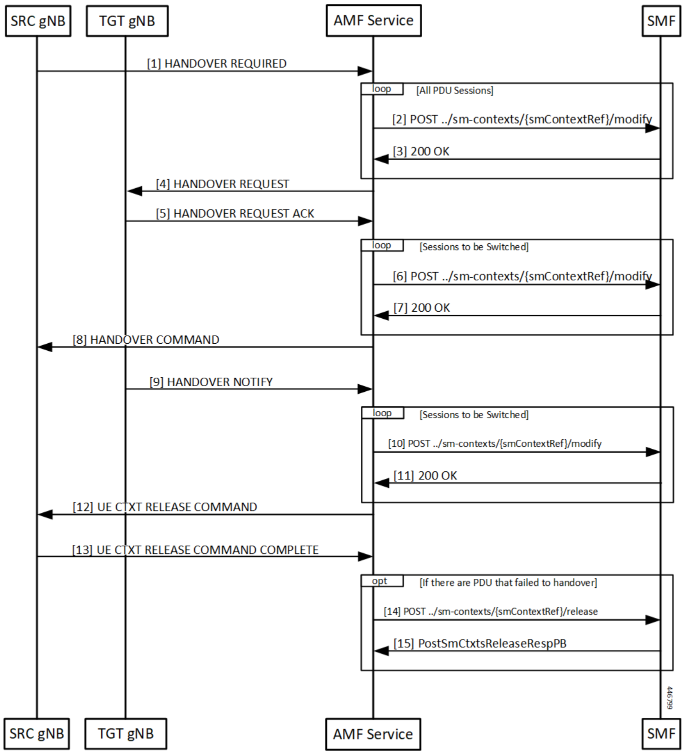

SRC gNB
TGT gNB
AMF Service
SMF
[1] HANDOVER REQUIRED
loop
[All PDU Sessions]
[2] POST ../sm-contexts/{smContextRef}/modify
[3] 200 OK
[4] HANDOVER REQUEST
[5] HANDOVER REQUEST ACK
loop
[Sessions to be Switched]
[6] POST ../sm-contexts/{smContextRef}/modify
[7] 200 OK
[8] HANDOVER COMMAND
[9] HANDOVER NOTIFY
loop
[Sessions to be Switched]
[10] POST ../sm-contexts/{smContextRef}/modify
[11] 200 OK
[12] UE CTXT RELEASE COMMAND
[13] UE CTXT RELEASE COMMAND COMPLETE
opt
[If there are PDU that failed to handover]
[14] POST ../sm-contexts/{smContextRef}/release
[15] PostSmCtxtsReleaseRespPB
446799
SRC gNB
TGT gNB
AMF Service
SMF

Table 93: N2 Handover without AMF Change Call Flow Description

Step	Description
1	With signaling from the UE, the source gNB starts the handover procedure by sending a HANDOVER REQUIRED message to the AMF.
2	The AMF finds a gNB that can support the signaled TargetId from the gNB. AMF rejects the message when it can't find gNB. The AMF creates a ModificationRequest and sends it to the SMF.
3	The SMF analyzes the TargetID and takes appropriate actions. The SMF then responds.
4	The AMF finds the gNB corresponding to the Target ID, and the NGAP EP that serves that gNB. The AMF then sends a handover required message to the target gNB.
5	Target gNB sets up the resources required for the handover and responds with an ACK message. This ACK message contains the PDU resources that failed to setup as well.
6	The AMF constructs a Sm Context Modify message to update the target gNB tunnel endpoint IDs to the SMF. The AMF starts a guard timer and forwards the message to the SMF.
7	The SMF updates the information in associated UPFs and responds to the AMF.
8	The AMF builds a HandoverCommand message and sends it to the source gNB.
9	The UE now completes the handover at the target gNB. The target gNB sends a HANDOVER NOTIFY message to the AMF.
10	The AMF constructs a Sm Context Modify request to inform the SMF that the handover is complete.
11	SMF responds to the update.
12	The Handover procedure ends. The source gNB receives a UE context release command.
13	If there are PDU sessions that fail to setup at the target gNB are now released at the SMF.

N2 Handover with AMF Change

Feature Description

AMF supports N2 handover whenever there's a change in AMF.

Unsupported Scenarios

The following scenarios aren't supported:

- Handover cancelation
- Secondary RAT usage data signaling
- Timeouts from SMF
- Suspend/resume of running procedures

- Handover restrictions
- Service area restrictions
- S-NSSAI checks
- Tracing requirements
- PCF reselection

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

N2 Handover with AMF Change Call Flow

This section describes the N2 Handover with AMF change call flow.

This call flow is similar to the N2 Handover without AMF change except the creation of the context on the new AMF and splitting up of the steps between the two nodes.

Figure 46: N2 Handover with AMF Change Call Flow

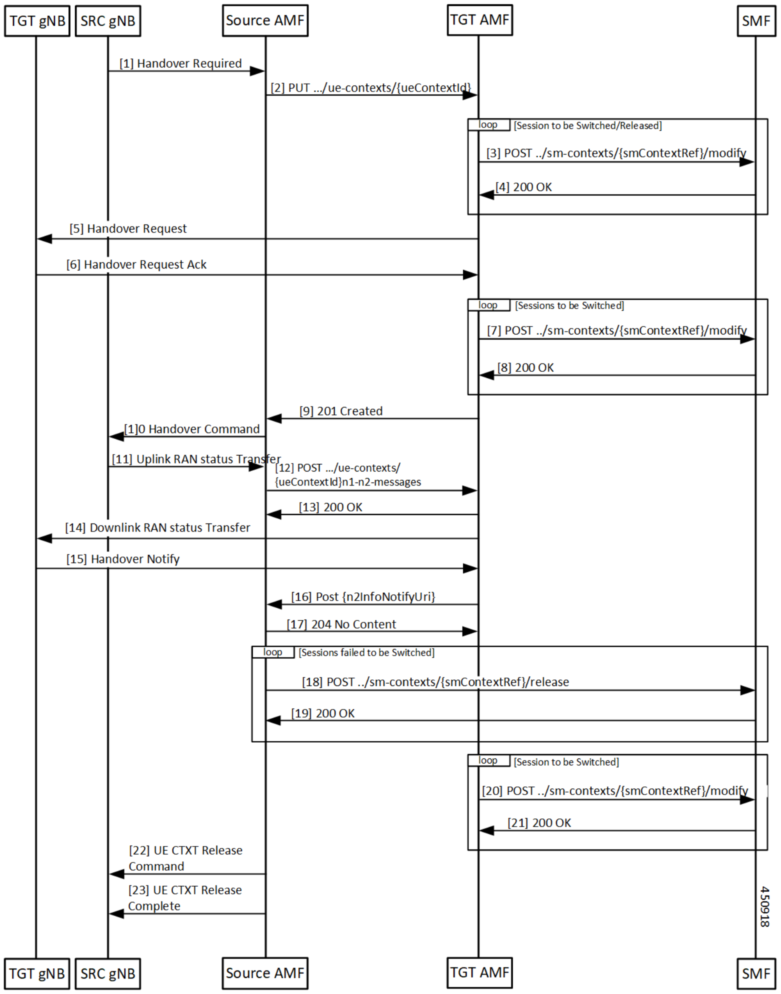

TGT gNB
SRC gNB
Source AMF
TGT AMF
SMF
[1] Handover Required
[2] PUT .../ue-contexts/{ueContextId}
loop [Session to be Switched/Released]
[3] POST ../sm-contexts/{smContextRef}/modify
[4] 200 OK
[5] Handover Request
[6] Handover Request Ack
loop [Sessions to be Switched]
[7] POST ../sm-contexts/{smContextRef}/modify
[8] 200 OK
[9] 201 Created
[1]0 Handover Command
[11] Uplink RAN status Transfer
[12] POST .../ue-contexts/{ueContextId}n1-n2-messages
[13] 200 OK
[14] Downlink RAN status Transfer
[15] Handover Notify
[16] Post {n2InfoNotifyUri}
[17] 204 No Content
loop [Sessions failed to be Switched]
[18] POST ../sm-contexts/{smContextRef}/release
[19] 200 OK
loop [Session to be Switched]
[20] POST ../sm-contexts/{smContextRef}/modify
[21] 200 OK
[22] UE CTXT Release Command
[23] UE CTXT Release Complete
450918
TGT gNB
SRC gNB
Source AMF
TGT AMF
SMF

Table 94: N2 Handover with AMF Change Call Flow Description

Step	Description
1	The source gNB sends a HANDOVER REQUIRED message to the AMF.
2	The AMF analyses the target identifier and recognizes that it's not a target it serves. The AMF selects a new AMF to serve the UE and sends it a CreateUE Context message.
3	The target AMF receives the message and verifies that it can serve the UE. For each PDU session that needs to be handed over, the AMF sends a Modify SM Context message to the SMF.
4	The SMF does all the necessary procedures required to handle the UE in the new target and responds to the AMF.
5	The target AMF identifies the gNB that is going to handle the UE and sends a HANDOVER REQUEST to the gNB.

Step	Description
6	Once the necessary resources are allocated by the target gNB, the target gNB responds with a HANDOVER REQUEST ACK.
7	The AMF updates the SMF with the message transfer IE from the gNB.
8	The SMF responds to the requests from the AMF.
9	The target AMF responds to the source AMF and includes any Target to Source container in the response. This response also includes any PDU sessions that have failed to set up in the target AMF due to any condition.
10	The source AMF sends a HANDOVER COMMAND to the source gNB.
11	The handover completes in the UE and the target gNB sends a HANDOVER NOTIFY to the target AMF.
12	The target AMF indicates receipt of the HANDOVER NOTIFY to the source AMF. This causes the source AMF to start a timer the expiry of which leads to release of resources from the source gNB.
13	The source AMF responds to the target.
14	The source AMF clears any PDU sessions that have failed to set up at the target.
15	The SMF responds to the release request from the source AMF.
16	The target AMF update the SMF on the completion of the handover.
17	The SMF acknowledges the message from the AMF.
18	When the timer expires for clearing of resources (or eventually when the UDM notifies the source that the registration for UECM isn’t valid), the source AMF releases resources both locally and at the gNB. The AMF releases the resources at the gNB by sending a UE CONTEXT RELEASE COMMAND.
19	The source gNB responds with a UE CONTEXT RELEASE COMPLETE message.

CHAPTER 26

Paging Support

Feature Summary and Revision History

Summary Data

Table 95: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 96: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

AMF uses the paging procedure when the network requires to signal the UE which is in CM-IDLE state. For example, N1 signaling to UE, or User Plane connection activation for PDU sessions (to deliver mobile terminated user data). AMF supports paging strategies to minimize the paging load.

Paging Request triggers the UE-initiated Service Request procedure and the paging procedure has the following three essential functionalities:

- Paging Initiation
- Selecting a paging profile
- Paging procedure

Paging Initiation

Paging is done in response to the network needing to communicate with a UE that is in CM-IDLE state. The first step in the process is to analyze the messages from a peer node and decide whether paging is needed or not. The operator policy can decide that paging isn't required under certain circumstances.

When AMF receives the N1N2MsgTransfer from SMF for a UE in CM-IDLE mode, it decides whether to trigger paging or not based on the following checks:

- PPF flag set to true, which indicates mobile reachability timer isn't expired.
- Incoming request doesn't have *skipind* attribute set in *N1N2MsgTransferReqData* IE.
- Incoming request doesn't indicate to transfer a N2 PDU Session Resource Release Command.
- Asynchronous type communication isn't activated at AMF.
- ARP-based paging priority comparisons for the newly received N1N2Msg from SMF with the previous N1N2Msg for which paging is already in progress.

AMF updates the SMF with the appropriate cause. When AMF is satisfied with the preceding checks, it selects paging profile based on the incoming triggers.

AMF doesn't perform any check, when the paging is triggered to Deregister a UE.

Selecting a Paging Profile

AMF supports multiple paging profiles. Paging usually happens in stages, with each stage having its own algorithm configured.

AMF selects the operator policy based on SUPI-prefix. If the SUPI-prefix match isn't found, it selects the operator-policy associated with the AMF-service.

The paging-map can be associated with the operator-policy. Each paging-map has a list of trigger-to-paging profile mapping to support unique precedence for each trigger. The available trigger types are:

- 5QI
- PPI
- DEREG
- DNN
- ARP

Paging profile selection is based on the configured precedence with matching trigger and value pair. When multiple trigger-value pair matches, AMF selects based on the higher precedence. Lower the value, higher the precedence.

Each paging profile has a list of stages with each stage defining a paging-algorithm to use.

Paging Procedure

Paging in AMF minimizes the load on the network and locates the UE with minimal area of paging and attempts.

The first response message from the UE terminates the paging.

Note AMF considers only service request from UE as response to paging.

AMF initiates the paging procedure in the following three scenarios:

- **Clear Subscriber at AMF:** AMF triggers paging, when a subscriber in CM-IDLE state gets cleared through AMF CLI. Paging is followed by the AMF-initiated UE deregistration procedure.
- **UDM-initiated UE Deregistration:** AMF initiates paging when UDM sends Deregistration notification (UDM-initiated UE Deregistration) to AMF for a subscriber which is in CM-IDLE state. If UE doesn't respond, AMF Deregisters the UE and clears the UE in SMF and in PCF. If there’s no paging response, no response is sent back to UDM.
- **N1N2MsgTransfer received from SMF:** AMF initiates paging when it receives N1N2MsgTransfer from SMF for a subscriber that is in CM-IDLE state. If UE doesn't respond, AMF sends N1N2MsgTxfrFailNotification back to SMF over the callback URI.

AMF performs the following procedures during paging:

- Filling of the following IEs in NGAP messages other than mandatory IEs:
  - Paging Discontinuous Reception (DRX)

    It’s filled based on the requested DRX parameters received from the UE during registration.
  - Assistance Data for Paging
    - Assistance Data for Recommended Cells is derived from the *Information on Recommended Cells and RAN Nodes for Paging* IE. AMF receives this IE as part of the UE Context Release Complete message from gNB.
    - AMF fills the *Paging Attempt Information* IE based on the paging algorithm used for the respective paging stage. Whenever there’s a change in the paging stage, AMF marks *Next Paging Area Scope* as changed. AMF doesn't fill *Next Paging Area Scope* for the last attempt of the last paging stage.
  - Paging priority

    It’s applicable if paging trigger is from SMF and priority mapping is configured.
- Handling of the new incoming N1N2Msg when paging is in progress for previous N1N2Msg:

- **Precedence Calculation**: AMF calculates the precedence (lower values considered as higher precedence) as per the incoming parameters along with the paging map configuration. It computes this precedence for the incoming N1N2Msg and performs the following:
  - If new precedence value is lower than ongoing precedence, AMF selects the new paging profile as per the new precedence.
  - If new precedence value is same or greater than ongoing precedence, no new profile is selected and AMF continues with the ongoing paging profile.
- **Priority Comparision**: Paging priority comparison is based on incoming ARP value and its mapped NGAP paging priority under AMF configuration. AMF compares the paging priority (lower values considered as higher priority) of ongoing paging with the new incoming paging, and performs the following:
  - AMF rejects the incoming N1N2 with the cause HIGHER_PRIORITY_REQUEST_ONGOING as part of N1N2MsgTransferError when:
    - The ongoing paging has high or same priority as incoming paging.
    - The incoming paging doesn’t have any paging priority mapped to it.

    In this scenario, AMF doesn't select any new paging profile. AMF fills N1N2MsgTxfrErrDetail as part of the N1N2MsgTransferError. AMF fills the *retryAfter* attribute, based on the ongoing and pending paging stages.
  - If incoming N1N2Msg has high priority, AMF triggers a new paging message with a new paging priority value. AMF triggers new paging as part of the ongoing paging attempt of the ongoing paging stage.

Note Paging profile selection and triggering of new paging with new priority are independent of each other.

- Sending a PAGING message to each gNB (belonging to the UE tracking areas) based on the actions configured under paging algorithm for respective paging stages
- Paging in stages, where each stage defines the scope of paging. Each paging stage is associated with a paging algorithm that consists of paging action.

  AMF supports the following paging actions:
  - PAGING_LAST_GNB_LAST_TAI
  - PAGING_LAST_N_GNB_LAST_TAI
  - PAGING_ALL_GNB_LAST_TAI
  - PAGING_ALL_GNB_ALL_TAI
  - PAGING_ALL_GNB_REM_TAI_ALL
  - PAGING_ALL_GNB_REM_TAI_SEQ

PAGING_LAST_GNB_LAST_TAI - As part of this action, AMF pages the last gNB in the last Tracking Area Identifier (TAI) from which UE contacted AMF.

PAGING_LAST_N_GNB_LAST_TAI - As part of this action, AMF pages the last n gNB in the last TAI from which UE contacted AMF.

PAGING_ALL_GNB_LAST_TAI - As part of this action, AMF pages all the gNBs in the last TAI from which UE contacted AMF.

PAGING_ALL_GNB_ALL_TAI - As part of this action, AMF pages all the gNBs in all the TAIs as part of UE restricted area.

PAGING_ALL_GNB_REM_TAI_ALL - As part of this action, AMF pages the remaining TAIs (Except the last known TAI) all together.

Example: If UE's registration area contains TAI A, B, C, and the last known TAI is A, AMF pages gNBs in TAI B, C together at the same time.

PAGING_ALL_GNB_REM_TAI_SEQ - As part of this action, AMF pages the remaining TAIs (Except the last known TAI) in a sequential manner. There’s no specific order in which AMF selects the TAI when paging is sequential.

Example: If UE's registration area contains TAI A, B, C, and the last known TAI is A, AMF first pages gNBs in TAI B. When no response is received for paging after reaching the maximum attempts, AMF proceeds to page gNBs in TAI C.

Note AMF doesn’t support PAGING_ALL_GNB_REM_TAI_ALL and PAGING_ALL_GNB_REM_TAI_SEQ as first stage of paging profile.

The t3513 timeout value and number of retries at a given stage is configurable as part of paging-algo. The maximum number of gNB to page is also configurable and it is applicable only to paging action PAGING_LAST_N_GNB_LAST_TAI.

AMF uses default paging-algo, when no paging map or profile or algo or matching triggers are configured for the incoming paging trigger.

Default paging-algo has only one stage and has the following parameters:

- action is all_gnb_last_tai, which is configured automatically.
- max-paging-attempts and timeout value is fetched from the configured t3513 timer under Call Control Profile.

  The default value of the t3513 timer is set to five seconds and the default paging retry count is set to two.

Feature Configuration

Configuring this feature involves the following steps:

1. Operator Policy - AMF allows you to configure the Operator defined policies. This configuration provides the commands to configure the operator defined policies for UE. For more information, refer to Configuring the Operator Policy, on page 182.

2. Paging Map - AMF allows you to map the precedence, trigger (traffic-type), trigger-value, and its profile name to the paging. This configuration provides the commands to configure the paging map for UE. For more information, refer to Configuring the Paging Map, on page 183.
3. Paging Profile - AMF allows you to configure paging stage and paging algorithm in paging profile. This configuration provides the commands to configure the paging profile for UE. For more information, refer to Configuring the Paging Profile, on page 184.
4. Paging Algorithm - AMF allows you to configure paging algorithm with its name, action and with other associated parameters. This configuration provides the commands to configure the paging algorithm for UE. For more information, refer to Configuring the Paging Algorithm, on page 185.
5. Paging Priority - AMF allows you to configure a map of ARP values to NGAP paging priority. This configuration provides the commands to configure the priority for the paging. For more information, refer to Configuring the Paging Priority, on page 186.

Configuring the Operator Policy

To configure the Operator Policy, use the following configuration:

```
config
 amf-global
  operator-policy operator_policy_name
   paging-map-name paging_map_name
   end
```

NOTES:

- **operator-policy** *operator_policy_name*—Specify the operator policy name.
- **paging-map-name** *paging_map_name*—Specify the name of paging map. Must be a string in the size of 1–64 characters.

Configuration Example

The following is an example configuration.

```
config
 amf-global
  operator-policy local
   paging-map-name pm1
   end
```

Configuration Verification

To verify the configuration:

```
show full-configuration amf-global operator-policy local
amf-global
operator-policy local
ccp-name local
paging-map-name pm1
```

Configuring the Paging Map

To configure the Paging Map, use the following configuration:

```
config
 amf-global
  paging-map paging_map_name
   precedence precedence_count
     trigger-type
      5qi { fiveqi-value fiveqi_value | paging-profile-name profile_name }
      arp { arp-value arp_value | paging-profile-name profile_name }
      dereg { dereg-value { amf_init paging-profile-name profile_name |
udm_init paging-profile-name profile_name } | paging-profile-name profile_name
 }
      dnn { dnn-value  dnn_value | paging-profile-name profile_name }
      ppi { ppi-value  ppi_value | paging-profile-name profile_name }
      end
```

NOTES:

- **paging-map** *paging_map_name*—Specify the paging map.

  Based on the fetched paging map from the operator policy, a matching paging map is selected from paging-map list configured in amf-global.

  Each paging-map is a list of triggers having unique precedence associated with them. Based on the high precedence value matched trigger (with trigger value), the associated paging-profile is selected.

- **precedence** *precedence_count* —Specify the map precedence level. Must be an integer in the range of 1–255. 1: High and 255: Low.

- **paging-profile-name** *profile_name*—Specify the paging profile name. Must be a string of 1–64 characters.

- **trigger-type**—Specify the trigger type. Trigger can be the traffic type. Must be one of the following:

  - 5qi - 5G QoS Identifier, received as part of N1N2 message from SMF.
  - dereg - Paging Policy Indicator, received as part of N1N2 message from SMF.
  - ppi - Paging triggered due to Deregistration by UDM or AMF.
  - dnn - DNN for which paging is triggered.
  - arp - Allocation and Retention Priority, received as part of N1N2 message from SMF.

- **fiveqi-value** *fiveqi_value* —Specify QoS Indicator value. Must be an integer in the range of 1–85.

- **arp-value** *arp_value*—Specify the allocation and retention priority value. Must be an integer in the range of 1–15.

- **dereg-value**—Specify the deregistration trigger value which is either amf_init or udm_init.

- **dnn-value** *dnn_value*—Specify the Data Network Name value. Must be a string of 1–64 characters.

- **ppi-value** *ppi_value*—Specify the Paging Policy Indicator value. Must be an integer in the range of 1–7.

Configuration Example

The following is an example configuration.

```
config
 amf-global
  paging-map pm1
   precedence 1
    trigger-type 5qi
    fiveqi-value 5
    paging-profile-name ppn1
    end
```

Configuration Verification

To verify the configuration:

```
show full-configuration amf-global paging-map pm1
amf-global
paging-map pm1
precedence 1
triggertype   5qi
fiveqi-value  5
paging-profile-name ppn1
```

Configuring the Paging Profile

To configure the Paging profile, use the following configuration:

```
config
 amf-global
  paging-profile paging_profile_name
   paging-stage paging_stage_count
   end
```

NOTES:

- **paging-profile** *paging_profile_name*—Specify the paging profile name. Each paging profile is a list of paging stages wherein stages are selected in increasing order of their number. Once paging stage is selected, paging algorithm associated with paging stage is selected.
- **paging-stage** *paging_stage_count*—Specify the paging stage precedence value in the range of 1-5. 1: High, 5: Low. Paging profile can have multiple stages. Stage defines the scope of paging.

Configuration Example

The following is an example configuration.

```
config
 amf-global
  paging-profile pp1
   paging-stage 1
    paging-algo pa1
```

Configuration Verification

To verify the configuration:

```
show full-configuration amf-global paging-profile pp1
amf-global
paging-profile pp1
paging-stage 1
paging-algo pa1
```

Configuring the Paging Algorithm

To configure Paging algorithm, use the following configuration:

```
config
 amf-global
  paging-algo paging_algorithm_name
   action { all_gnb_all_tai | all_gnb_last_tai | all_gnb_remaining_tai_all
  | all_gnb_remaining_tai_seq | last_gnb_last_tai | last_n_gnb_last_tai }
    max-n-gnb max_n_gnb_count
    max-paging-attempts attempts_count
    t3513-timeout timeout_value
    end
```

NOTES:

- **paging-algo** *paging_algorithm_name*—Specify the paging algorithm.
- **action { all_gnb_all_tai | all_gnb_last_tai | all_gnb_remaining_tai_all | all_gnb_remaining_tai_seq | last_gnb_last_tai | last_n_gnb_last_tai }**—Specify the paging action.
- **max-n-gnb** *max_n_gnb_count*—Specify the number of gNBs to page. It's the number of last gNBs from which UE contacted AMF. Must be an integer in the range of 1–5.

  AMF uses **max-n-gnb** when paging action is **last_n_gnb_last_tai**.
- **max-paging-attempts** *attempts_count* —Specify the maximum number of paging attempts. It's an integer in the range of 1–5.
- **t3513-timeout** *timeout_value*—Specify the paging timeout in seconds. Stops paging if all retries are done otherwise it performs retry. Must be an integer in the range of 1–10.

Configuration Example

The following is an example configuration.

```
config
 amf-global
  paging-algo pa1
   action last_gnb_last_tai
    max-n-gnb 5
    max-paging-attempts 2
    t3513-timeout 5
    end
```

Configuration Verification

To verify the configuration:

```
show full-configuration amf-global paging-algo pa1
amf-global
paging-algo pa1
```

```
action last_gnb_last_tai
max-n-gnb 5
t3513  5
max-paging-attempts 2
```

Configuring the Paging Priority

To configure the Paging priority, use the following configuration:

```
config
 amf-global
  call-control-policy call_control_policy_name
   paging-priority map arp arp_value ngap-paging-priority priority_value
   end
```

NOTES:

- **call-control-policy** *call_control_policy_name*—Specify the operator policy name.
- **paging-priority map arp** *arp_value* **ngap-paging-priority** *priority_value*—Specify the paging priority mapping value for ARP and NGAP. The NGAP paging priority value must be an integer in the range of 0-7.

  AMF allows you to map incoming ARP value from SMF to NGAP paging priority.

  When configured, AMF does the following:

  - Populates the paging priority IE in PAGING message and sends to gNB.
  - Handles new incoming N1N2 message as per the configuration, when paging is already in progress.

Configuration Example

The following is an example configuration.

```
config
  amf-global
   call-control-policy local
    paging-priority map arp 5 ngap-paging-priority 1
    paging-priority map arp 8 ngap-paging-priority 2
    end
```

Configuration Verification

To verify the configuration:

```
show full-configuration amf-global call-control-policy local paging-priority
amf-global
call-control-policy local
paging-priority map arp 5 ngap-paging-priority 1
paging-priority map arp 8 ngap-paging-priority 2
```

AMF Paging Configuration Example

The following is an example configuration.

```
config
amf-global
```

```
operator-policy local
  ccp-name        local
  paging-map-name pm1
  ..
 exit
paging-map pm1
  precedence 1
   trigger-type        arp
   arp-value           5
   paging-profile-name pp3
  exit
  precedence 2
   trigger-type        dereg
   dereg-value         udm_init
   paging-profile-name pp4
  exit
  precedence 3
   trigger-type        ppi
   ppi-value           7
   paging-profile-name pp1
  exit
  precedence 4
   trigger-type        5qi
   fiveqi-value        5
   paging-profile-name pp4
  exit
  precedence 5
   trigger-type        dereg
   dereg-value         amf_init
   paging-profile-name pp4
  exit
  precedence 6
   trigger-type        ppi
   ppi-value           6
   paging-profile-name pp5
  exit
precedence 9
   trigger-type        dnn
   dnn-value           starent1.com
   paging-profile-name pp4
  exit
 exit
 paging-profile pm1
 exit
 paging-profile pp1
  paging-stage 1
   paging-algo pa1
  exit
 exit
 paging-profile pp2
  paging-stage 1
   paging-algo pa2
  exit
 exit
 paging-profile pp3
  paging-stage 2
   paging-algo pa4
  exit
  paging-stage 3
   paging-algo pa1
  exit
  paging-stage 4
   paging-algo pa2
  exit
  paging-stage 5
   paging-algo pa3
  exit
 exit
 paging-profile pp4
  paging-stage 1
   paging-algo pa1
  exit
  paging-stage 2
   paging-algo pa2
  exit
  paging-stage 3
   paging-algo pa3
  exit
  paging-stage 4
   paging-algo pa6
  exit
  paging-stage 5
   paging-algo pa4
  exit
 exit
 paging-profile pp5
  paging-stage 5
   paging-algo pa5
  exit
 exit
 paging-algo pa1
  action              last_gnb_last_tai
  max-n-gnb           3
  t3513-timeout       2
  max-paging-attempts 1
 exit
 paging-algo pa2
  action              last_n_gnb_last_tai
  max-n-gnb           3
  t3513-timeout       3
  max-paging-attempts 2
 exit
 paging-algo pa3
  action              all_gnb_last_tai
  max-n-gnb           5
  t3513-timeout       4
  max-paging-attempts 3
 exit
 paging-algo pa4
  action              all_gnb_all_tai
  max-n-gnb           5
  t3513-timeout       5
  max-paging-attempts 5
 exit
 paging-algo pa5
  action              all_gnb_all_tai
  max-n-gnb           5
  t3513-timeout       10
  max-paging-attempts 5
 exit
 paging-algo pa6
  action              all_gnb_remaining_tai_all
  max-n-gnb           5
  t3513-timeout       5
  max-paging-attempts 1
 end
```

CHAPTER 27

gNB-Initiated Reset Procedure

Feature Summary and Revision History

Summary Data

Table 97: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 98: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

If a failure occurs at the NG-RAN node, it causes data loss in all or part of the transaction reference information. In order to recover from the failure, the gNB initiates a reset procedure towards AMF to release the resources. This procedure initializes or reinitializes the RAN, and provides an opportunity for new transactions.

The NG reset procedure resets all the UE sessions; during partial reset, you can reset particular UE sessions by using the partOfNG-Interface IE when sending NG Application Protocol (NGAP) ID for those sessions.

A sample partial reset IE:

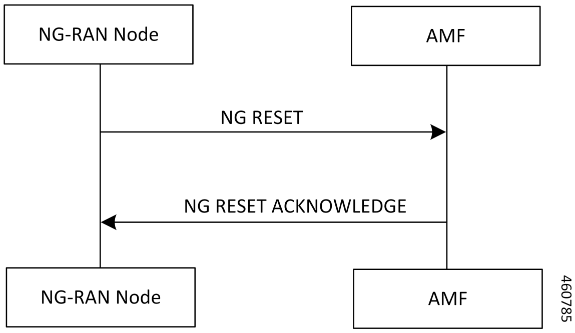
```
IE Type: id-ResetType(88)
{'ResetType': {'choice-Extensions': None,
'nG-Interface': None,
'partOfNG-Interface': {0: {'UE-associatedLogicalNG-connectionItem': {'aMF-UE-NGAP-ID':
4194359,
'iE-Extensions': None,
'rAN-UE-NGAP-ID': 12346}}}}}
```

How it Works

The gNB sends a Reset message to AMF when an event fails on the NG-RAN node. On receiving the message, the AMF releases all the allocated resources specified (implicitly and explicitly) in the Reset message. AMF allocates the resources related to UE associations on the NG node. The AMF also erases the NGAP ID assigned to the UE associations. After resetting the resources, the AMF sends a Reset Acknowledgment message to gNB indicating that the procedure is complete.

The following figure illustrates the reset procedure between gNB and AMF.

Figure 47: Reset Procedure Initiated from gNB to AMF



CHAPTER 28

Periodic Registration Support

Feature Summary and Revision History

Summary Data

Table 99: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 100: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

The Access and Mobility Management Function (AMF) supports periodic registration to the UE to confirm its availability. The procedure is controlled in the UE by the periodic registration update timer, T3512.

The timer that is run in the AMF is called the Mobile Reachability timer. It is configurable but is different from T3512. T3512 is the configured in the UE, and the Mobile Reachability (MR) Timer is set to 4 minutes higher than T3512

The MR timer in the AMF is restarted every time the UE moves to Idle, and stopped when the AMF receives any message from the UE.

When the MR timer expires, the AMF stops paging the UE.

The periodic registration timer (T3512) is supported as per 3GPP TS 24.501 v15.0.0. Currently, in AMF, the T3512 timer expiry supports implicit deregistration.

T3512 Timer Start

The T3512 timer value is read from configuration. If the value is not configured, then the default value of 54 minutes is used.

The T3512 timer starts for a subscriber when the UE moves to IDLE state (releases N2 connection).

The value of the T3512 timer is sent by the AMF to the UE in the Registration Accept message. The UE registers periodically as per the T3512 timer interval.

T3512 Timer Stop

The T3512 timer value stops when the UE moves to CONNECTED state (establishes an N2 connection).

Sending T3512 Value in Registration Accept

The AMF sends the T3512 timer value in the Registration Accept message and the UE uses this value to send periodic registration information.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows of Priodic Registration feature.

Periodic Registration without Authentication Call Flow

This section describes the Periodic Registration without Authentication call flow.

Figure 48: Periodic Registration without Authentication Call Flow

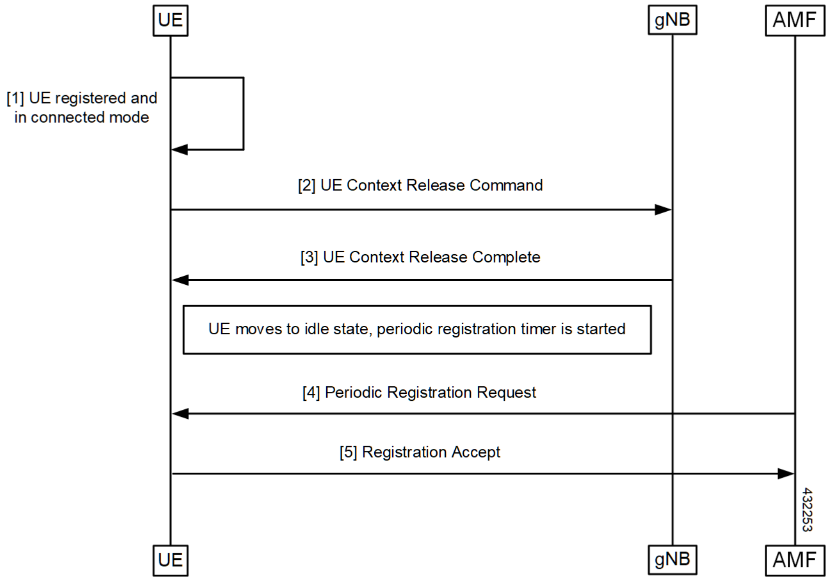

UE
gNB
AMF
[1] UE registered and in connected mode
[2] UE Context Release Command
[3] UE Context Release Complete
UE moves to idle state, periodic registration timer is started
[4] Periodic Registration Request
[5] Registration Accept
432253
UE
gNB
AMF

Table 101: Periodic Registration without Authentication Call Flow Description

Step	Description
1	UE registerd with the network and it is in connected mode.
2, 3	UE sends context Release command to gNB and receives response from it.
4, 5	When UE moves to IDLe state, a periodic timer started and AmF sends periodic registration request to UE and receives registration accept from UE.

Periodic Registration with Authentication Call Flow

This section describes the Periodic Registration with Authentication call flow.

Figure 49: Periodic Registration with Authentication Call Flow

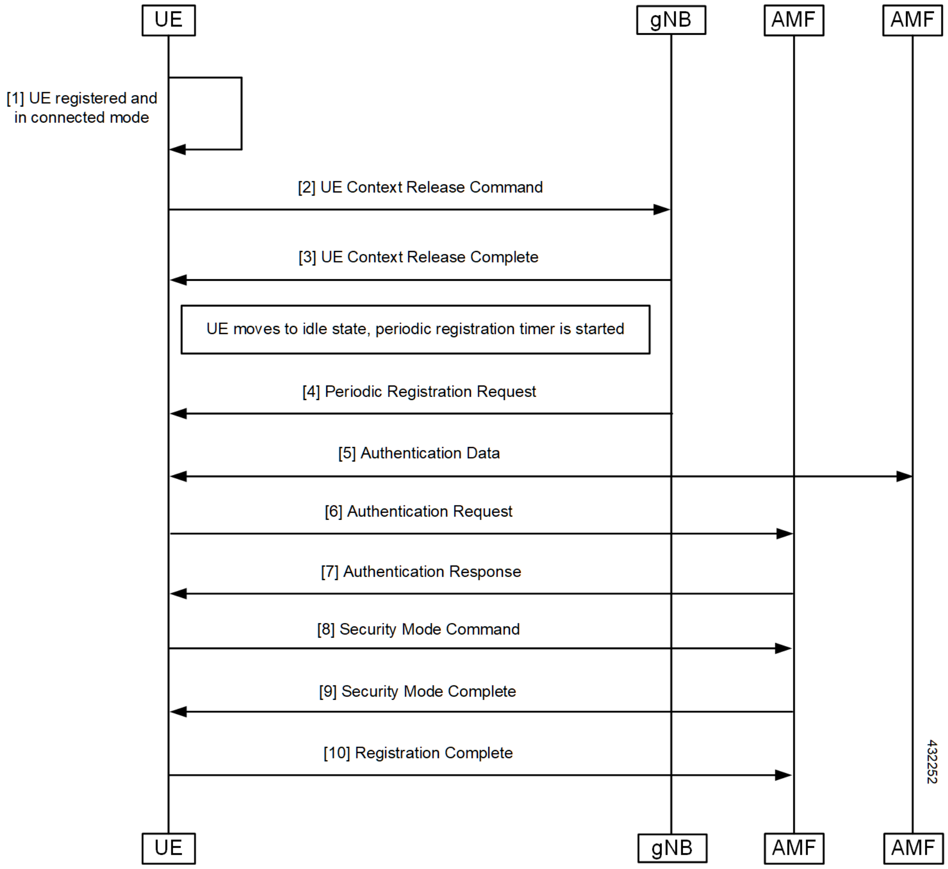

UE
gNB
AMF
AMF
[1] UE registered and in connected mode
[2] UE Context Release Command
[3] UE Context Release Complete
UE moves to idle state, periodic registration timer is started
[4] Periodic Registration Request
[5] Authentication Data
[6] Authentication Request
[7] Authentication Response
[8] Security Mode Command
[9] Security Mode Complete
[10] Registration Complete
432252
UE
gNB
AMF
AMF

Table 102: Periodic Registration with Authentication Call Flow Description

Step	Description
1	Periodic Registration with Authentication UE registerd with the network and it is in connected mode.
2, 3	UE sends context Release command to gNB and receives response from it.
4	When UE moves to IDLe state, a periodic timer started and gNB sends periodic registration request to UE .
5	Authentication data exchanged between UE and AMF.
6, 7	UE sends authentication request to AMF and receives respose from it.
8, 9	UE sends security mode command to AMF and receives security mode complete command from it.
10	UE sends Registration complete message to gNB.

Feature Configuration

Configuring this feature involves the following steps.

- T3512 timer is configured in the call-control profile. For more information, refer to Configuring the T3512 Timer, on page 195.
- Periodic registration is enabled in the call-control profile. For more information, refer to Configuring Authentication Enable, on page 195.

Configuring the T3512 Timer

To configure the T3512 timer, use the following configuration.

```
config
   amf-global
      call-control-policy policy_name
         timers t3512 value value_in_seconds
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the UE call control polocy name.
- **timers t3512 value** *value_in_seconds*—Specify the T3512 timer value in seconds. It's an unsigned integer in the range from 0-35712000.

Configuring Authentication Enable

To enable the authentication, use the following configuration.

```
configure
   amf-global
      call-control-policy policy_name
         enable-auth-periodic-reg [ false | true ]
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the UE call control polocy name.
- **enable-auth-periodic-reg [false | true]**—Allows to set enabling authenticated periodic registration request as true or false.

OAM Support

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

Bulk Statistics Support

The following statistics are supported for the periodic registration feature

- periodic_registration_request - The number of Periodic Registration Request messages received.
- NumPeroidicRegTimerExpiry - The number of Periodic Registration timer expires.

CHAPTER 29

SCTP Multihoming

Feature Summary and Revision History

Summary Data

Table 103: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 104: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

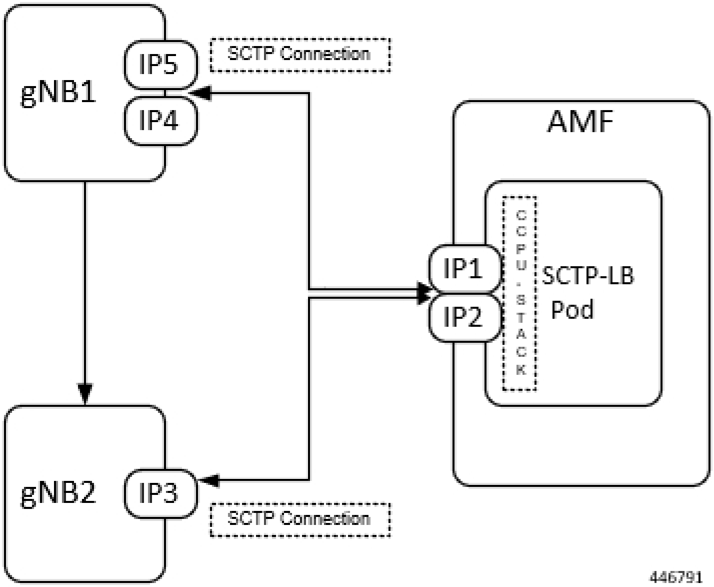
Feature Description

AMF now supports a single SCTP POD (single instance) SCTP multihoming where in the ccpu-sctp stack comes up with list of supported Host IPs. As a part of the association formation the association Id corresponds to the list of IPs, instead of single IP.

The stack also supports multihoming for scenarios such as, one-to-many and many-to-many connections until any of IPs are available on either side of SCTP end points (AMF and gNB). At the same time, traffic over multiple IPs is also possible.

The following figure is a depiction of SCTP Multihoming support:

Figure 50: SCTP Multihoming Support



As per the figure following SCTP associations are formed:

1. Associd – 0 [{IP1,IP2},{IP4,IP5}]
2. Associd – 1 [{IP1,IP2},{IP3}]

Limitations

The SCTP multihoming feature has the following limitations:

Currently, dynamic adding/removing IPs from multihoming configuration without POD restart is not supported. POD restart is required.

CHAPTER 30

Service Request Procedure

Feature Summary and Revision History

Summary Data

Table 105: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 106: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

The AMF supports the Service Request procedure, used by a UE in CM-IDLE state or the 5GC, to request the establishment for a secure connection to an AMF. The Service Request procedure is also used when the

UE is in CM-IDLE and in CM-CONNECTED state to activate a User Plane connection for an established PDU Session.

Limitations

In this release, the known limitations of this feature include:

- AMF supports only the UE triggered service request.
- Authentication is not done for service request.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows of Service Request Procedure feature.

UE Triggered Service Request

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. After receiving the Service Request message, the AMF performs authentication. After the establishment of the signaling connection to an AMF, the UE or network sends signaling messages, for example, PDU Session establishment from UE to the SMF, through the AMF.

The Service Request procedure is used by a UE in CM-CONNECTED state to request activation of User Plane connection for PDU Sessions and to respond to a NAS Notification message from the AMF.

For any Service Request, the AMF responds with a Service Accept message to synchronize PDU Session status between UE and network, if necessary. If the Service Request cannot be accepted by the network, the AMF responds with a Service Reject message to UE. The Service Reject message includes an indication or cause-code requesting the UE to perform Registration Update procedure. The Service Reject message is sent for unknown subscriber or if the TAC in Service Request does not match the last known user location.

Idle Mode Call Flow

The following section describes Idle Mode call flow for Service Request triggered by UE in Idle mode.

Figure 51: Idle Mode Call Flow

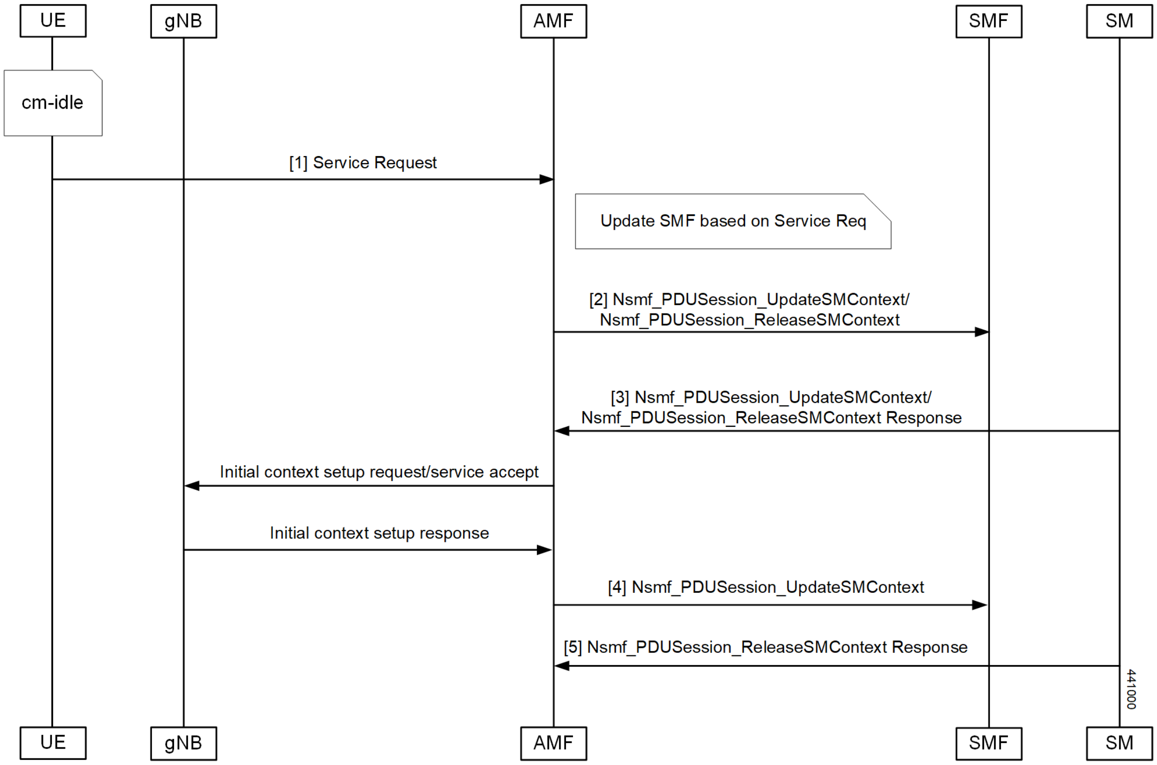

UE
gNB
AMF
SMF
SM
cm-idle
[1] Service Request
Update SMF based on Service Req
[2] Nsmf_PDUSession_UpdateSMContext/
Nsmf_PDUSession_ReleaseSMContext
[3] Nsmf_PDUSession_UpdateSMContext/
Nsmf_PDUSession_ReleaseSMContext Response
Initial context setup request/service accept
Initial context setup response
[4] Nsmf_PDUSession_UpdateSMContext
[5] Nsmf_PDUSession_ReleaseSMContext Response
441000
UE
gNB
AMF
SMF
SM

Table 107: Idle Mode Call Flow Description

Step	Description
1	UE initiates Service Request procedure by sending Service Request to (R)AN : AN message (AN parameters, Service Request (List Of PDU Sessions To Be Activated, List Of Allowed PDU Sessions, security parameters, PDU Session status)). The Service Request message is sent in INITIAL UE Message.
2	AMF determines the PDU Session(s) to be activated and sends an Nsmf_PDUSession_UpdateSMContext Request to SMF(s) associated with the PDU Session(s) with upCnxState set to "ACTIVATING". AMF also initiates PDU Session Release procedure in the network for the PDU Sessions whose PDU Session ID(s) were indicated by the UE as not available in the PDU Session status.
3	For a PDU Session that the SMF has determined to accept the activation of UP connection, the SMF sends Nsmf_PDUSession_UpdateSMContext Response with N2 SM information to the AMF. The N2 SM information contains information that the AMF provides to the NG-RAN. If SMF rejects the activation of UP of the PDU Session, it sends Nsmf_PDUSession_UpdateSMContext Response with cause.

Step	Description
4	AMF to (R)AN: If the Service Request was triggered in CM-IDLE state, AMF sends Initial Context Setup Request with the N2 SM information received from SMF, MM NAS Service Accept and the other required parameters. If the Service Request was triggered in CM-CONNECTED state, AMF sends PDU Session Resource Setup Request with N2 SM information received from SMF and MM NAS Service Accept. MM NAS Service Accept includes PDU Session status in AMF. If the activation of UP of a PDU Session is rejected by an SMF, then the MM NAS Service Accept includes the PDU Session ID and the cause why the User Plane resources were not. Any local PDU Session Release during the Service Request procedure is indicated to the UE via the Session Status. If there are multiple PDU Sessions that involves SMF update, AMF waits for response from all SMFs before sending N2 SM information and MM NAS Service Accept to the RAN.
5	AMF receives N2 Request Ack and if this contains N2 SM information, then it sends Nsmf_PDUSession_UpdateSMContext Request per PDU Session with this information to the SMF.

Connected Mode Call Flow

The following figure illustrates the flow for Service Request triggered by UE in Connected mode.

Figure 52: Connected Mode Call Flow

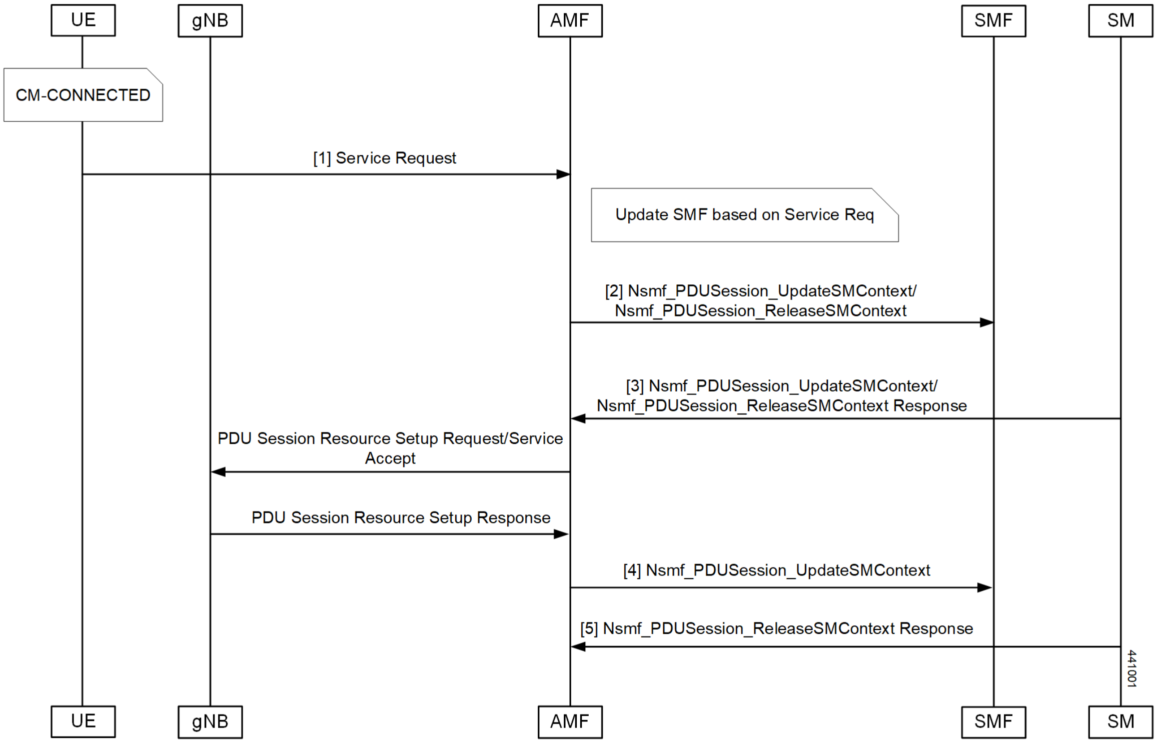

UE
gNB
AMF
SMF
SM
CM-CONNECTED
[1] Service Request
Update SMF based on Service Req
[2] Nsmf_PDUSession_UpdateSMContext/ Nsmf_PDUSession_ReleaseSMContext
[3] Nsmf_PDUSession_UpdateSMContext/ Nsmf_PDUSession_ReleaseSMContext Response
PDU Session Resource Setup Request/Service Accept
PDU Session Resource Setup Response
[4] Nsmf_PDUSession_UpdateSMContext
[5] Nsmf_PDUSession_ReleaseSMContext Response
441001
UE
gNB
AMF
SMF
SM

Table 108: Connected Mode Call Flow Description

Step	Description
1	UE initiates Service Request procedure by sending Service Request to (R)AN : AN message (AN parameters, Service Request (List Of PDU Sessions To Be Activated, List Of Allowed PDU Sessions, security parameters, PDU Session status)). The Service Request message is sent in UPLINK NAS TRANSPORT Message.
2	AMF determines the PDU Session(s) to be activated and sends an Nsmf_PDUSession_UpdateSMContext Request to SMF(s) associated with the PDU Session(s) with upCnxState set to "ACTIVATING". AMF also initiates PDU Session Release procedure in the network for the PDU Sessions whose PDU Session ID(s) were indicated by the UE as not available in the PDU Session status.
3	For a PDU Session that the SMF has determined to accept the activation of UP connection, the SMF sends Nsmf_PDUSession_UpdateSMContext Response with N2 SM information to the AMF. The N2 SM information contains information that the AMF provides to the NG-RAN. If SMF rejects the activation of UP of the PDU Session, it sends Nsmf_PDUSession_UpdateSMContext Response with cause.
4	AMF to (R)AN: If the Service Request was triggered in CM-IDLE state, AMF sends Initial Context Setup Request with the N2 SM information received from SMF, MM NAS Service Accept and the other required parameters. If the Service Request was triggered in CM-CONNECTED state, AMF sends PDU Session Resource Setup Request with N2 SM information received from SMF and MM NAS Service Accept. MM NAS Service Accept includes PDU Session status in AMF. If the activation of UP of a PDU Session is rejected by an SMF, then the MM NAS Service Accept includes the PDU Session ID and the cause why the User Plane resources were not. Any local PDU Session Release during the Service Request procedure is indicated to the UE via the Session Status. If there are multiple PDU Sessions that involves SMF update, AMF waits for response from all SMFs before sending N2 SM information and MM NAS Service Accept to the RAN.
5	AMF receives N2 Request Ack and if this contains N2 SM information, then it sends Nsmf_PDUSession_UpdateSMContext Request per PDU Session with this information to the SMF.

OAM Support

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

Statistics

The following statistics are available in support of the Service Request Procedure feature:

- Number of Service Requests Received
- Number of Service Accepts Sent

- Number of Service Rejects Sent

CHAPTER 31

Session Timers

Feature Summary and Revision History

Summary Data

Table 109: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 110: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF supports the following timers:

- **T3502** (t3502): It operates in the 5GMM-DEREGISTERED and 5GMM-REGISTERED states. AMF provides this timer value to UE in the Registration Accept and Registration Reject messages.
- **T3512** (t3512): It operates in the 5GMM-REGISTERED state. AMF provides this timer value to UE in the Registration Accept message.
- **T3513**: It operates in the 5GMM-REGISTERED state. It starts when the Paging procedure is initiated (with default paging algorithm) and stops when the Paging procedure ends (with the reception of paging response).
- **T3522** (t3522): It operates in the 5GMM-DEREGISTERED-INITIATED state. It starts with the transmission of Deregistration Request message and stops after receiving Deregistration Accept message.
- **T3550** (t3550): It operates in the 5GMM-COMMON-PROCEDURE-INITIATED state. It starts with the transmission of Registration Accept message and stops after receiving the Registration Complete message.
- **T3555** (t3555): It operates in the 5GMM-REGISTERED state. It starts with the transmission of Configuration Update Command message with the ACK bit set in the Configuration Update Indication IE. Stops with the Configuration Update complete message.
- **T3560** (t3560): It operates in the 5GMM-COMMON-PROCEDURE-INITIATED state. It starts with the transmission of Authentication Request message and Security Mode Command. Stops after receiving the following messages:
  - Authentication Response
  - Authentication Failure
  - Security Mode Complete
  - Security Mode Reject
- **T3570** (t3570): It operates in the 5GMM-REGISTERED state. It starts with the transmission of Identity Request message and stops after receiving the Identity Response message.
- **HO Supervisory** (ho-supervisory): It supervises PDU responses from SMF during N2, N26, and Xn handovers.
- **Tidt** (tidt): It starts after four minutes of T3512 timer expiry. The subscriber gets Deregistered implicitly upon this timer expiry.
- **Tpurge** (tpurge): It starts when the Tidt timer expires. AMF sends a request to the UDM to Deregister (purge) the UE from the UDM for 3GPP access upon this timer expiry.

For information on the timer configurations, refer to Feature Configuration, on page 211.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for the AMF timers.

T3502 Call Flow

This section describes the T3502 timer call flow.

Figure 53: T3502 Timer Call Flow

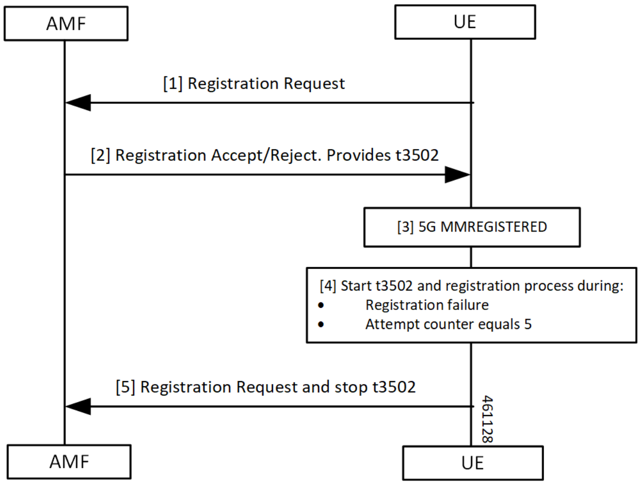

AMF
UE
[1] Registration Request
[2] Registration Accept/Reject. Provides t3502
[3] 5G MMREGISTERED
[4] Start t3502 and registration process during:
• Registration failure
• Attempt counter equals 5
[5] Registration Request and stop t3502
461128
AMF
UE

Table 111: T3502 Timer Call Flow Description

Step	Description
1, 2	The UE sends the Registration Request to the AMF and receives response of reject or accept. The UE starts the T3502 timer.
3	The 5G MM Registration process takes place at the UE.
4	The UE starts the T3502 timer and the Registration process during: • Registration failure or • Attempt counter equals 5.
5	The UE sends Registration Request to the AMF and stops the T3502 timer.

T3512 Call Flow

This section describes the T3512 timer call flow.

Figure 54: T3512 Timer Call Flow

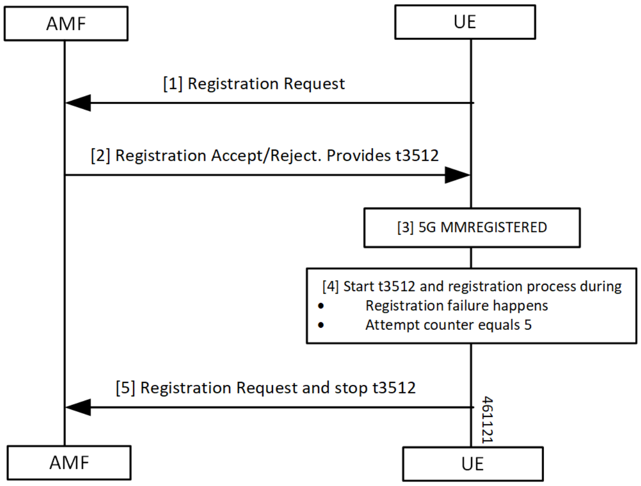

AMF
UE
[1] Registration Request
[2] Registration Accept/Reject. Provides t3512
[3] 5G MMREGISTERED
[4] Start t3512 and registration process during
• Registration failure happens
• Attempt counter equals 5
[5] Registration Request and stop t3512
461121
AMF
UE

Table 112: T3512 Timer Call Flow Description

Step	Description
1, 2	The UE sends Registration Request to the AMF and receives response of reject or accept. The UE starts the T3512 timer.
3	The 5G MM Registration process takes place at the UE.
4	The UE starts the T3512 timer and the Registration process during: • Registration failure or • Attempt counter equals 5.
5	The UE sends Registration Request to the AMF and stops the T3512 timer.

T3522 Call Flow

This section describes the T3522 timer call flow.

Figure 55: T3522 Timer Call Flow

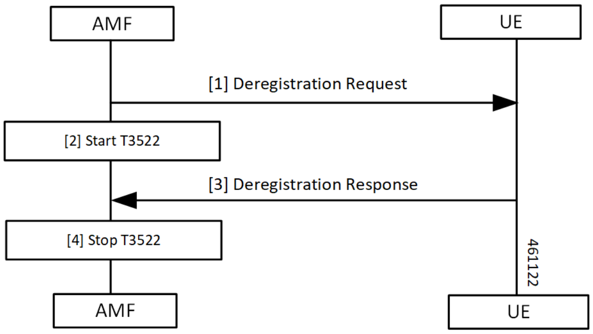


Table 113: T3522 Timer Call Flow Description

Step	Description
1, 2	The AMF sends the Deregistration Request to the UE and starts the T3522 timer.
3, 4	The AMF receives the Deregistration Response from the UE and stops the T3522 timer.

T3550 Call Flow

This section describes the T3550 call flow.

Figure 56: T3550 Timer Call Flow

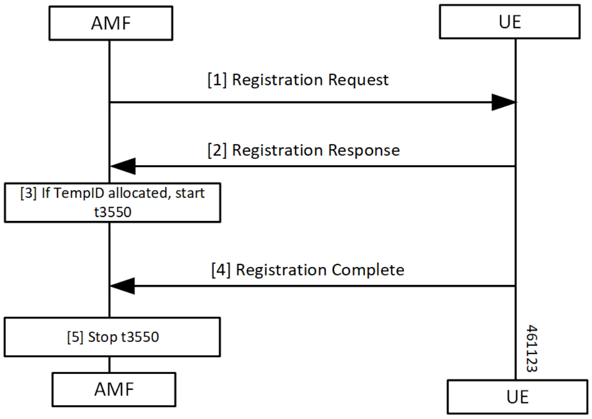

AMF
UE
[1] Registration Request
[2] Registration Response
[3] If TempID allocated, start t3550
[4] Registration Complete
[5] Stop t3550
AMF
UE
461123

Table 114: T3550 Timer Call Flow Description

Step	Description
1, 2	The AMF sends the Deregistration Request to the UE and receives the response.
3	The AMF starts the timer T3550 when temporary ID is allocated.
4, 5	AMF receives Deregistration Response from the UE and stops the T3550 timer.

T3555 Call Flow

This section describes the T3555 call flow.

Figure 57: T3555 Timer Call Flow

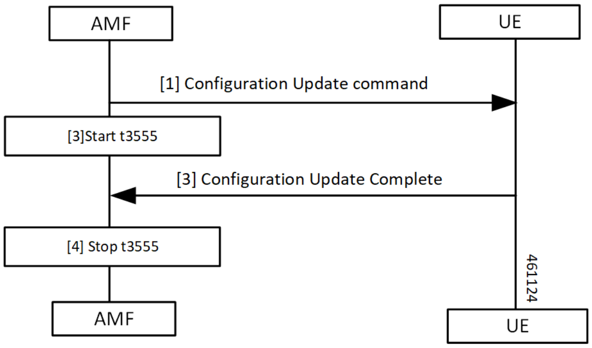

AMF
UE
[1] Configuration Update command
[3]Start t3555
[3] Configuration Update Complete
[4] Stop t3555
461124
AMF
UE

Table 115: T3555 Timer Call Flow Description

Step	Description
1, 2	The AMF sends the Configuration Update Command to the UE and starts the T3555 timer.
3, 4	The AMF receives the Configuration Update Complete from the UE and stops the T3555 timer.

T3560 Call Flow

This section describes the T3560 timer call flow.

Figure 58: T3560 Call Flow

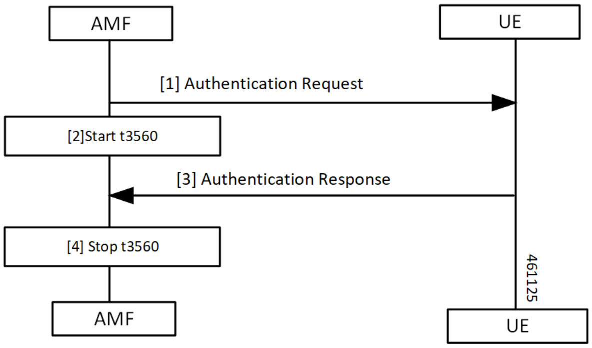


Table 116: T3560 Timer Call Flow Description

Step	Description
1, 2	The AMF sends the Authentication Request to the UE and starts the T3560 timer.
3, 4	The AMF receives the Authentication Response from the UE and stops the T3560 timer.

T3570 Call Flow

This section describes the T3570 timer call flow.

Figure 59: T3570 Call Flow

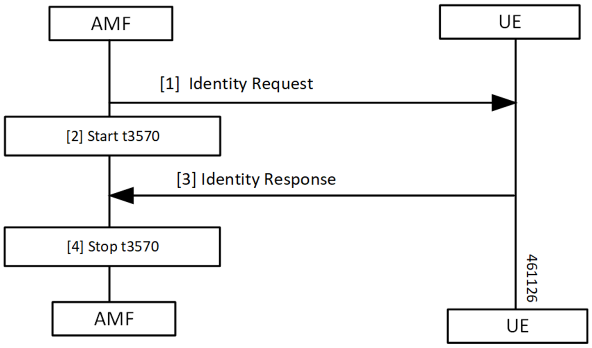


Table 117: T3570 Timer Call Flow Description

Step	Description
1, 2	The AMF sends the Identity Request to the UE and starts the T3570 timer.
3, 4	The AMF receives the Identity Response from the UE and stops the T3570 timer.

Feature Configuration

To configure this feature, use the following configuration:

```
config
 amf-global
   call-control-policy policy_name
    timers timer_type { retry retry_count | value timeout_value }
    end
```

NOTES:

- **timers** *timer_type* **retry** *retry_count*—Specify the retry count.
- **timers** *timer_type* **value** *timeout_value*—Specify the timeout value.

  For the timer_type, refer to the following table.

Table 118: 3GPP Timers and Values

Timer	Retry Count	Timeout Value
tidt	Not Applicable	Must be an integer in the range of 0–35712000 seconds. The default value is 3480 seconds.
ho-supervisory	Not Applicable	Must be an integer in the range of 100–10000 mill seconds. The default value is 500 milliseconds.

Timer	Retry Count	Timeout Value
tpurge	Not Applicable	Must be an integer in the range of 0–35712000 seconds. The default value is 86400.
t3502	Not Applicable	Must be an integer in the range of 0–35712000 seconds. The default value is 720 seconds.
t3512	Not Applicable	Must be an integer in the range of 0–35712000 seconds. The default value is 3240 seconds.
t3513	Must be an integer in the range of 1–5. The default value is 2.	Must be an integer in the range of 1–10 seconds. The default value is 5 seconds.
t3522	Must be an integer in the range of 0–5. The default value is 4.	Must be an integer in the range of 0–30 seconds. The default value is 6 seconds.
t3550	Must be an integer in the range of 0–5. The default value is 4.	Must be an integer in the range of 0–30 seconds. The default value is 6 seconds.
t3555	Must be an integer in the range of 0–5. The default value is 4.	Must be an integer in the range of 0–30 seconds. The default value is 6 seconds.
t3560	Must be an integer in the range of 0–5. The default value is 4.	Must be an integer in the range of 0–30 seconds. The default value is 6 seconds.
t3570	Must be an integer in the range of 0–5. The default value is 4.	Must be an integer in the range of 0–30 seconds. The default value is 6 seconds.

CHAPTER 32

SMF Feature Updates without SMF IEs

Feature Summary and Revision History

Summary Data

Table 119: Summary Data

Applicable Products or Functional Area	AMF
Applicable Platforms	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 120: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

When the gNB fails to send the PDU-x-Release (**pdu-rsc-rel**) information elements (IE), the AMF shows a distinct customary behavior.

This AMF behaviour is specific to:

- The UE context release procedure
- The UE context release request message and the UE context release complete message—Both messages not having the specified information elements

By default, this feature is disabled (false).

When the configuration is enabled, the AMF sends the required updates to SMF, even when the gNB doesn't send these information elements.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy ccp_name
         policy context-release force-smf-update { false | true }
         end
```

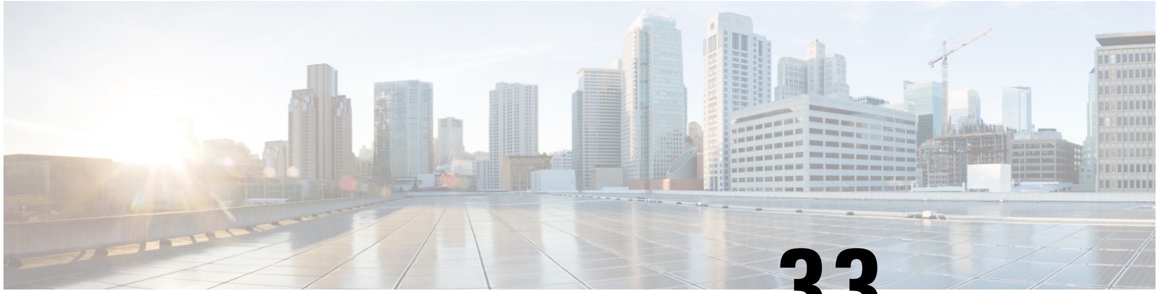
NOTES:

- **call-control-policy** *ccp_name*—Specify the UE-specific name for the call control policy.
- **context-release**—Configure the UE context release procedure as per the console.
- **force-smf-update { false | true }**—Initiate the SMF update procedure, when the PDU list isn’t available in release messages, as a part of the UE Context Release procedure. The default value is disabled (false).

Configuration Example

The following is an example configuration.

```
config
    amf-global
        call-control-policy pdu-rsc-rel
            policy context-release force-smf-update true
            end
```



CHAPTER 33

S-NSSAI based SMF Selection

Feature Summary and Revision History

Summary Data

Table 121: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 122: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

For Custom Slice selection without NSSF, AMF now supports SMF selection based on S-NSSAIs received from UE (Requested S-NSSAI) during PDU session establishment procedures.

AMF supports SNNSAI-based SMF selection only using NRF (Network Repository Function).

During PDU session establishment procedure, AMF queries the necessary NRF serving PLMN by issuing the Nnrf_NFDiscovery_Request including SNSSAI to select SMF.

The NRF serving PLMN provides a set of the discovered SMF instances or Endpoint Addresses of SMF service instance(s) in Nnrf_NFDiscovery_Request response message. AMF uses the information provided by NRF and connects to the necessary SMF for further interactions.

Feature Configuration

To configure this feature, use the following configuration:

```
config
 profile
  network-element network_element network_element_name
   nf-client-profile nf_client_profile_name
   query-params query_params
   end
```

NOTES:

- **network-element** *network_element network_element_name*—Specify the peer network element and its name.
- **nf-client-profile** *nf_client_profile_name*—Specify the NF client profile name.
- **query-params** *query_params*—Specify the query parameter for NF discovery.

Configuration Example

The following is an example configuration.

```
config
 profile
  network-element smf SMF1
   nf-client-profile SMF1
   query-params [ snssais ]
   end
```

Configuration Verification

To verify the configuration:

```
show running-config profile network-element
Wed Oct  20 07:22:45.870 UTC+00:00
profile network-element smf SMF1
nf-client-profile SMF1
query-params [ snssais ]
```

CHAPTER 34

Subscription Concealed Identifier Profile

Feature Summary and Revision History

Summary Data

Table 123: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 124: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

Subscription Concealed Identifier (SUCI) is a privacy-preserving identifier that contains the SUPI in a concealed method.

SUCI consists of the SUPI, Routing Indicator (RI), Protection Scheme Identifier, Home Network Public Key Identifier, and Scheme Output. The AMF derives the SUPI when all the other parameters besides the SUPI are decrypted during the Registration Request sent from the UE to the AMF.

Note The AMF can derive the SUPI value from SUCI only when the null-scheme is supported.

The AMF derives RI to enable routing of the network signaling with SUCI to AUSF. If the service provider has configured the SUCI profile, then RI is used for the AUSF and the UDM discovery.

Note AMF supports only the IMSI type SUPI.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   profile network-element { ausf | udm }
      query-params [ routing-indicator ]
      end
```

NOTES:

- **profile network-element { ausf | udm }**—Configure the peer network element configuration.
- **query-params [routing-indicator]**—Configure the query parameters for the network element's discovery. The network element specified in the previous step is considered for the discovery.

Configuration Example

The following is an example configuration.

```
config
   profile network-element ausf
       query-params routing-indicator
       exit
    profile network-element udm
       query-params routing-indicator
       end
```

CHAPTER 35

TLS Transport

Feature Summary and Revision History

Summary Data

Table 125: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 126: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF supports HTTP2 over a TLS secure channel for all SBA interfaces towards NRF, NSSF, AUSF, UDM, PCF, SMF, and so on.

This feature supports the server and client certificate management. It stores the certificates as k8 secrets.

Note You must generate and configure ca-certificates, and certificates for the server and client.

Feature Configuration

Configuring this feature involves the following steps:

- Client Certificates Configuration - This configuration provides the commands to configure the client certificates. For more information, refer to Configuring the Client Certificates, on page 220.
- Server Certificates configuration - This configuration provides the commands to configure the server certificates. For more information, refer to Configuring the Server Certificates, on page 220.
- TLS Enable Configuration - This configuration enables the TLS. For more information, refer to Enabling the TLS, on page 221.

Configuring the Client Certificates

To configure the Client certificates, use the following configuration:

```
config
  nf-tls ca-certificates certificate_name
   cert-data certificate_data
   end
```

NOTES:

- **ca-certificates** *certificate_name*—Specify the certificate name and data.
- **cert-data** *certificate_data*—Specify the certificate data in PEM format.

Configuring the Server Certificates

To configure the Server certificates, use the following configuration:

```
config
  nf-tls certificates certificate_name
   cert-data certificate_data
   private-key private_key_data
   end
```

NOTES:

- **nf-tls certificates** *certificate_name*—Specify the certificate name, data, and key.
- **cert-data** *certificate_data*—Specify the certificate data in PEM format.
- **private-key** *private_key_data*—Specify the certificate private key in PEM format.

Enabling the TLS

To configure the TLS enable, use the following configuration:

```
config
 instance instance-id instance_id
  endpoint sbi
   uri-scheme { http | https }
   certificate-name certificate_name
   end
```

NOTES:

- **instance instance-id** *instance_id*—Specify the instance ID.
- **endpoint sbi**—Specify the endpoint as sbi.
- **uri-scheme { http | https }**—Specify the uri scheme either http or https.
- **certificate-name** *certificate_name*—Specify the certificate name.

Configuration Verification

To verify the configuration:

```
show running-config instance instance-id 1 endpoint
instance instance-id 1
endpoint sbi
replicas     2
loopbackPort 8091
instancetype IPv4
vip-ip 1.1.1.0 vip-port 1000
exit
endpoint sctp
replicas 2
nodes    2
vip-ipv6 1000:1003::10:100 vip-ipv6-port 1001
exit
endpoint nodemgr
replicas 1
```

```
show nf-tls certificate-status days
CERTIFICATE NAME POD INSTANCE DAYS
--------------------------------------------
octrel-amf-server amf-amf-rest-ep-0 3632
octrel-lfs-server amf-amf-rest-ep-0 3632
```

Troubleshooting Information

This section describes troubleshooting information for this feature.

Trouble Ticket Data Collection

To debug the content data collection issues, use the following commands.

If the commands don’t assist you in resolving the issue, analyze the diagnostic data that is available in the form of logs.

- **helm list -n** *namespace*
- **kubectl get pods -n** *namespace*
- **kubectl get pod -o yaml -n** *namespace*
- **kubectl get pod -o yaml -n** *namespace pod_name*

CHAPTER 36

VoNR Support

Feature Summary and Revision History

Summary Data

Table 127: Summary Data

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

Revision History

Table 128: Revision History

Revision Details	**Release**
First introduced.	2021.04.0

Feature Description

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

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

Multiple PDU Sessions for VoNR

Feature Description

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

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

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

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

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

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Initial/Mobility Registration - IMS VoNR Support Procedure Call Flow

This section describes the Initial/Mobility Registration - IMS VoNR Support procedure call flow.

Figure 60: Initial/Mobility Registration - IMS VoNR Support Procedure Call Flow

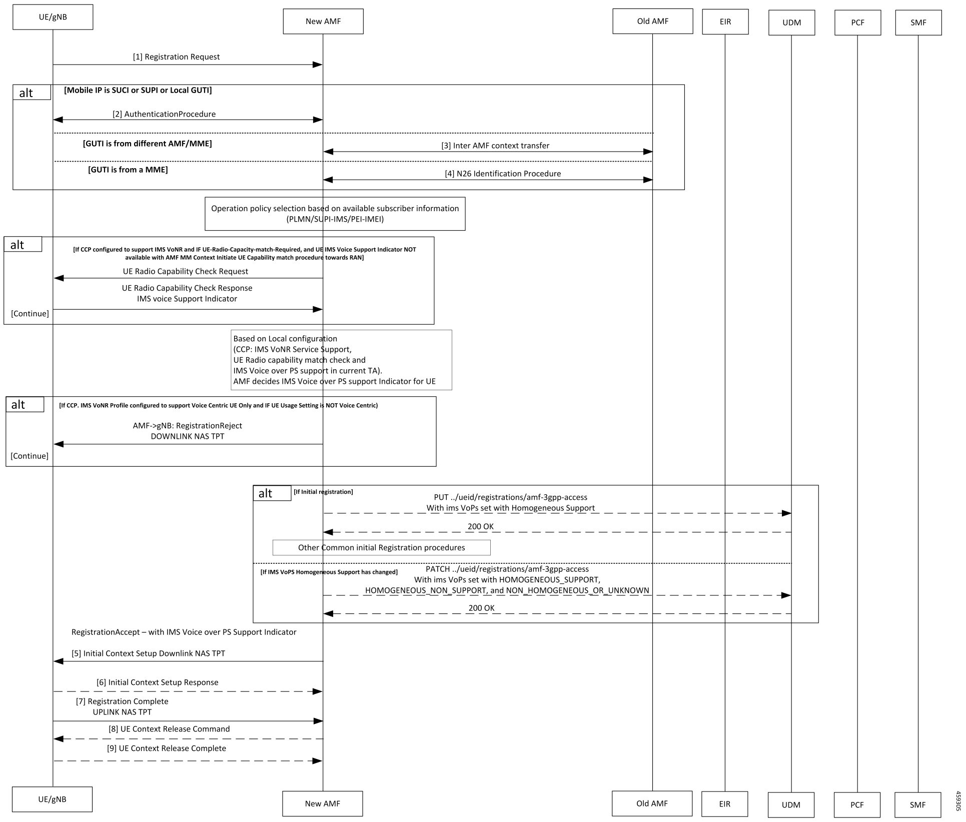

UE/gNB
New AMF
Old AMF
EIR
UDM
PCF
SMF
[1] Registration Request
alt
[Mobile IP is SUCI or SUPI or Local GUTI]
[2] AuthenticationProcedure
[GUTI is from different AMF/MME]
[3] Inter AMF context transfer
[GUTI is from a MME]
[4] N26 Identification Procedure
Operation policy selection based on available subscriber information (PLMN/SUPI-IMS/PEI-IMEI)
alt
[If CCP configured to support IMS VoNR and IF UE-Radio-Capacity-match-Required, and UE IMS Voice Support Indicator NOT available with AMF MM Context Initiate UE Capability match procedure towards RAN]
UE Radio Capability Check Request
UE Radio Capability Check Response
IMS voice Support Indicator
[Continue]
Based on Local configuration
(CCP: IMS VoNR Service Support,
UE Radio capability match check and
IMS Voice over PS support in current TA).
AMF decides IMS Voice over PS support Indicator for UE
alt
[If CCP. IMS VoNR Profile configured to support Voice Centric UE Only and IF UE Usage Setting is NOT Voice Centric]
AMF->gNB: RegistrationReject
DOWNLINK NAS TPT
[Continue]
alt
[If Initial registration]
PUT ../ueid/registrations/amf-3gpp-access
With ims VoPs set with Homogeneous Support
200 OK
Other Common initial Registration procedures
[If IMS VoPS Homogeneous Support has changed]
PATCH ../ueid/registrations/amf-3gpp-access
With ims VoPs set with HOMOGENEOUS_SUPPORT,
HOMOGENEOUS_NON_SUPPORT, and NON_HOMOGENEOUS_OR_UNKNOWN
200 OK
RegistrationAccept – with IMS Voice over PS Support Indicator
[5] Initial Context Setup Downlink NAS TPT
[6] Initial Context Setup Response
[7] Registration Complete
UPLINK NAS TPT
[8] UE Context Release Command
[9] UE Context Release Complete
UE/gNB
New AMF
Old AMF
EIR
UDM
PCF
SMF
459305

Table 129: Initial/Mobility Registration - IMS VoNR Support Procedure Call Flow Description

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

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

Provide UE Information for Terminating Domain Selection Call Flow

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

Figure 61: Provide UE Information for Terminating Domain Selection Call Flow

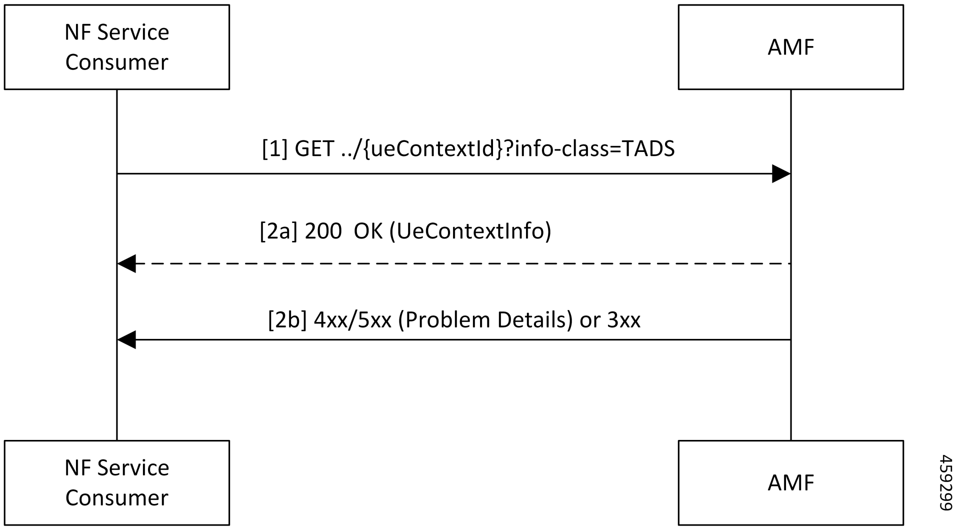

NF Service Consumer
AMF
[1] GET ../{ueContextId}?info-class=TADS
[2a] 200 OK (UeContextInfo)
[2b] 4xx/5xx (Problem Details) or 3xx
NF Service Consumer
AMF
459299

Table 130: Provide UE Information for Terminating Domain Selection Call Flow Description

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

Limitations

This feature has the following limitations in this release:

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

Feature Configuration

Configuring this feature involves the following steps:

1. Enable AMF to indicate if the UE is capable to handle IMS Voice over Packet-Switched (VoPS) sessions. For more information, refer to Configuring Support to Indicate IMS VoPS Support, on page 228.
2. Configure IMS VoPS service for the configured TALs. For more information, refer to Configuring the TAL-level IMS VoPS, on page 228.

Configuring Support to Indicate IMS VoPS Support

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

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

NOTES:

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

Configuring the TAL-level IMS VoPS

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

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

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

NOTES:

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

OAM Support

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

Statistics

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

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

PDN Creation, Modification, and Release

Feature Description

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

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

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

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

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

SM Context Update Call Flow

This section describes the SM Context Update call flow.

Figure 62: SM Context Update Call Flow

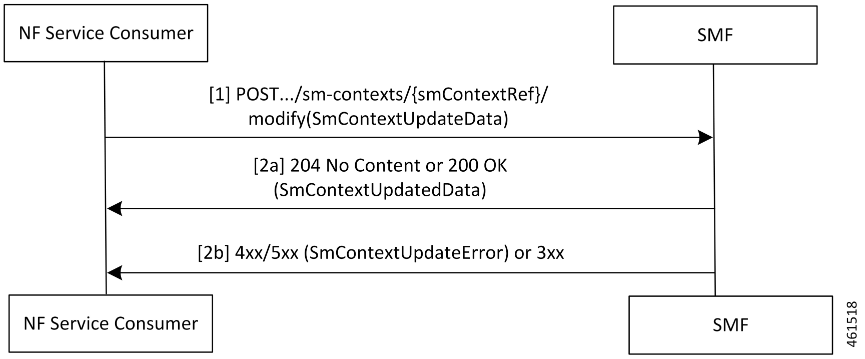

NF Service Consumer
SMF
[1] POST.../sm-contexts/{smContextRef}/
modify(SmContextUpdateData)
[2a] 204 No Content or 200 OK
(SmContextUpdatedData)
[2b] 4xx/5xx (SmContextUpdateError) or 3xx
NF Service Consumer
SMF
461518

Table 131: SM Context Update Call Flow Description

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

Feature Configuration

Configuring this feature involves the following steps:

1. Configure the UDM initiated PCSF restoration procedure at AMF. For more information, refer to Configuring the PCSF Restoration Feature, on page 231.

2. Configure the IMS for identifying the PDU session with DNN name. For more information, refer to Configuring the IMS for DNN, on page 231.
3. Configure the query selection parameter to select the SMF instance that supports SMF and PGW-C. For more information, refer to Configuring the Query Selection Parameter, on page 231.

Configuring the PCSF Restoration Feature

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

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

NOTES:

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

Configuring the IMS for DNN

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

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

NOTES:

- **amf-name** *amf_name*—Specify AMF name.
- **network-element smf** *smf_instance*—Specify the NF instance name to establish the peer configuration.
- **dnn-policy** *policy_name*—Specify the DNN policy name.
- **ims-enabled { true | false }**—Enable or disable IMS for the configured DNN.

Configuring the Query Selection Parameter

To configure the query parameter, use the following configuration:

```
config
   profile
      network-element smf smf_instance
```

```
query-params [ pgwind ]
end
```

NOTES:

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

CHAPTER 37

Xn Handover

Feature Summary and Revision History

Summary Data

Table 132: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 133: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

AMF now supports Xn Handover. In Xn Handover, the source and destination gNBs are interconnected. The gNB communicates with each other to complete some aspects of the handover and the destination gNB sends a path switch request. The path switch request contains the source UE AMF NGAP ID used by the AMF to search the UE which is being handed over.

Supported Scenarios

Path switch request is supported for:

- Single PDU resource
- Multiple PDU resources
- Multiple, with some failed to handover at the target gNB
- Multiple, with some failing at the SMF
- Requests timing out at the SMF
- Expiry of guard timer
- Error conditions at the SMF: handling of the error and sending the right errors so that resources are cleared at the UE
- Error condition at the AMF: If invalid Session ID comes in Path Switch Request Ack, in either ToBeSwithched or FailedToSetup, AMF sends Path Switch Request Failure with Unknown Session ID as the cause.
- If SMF rejects all PDUs, then AMF sends Path Switch Request Failure with cause as HO-Failure-in-target-5GC-ngran-node-or-target-system.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Xn Handover Call Flow

This section describes Xn Handover call flow.

Figure 63: Xn Handover Call Flow

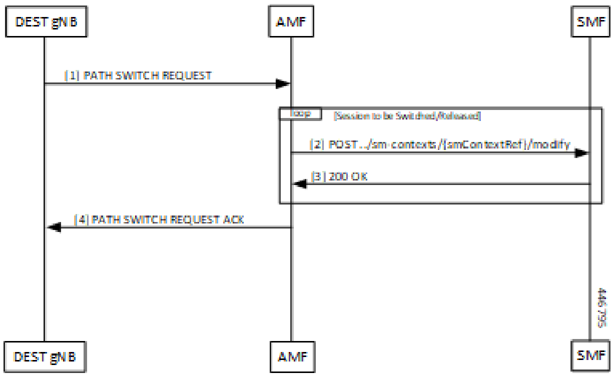

DEST gNB
AMF
SMF
[1] PATH SWITCH REQUEST
loop
[Session to be Switched/Released]
[2] POST../sm-contexts/{smContextRef}/modify
[3] 200 OK
[4] PATH SWITCH REQUEST ACK
446795
DEST gNB
AMF
SMF

Table 134: Xn Handover Call Flow Description

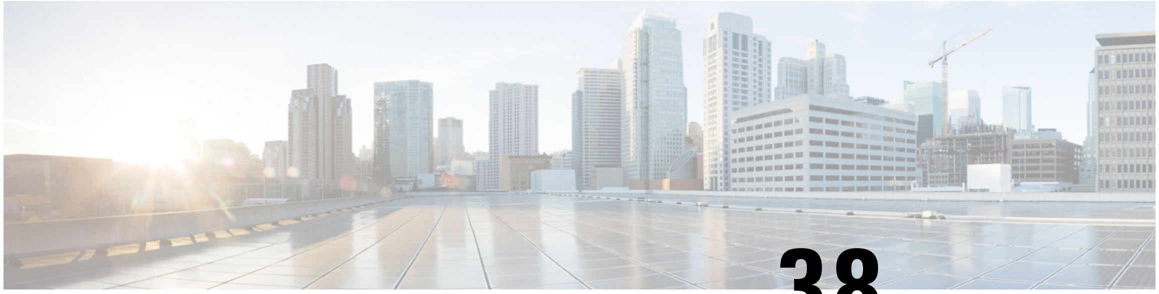
Step	Description
1	Once signaling that involves the UE, source and destination gNB have taken the decision to handover, the destination gNB constructs a PATH SWITCH REQUEST with the list of PDU sessions that have successfully switched and the list of PDU sessions that were not successful.
2	For each of the PDU Sessions, the AMF constructs a SmContext Modify request and sends it to the corresponding SMF to update the tunnel endpoint ID for the gNB.
3	The SMF responds with either 200 OK or an appropriate cause code.
4	The AMF creates a PATH SWITCH REQUEST ACKNOWLEDGEMENT including PDU sessions that are successful in a success list and the PDU sessions that have failed in a failure list and sends them to the destination gNB. The AMF clears the source gNB context and attaches the destination gNB context to the UE context.

OAM Support

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

Bulk Statistics Support

- Support for message level statistics for PATH SWITCH REQUEST and PATH SWITCH REQUEST ACKNOWLEDGEMENT, on a per peer gNB basis.
- Support for procedure level statistics for Xn Handover, with Attempted, Success and Failure.



CHAPTER 38

AMF Troubleshooting

show subscriber

This section describes the **show subscriber** commands for the existing subscribers sessions.

Table 135: show subscriber Command Output Description

Field	Description
|	Output modifiers.
all	Displays all the existing subscriber sessions.
supi	Displays subscriber sessions based on SUPI ID.
gnodeb-id	Displays the gnodeb-id of the session.

clear subscriber

This section describes the **clear subscriber** commands for the existing subscribers sessions.

Table 136: clear subscriber Command Output Description

Field	Description
|	Output modifiers.
all	Clears all the subscriber sessions.
gnodeb-id	Clears the sessions that have the specified gnodeb-id.
supi	Clears the sessions based on the SUPI value.

CHAPTER 39

Sample AMF Configuration

Sample Configuration

Use **show** command to view the sample configuration that is provided only for reference. You must create and modify your own configuration file according to the specific needs of your deployment.

```
show running-config | nomore
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
group nrf discovery NRFDISCOVERY
 service type nrf nnrf-disc
  endpoint-profile
   name       ep1
   uri-scheme http
   version
    uri-version v1
     full-version 1.1.1.[1]
    exit
   exit
   endpoint-name en1
    priority 56
    primary ip-address ipv4 172.16.186.13
    primary ip-address port 8095
   exit
  exit
 exit
exit
group nrf mgmt MGMT
 service type nrf nnrf-nfm
  endpoint-profile
   name       mgmt-prof
   uri-scheme http
   endpoint-name mgmt-1
    primary ip-address ipv4 172.16.186.13
    primary ip-address port 8095
   exit
  exit
 exit
exit
amf-global
 amf-name AMF1
```

```
call-control-policy CCP1
 disable-init-csr-reg false
 am-policy skip false
 default-slice name n26 sst 1 sdt 000000
 timers t3560 value 10
 timers t3560 retry 3
 timers t3550 value 5
 timers t3550 retry 3
 timers t3570 value 5
 timers t3570 retry 3
 timers t3522 value 5
 timers t3522 retry 3
 timers tidt value 3480
 timers tguard value 30
 timers tpurge value 0
 timers t3502 value 60
 timers t3512 value 3240
 timers ho-supervisory value 500
 tai-group            VoPS_tailist
 policy context-release force-smf-update true
 feature-support-ie ims-vops-service-3gpp supported true
 feature-support-ie pcscf-restoration-supported true
 feature-support-ie iwk-n26-supported
 feature-support-ie redirection-eps-fallback supported
 security-algo 1 ciphering-algo 5G-EA0
 security-algo 1 integity-prot-algo 5G-IA0
 security-algo 2 ciphering-algo 128-5G-EA1
 security-algo 2 integity-prot-algo 128-5G-IA1
 security-algo 3 ciphering-algo 128-5G-EA2
 security-algo 3 integity-prot-algo 128-5G-IA2
 paging-priority map arp 5 ngap-paging-priority 0
 paging-priority map arp 8 ngap-paging-priority 2
exit
dnn-policy Spectrum-Mobile
 network-element-profile-list smf SMF1
exit
dnn-policy emergency
 network-element-profile-list smf SMF1
exit
dnn-policy ims
 ims-enabled true
 network-element-profile-list smf SMF1
exit
dnn-policy internet
 network-element-profile-list smf SMF1
exit
dnn-policy intershat
 network-element-profile-list smf SMF1
exit
dnn-policy starent
 network-element-profile-list smf SMF1
exit
dnn-policy starent.com
 network-element-profile-list smf SMF1
exit
operator-policy OPR-POLICY-1
 ccp-name        CCP1
 paging-map-name pm1
 network-element-profile-list ausf AUSF1
 network-element-profile-list smf SMF1
 network-element-profile-list pcf PCF1
 network-element-profile-list udm UDM1
 network-element-profile-list amf AMF2
 network-element-profile-list nssf NSSF1
```

```
exit
supi-policy 001
 operator-policy-name OPR-POLICY-1
exit
supi-policy 314
 operator-policy-name OPR-POLICY-1
exit
paging-map pm1
 precedence 1
  trigger-type        arp
  arp-value           5
  paging-profile-name pp4
 exit
 precedence 2
  trigger-type        arp
  arp-value           8
  paging-profile-name pp4
 exit
 precedence 3
  trigger-type        dereg
  dereg-value         udm_init
  paging-profile-name pp4
 exit
 precedence 4
  trigger-type        ppi
  ppi-value           7
  paging-profile-name pp1
 exit
 precedence 5
  trigger-type        5qi
  fiveqi-value        5
  paging-profile-name pp4
 exit
 precedence 6
  trigger-type        dereg
  dereg-value         amf_init
  paging-profile-name pp4
 exit
 precedence 7
  trigger-type        ppi
  ppi-value           6
  paging-profile-name pp5
 exit
 precedence 9
  trigger-type        dnn
  dnn-value           Spectrum-Mobile
  paging-profile-name pp4
 exit
exit
paging-profile pm1
exit
paging-profile pp1
 paging-stage 1
  paging-algo pa1
 exit
exit
paging-profile pp2
 paging-stage 1
  paging-algo pa2
 exit
exit
paging-profile pp3
 paging-stage 2
  paging-algo pa4
 exit
 paging-stage 3
  paging-algo pa1
 exit
 paging-stage 4
  paging-algo pa2
 exit
 paging-stage 5
  paging-algo pa3
 exit
exit
paging-profile pp4
 paging-stage 1
  paging-algo pa1
 exit
 paging-stage 2
  paging-algo pa2
 exit
 paging-stage 3
  paging-algo pa3
 exit
 paging-stage 4
  paging-algo pa6
 exit
 paging-stage 5
  paging-algo pa4
 exit
exit
paging-profile pp5
 paging-stage 5
  paging-algo pa5
 exit
exit
paging-algo pa1
 action               last_gnb_last_tai
 max-n-gnb            3
 t3513-timeout        2
 max-paging-attempts 1
exit
paging-algo pa2
 action               last_n_gnb_last_tai
 max-n-gnb            3
 t3513-timeout        3
 max-paging-attempts 2
exit
paging-algo pa3
 action               all_gnb_last_tai
 max-n-gnb            5
 t3513-timeout        4
 max-paging-attempts 3
exit
paging-algo pa4
 action               all_gnb_all_tai
 max-n-gnb            5
 t3513-timeout        5
 max-paging-attempts 5
exit
paging-algo pa5
 action               all_gnb_all_tai
 max-n-gnb            5
 t3513-timeout        10
 max-paging-attempts 5
exit
paging-algo pa6
```

```
  action              all_gnb_remaining_tai_seq
  max-n-gnb           5
  t3513-timeout       5
  max-paging-attempts 1
 exit
exit
profile network-element amf AMF2
 nf-client-profile        AMF2
 failure-handling-profile FH1
 query-params [ target-plmn ]
exit
profile network-element pcf PCF1
 nf-client-profile        PP1
 failure-handling-profile FH1
exit
profile network-element udm UDM1
 nf-client-profile        UP1
 failure-handling-profile FH1
exit
profile network-element ausf AUSF1
 nf-client-profile        AUP1
 failure-handling-profile FH1
exit
profile network-element smf SMF1
 nf-client-profile SMF1
 query-params [ dnn ]
exit
profile network-element nssf NSSF1
 nf-client-profile NSSF1
exit
profile nf-client nf-type ausf
 ausf-profile AUP1
  locality LOC1
   priority 30
   service name type nausf-auth
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 172.16.186.13
      primary ip-address port 8047
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type udm
 udm-profile UP1
  locality LOC1
   service name type nudm-sdm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      primary ip-address ipv4 172.16.186.13
      primary ip-address port 9001
     exit
    exit
   exit
   service name type nudm-uecm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 172.16.186.13
      primary ip-address port 9001
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type pcf
 pcf-profile PP1
  locality LOC1
   priority 30
   service name type npcf-am-policy-control
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 172.16.186.13
      primary ip-address port 9082
     exit
     endpoint-name EP2
      priority 20
      primary ip-address ipv4 172.16.186.13
      primary ip-address port 9082
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type amf
 amf-profile AMF2
  locality LOC1
   priority 56
   service name type namf-comm
    endpoint-profile EP1
     capacity   30
     priority   30
     uri-scheme http
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 172.16.186.13
      primary ip-address port 9052
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type smf
 smf-profile SMF1
  locality LOC1
   priority 56
   service name type nsmf-pdusession
    endpoint-profile EP1
     capacity   30
     priority   30
     uri-scheme http
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 172.16.186.13
      primary ip-address port 9050
     exit
    exit
   exit
  exit
 exit
exit
profile nf-pair nf-type NRF
 nrf-discovery-group NRFDISCOVERY
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type UDM
 nrf-discovery-group NRFDISCOVERY
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation true
exit
profile nf-pair nf-type AMF
 nrf-discovery-group NRFDISCOVERY
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type SMF
 nrf-discovery-group NRFDISCOVERY
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation false
exit
profile nf-pair nf-type AUSF
 nrf-discovery-group NRFDISCOVERY
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation true
exit
profile nf-pair nf-type PCF
 nrf-discovery-group NRFDISCOVERY
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation true
exit
profile nf-pair nf-type NSSF
 nrf-discovery-group NRFDISCOVERY
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-client-failure nf-type udm
 profile failure-handling FH1
  service name type nudm-uecm
  exit
 exit
exit
profile nf-client-failure nf-type pcf
```

```
 profile failure-handling FH1
  service name type npcf-am-policy-control
   message type PcfAmfPolicyControlCreate
    status-code httpv2 201
     action continue
    exit
   exit
  exit
 exit
exit
amf-services AMF
 amf-name             AMF1
 validate-Tais        false
 locality             LOC1
 operator-policy-name OPR-POLICY-1
 peer-mme gummei mcc 311 mnc 480 group-id 32888 mme-code 36 address 172.16.171.13
 peer-mme gummei mcc 314 mnc 020 group-id 32777 mme-code 1 address 172.16.171.13
 peer-mme tai-match priority 1 mcc 311 mnc 480 tac 23 address 172.16.171.13
 peer-mme tai-match priority 1 mcc 314 mnc 020 tac 23 address 172.16.171.13
 pgw fqdn Spectrum-Mobile smf-network-element-profile SMF1
 guamis mcc 314 mnc 020 region-id 206 set-id 129 pointer 5
 tai-groups TAI-GRP1
 exit
 slices name SLICE1
  sst 3
  sdt 000000
 exit
 slices name SLICE2
  sst 1
  sdt 000000
 exit
exit
tai-group name TAI-GRP1
 tais name TAI-LIST-1
  mcc 314 mnc 020
   tac list [ 5431 5432 5433 ]
  exit
 exit
 tais name TAI-LIST-2
  mcc 314 mnc 020
   tac list [ 20 21 22 ]
  exit
 exit
 tais name TAI-LIST-3
  mcc 001 mnc 00
   tac list [ 20 30 40 ]
  exit
 exit
 tais name TAI-LIST-4
  mcc 314 mnc 020
   tac list [ 5440 5441 5442 5443 5444 5445 5446 ]
  exit
 exit
 tais name TAI-LIST-5
  mcc 314 mnc 020
   tac list [ 50 51 52 ]
  exit
 exit
exit
tai-group name TAI-GRP2
 tais name TAI-LIST-1
  mcc 314 mnc 020
   tac list [ 5434 5435 5436 ]
  exit
 exit
 tais name TAI-LIST-2
  mcc 314 mnc 020
   tac list [ 5437 5438 5439 5440 ]
  exit
 exit
 tais name TAI-LIST-3
  mcc 314 mnc 020
   tac list [ 40 41 42 43 44 ]
  exit
 exit
exit
tai-group name VoPS_tailist
 tais name tai-list1
  ims-voice-over-ps-supported true
  mcc 314 mnc 020
   tac list [ 1111 2222 3333 ]
  exit
 exit
exit
infra metrics verbose load-balancer
 level production
exit
client outbound host ping timeout 3000
client outbound host ping interval 5000
instance instance-id 1
 endpoint li
  replicas 1
  nodes    2
  vip-ip 172.16.171.4
  vip-ip 172.16.171.8
 exit
 endpoint sctp
  replicas 2
  nodes    2
  vip-ip 172.17.0.8 vip-port 1000
  vip-ipv6 2001:172:17::8 vip-ipv6-port 1000
 exit
 endpoint nodemgr
  replicas 1
  nodes    2
 exit
 endpoint gtp
  nodes 1
  retransmission timeout 2 max-retry 5
  vip-ip 172.16.171.8
 exit
 endpoint service
  replicas 2
  nodes    2
 exit
 endpoint protocol
  replicas 2
  nodes    2
  vip-ip 172.16.171.8
 exit
 endpoint ngap
  replicas 2
 exit
 endpoint sbi
  replicas     2
  loopbackPort 8091
  instancetype IPv4
  vip-ip 172.16.186.8 vip-port 8070
 exit
exit
logging level application error
logging level transaction error
logging level tracing error
logging name amf-protocol-ep.amf-app.nas level application error
logging name amf-protocol-ep.amf-app.nas level transaction error
logging name amf-rest-ep.amf-app.nrf level application error
logging name amf-service.amf-app.Config level application error
logging name amf-service.amf-app.Config level transaction error
logging name amf-service.amf-app.NwConfig level application error
logging name amf-service.amf-app.NwConfig level transaction error
logging name amf-service.amf-app.ausf level application error
logging name amf-service.amf-app.ausf level transaction error
logging name amf-service.amf-app.gen level application error
logging name amf-service.amf-app.gen level transaction error
logging name amf-service.amf-app.messageprocessor level application error
logging name amf-service.amf-app.messageprocessor level transaction error
logging name amf-service.amf-app.nas level application error
logging name amf-service.amf-app.nas level transaction error
logging name amf-service.amf-app.ngap level application error
logging name amf-service.amf-app.ngap level transaction error
logging name amf-service.amf-app.pcf level application error
logging name amf-service.amf-app.pcf level transaction error
logging name amf-service.amf-app.subs level application error
logging name amf-service.amf-app.subs level transaction error
logging name amf-service.amf-app.udm level application error
logging name amf-service.amf-app.udm level transaction error
logging name infra.cache_client.core
logging name infra.config.core
logging name infra.message_log.core
logging name infra.resource_monitor.core
logging name infra.sctp_server.core level application error
logging name infra.topology.core
deployment
 app-name               amf5
 cluster-name           clu005
 dc-name                sys005
 resource cpu 9000
 logical-nf-instance-id 5
exit
k8 label protocol-layer key smi.cisco.com/node-type-2 value protocol
exit
k8 label service-layer key smi.cisco.com/node-type-3 value service
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit
k8 label sctp-layer key smi.cisco.com/node-type-2 value protocol
exit
instances instance 1
 system-id  sys005
 cluster-id clu005
 slice-name 1
exit
local-instance instance 1
datastore notification-ep host 172.16.184.8
datastore notification-ep port 8012
datastore session-db endpoints datastore-ep-session.cdl-amf.svc.cluster.local
 port 8882
exit
system mode running
helm default-repository base-repos
helm repository base-repos
 url https://charts.171.11.189.31.nip.io/amf.2021.04.0.i112
```

```
exit
k8s name          amf-cndp-b19-3
k8s namespace     amf-ins5
k8s nf-name       amf
k8s registry      docker.171.11.189.31.nip.io/amf.2021.04.m0.i26
k8s single-node   false
k8s use-volume-claims true
k8s ingress-host-name 10.84.125.78.nip.io
k8s nodes amf-cndp-b19-3-master-1
 node-type   master
 worker-type master
exit
k8s nodes amf-cndp-b19-3-master-2
 node-type   master
 worker-type master
exit
k8s nodes amf-cndp-b19-3-master-3
 node-type   master
 worker-type master
exit
aaa authentication users user admin
 uid        1117
 gid        1117
 password   $1$iQJO2wld$7jGfAw6qA3j0mfXeSvk5e/
 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-amf
   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 ops-center-security
  group [ * ]
  rule change-self-password
   module-name       ops-center-security
   path              /smiuser/change-self-password
   access-operations exec
   action            permit
  exit
  rule smiuser
   module-name       ops-center-security
   path              /smiuser
   access-operations exec
   action            deny
  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-amf
   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-amf
   path              /clear/lawful-intercept
   access-operations *
   action            deny
  exit
 exit
```