Ultra Cloud Core 5G Access and Mobility Management Function, Release 2024.01 - Configuration and Administration Guide

First Published: 2024-01-31

Last Modified: 2024-04-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this Guide

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.

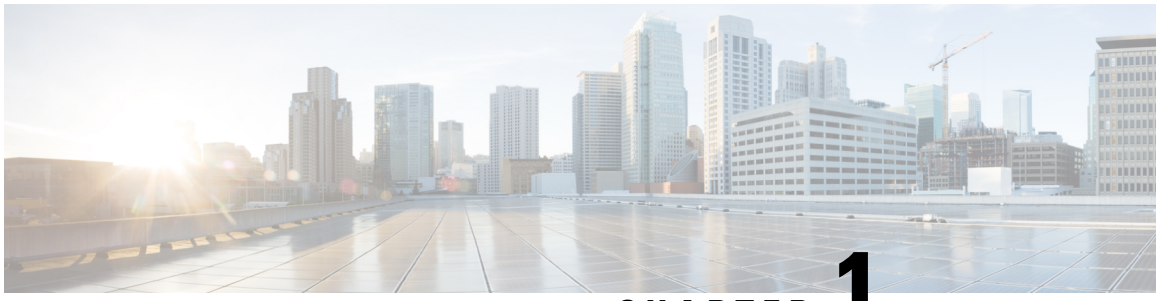
Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`

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

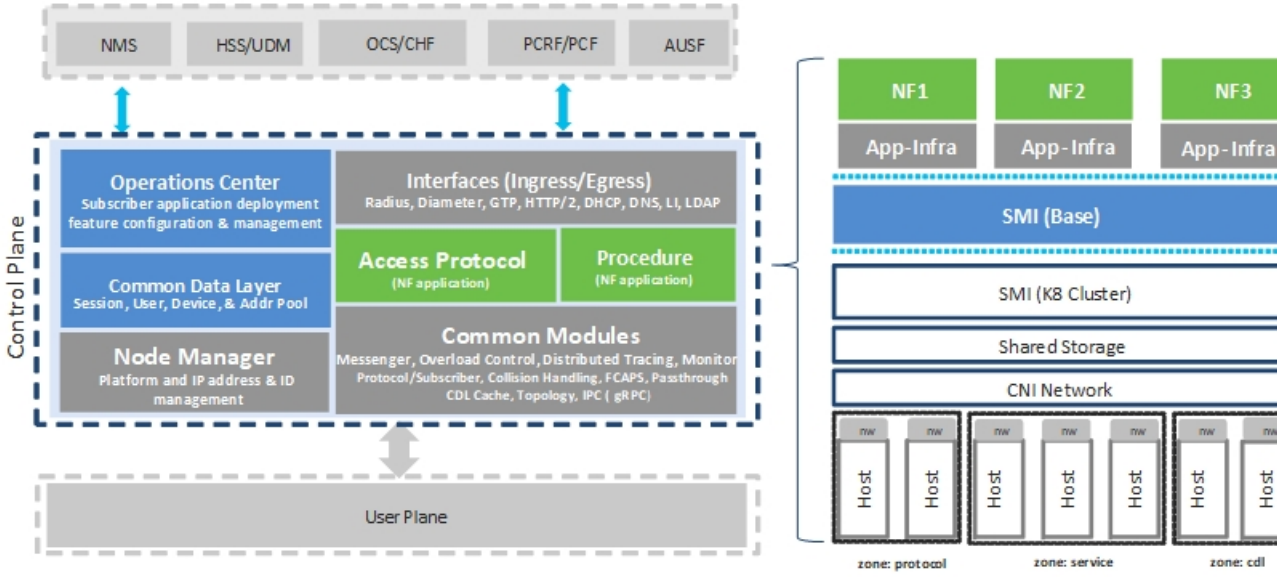
The CP-related NFs that comprise the Ultra Cloud Core are based on a common architecture that is designed around the following tenants:

- 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 control plane NFs are each designed as containerized applications (for example microservices) for deployment through the Subscriber Microservices Infrastructure (SMI).

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

Figure 1: Ultra Cloud Core CP Architectural Components



User Plane Network Function

The 5G UP NF within the Ultra Cloud Core is the User Plane Function (UPF). 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 4G CUPS architecture. This commonality ensures the delivery of a consistent set of capabilities between 4G and 5G such as:

- Ultrafast 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.

Subscriber Microservices Infrastructure Architecture

The Ultra Cloud Core (UCC) 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.

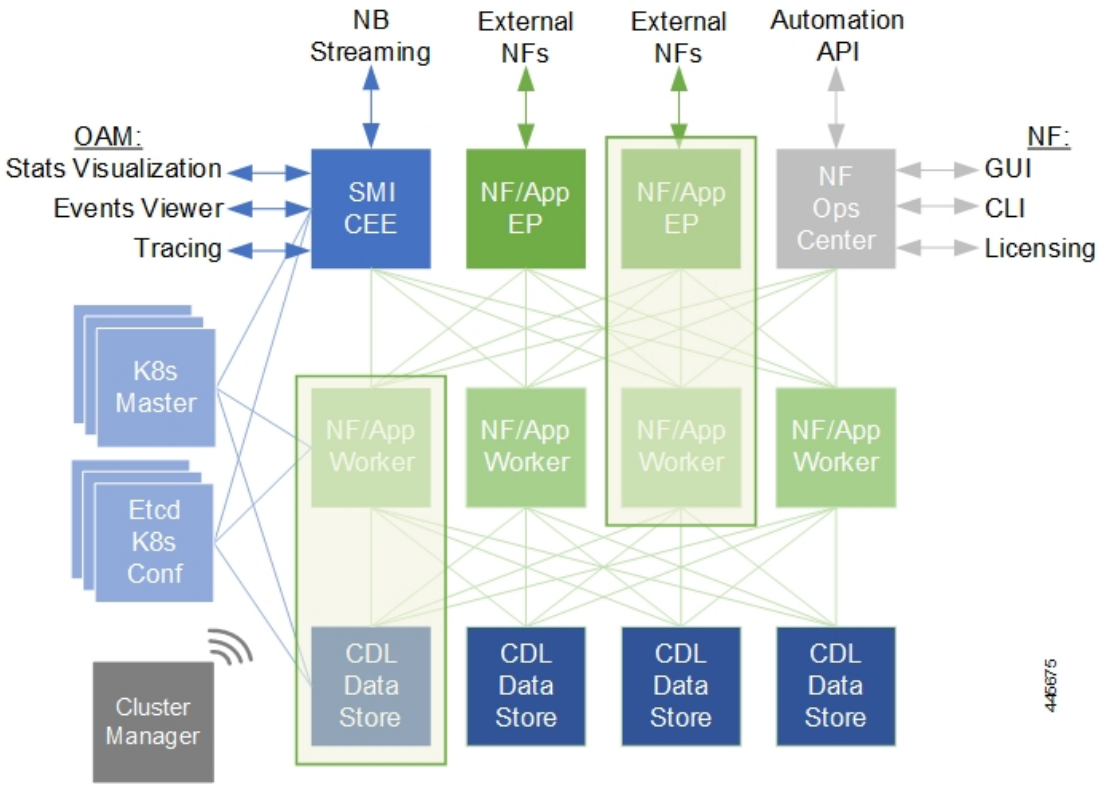
The SMI stack consists of the following:

- 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 primary and etcd functions, which provide LCM for the NF applications that are 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. Also, 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 high availability in local or geo-redundant deployments.
- Service Mesh—Provides sophisticated message routing between application containers, enabling managed interconnectivity, extra 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 or Application Worker Nodes—The containers that comprise an NF application pod.
- NF or Application Endpoints (EPs)—The NFs or applications and their 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 or application.

Figure 2: SMI Components



For more information on SMI components, see Ultra Cloud Core Subscriber Microservices Infrastructure and the related-documentation at *Deployment Guide* > *Overview* chapter.

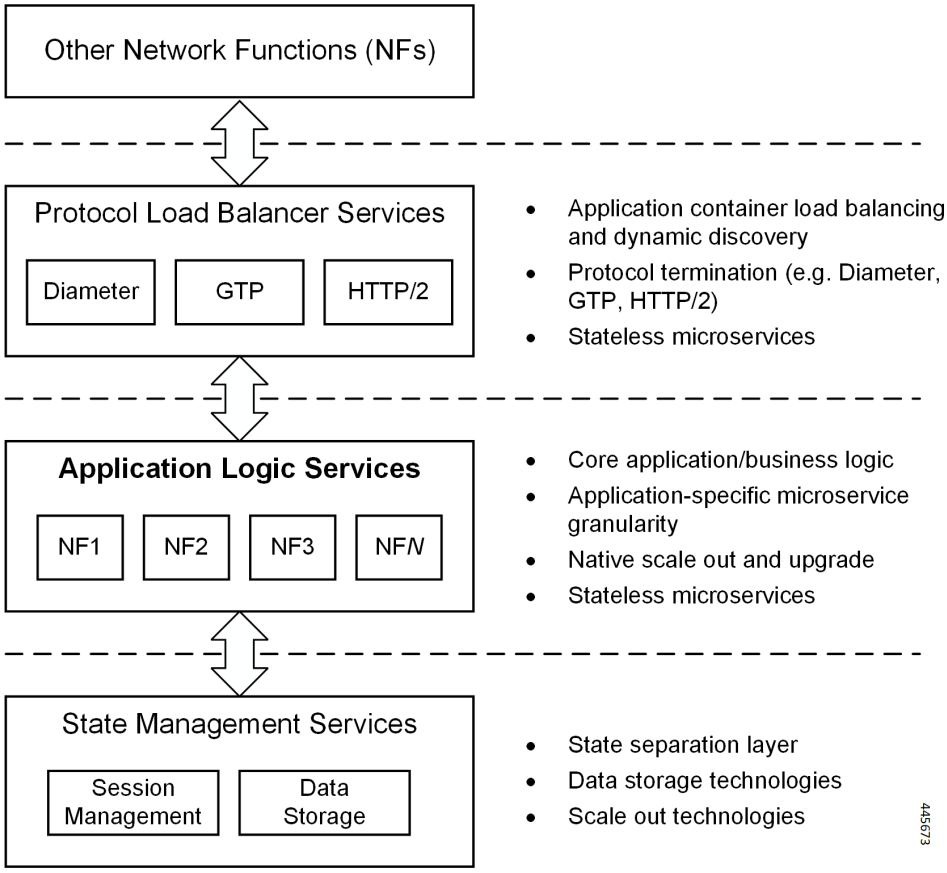
Control Plane Network Function Architecture

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

The architectural tiers are as follows:

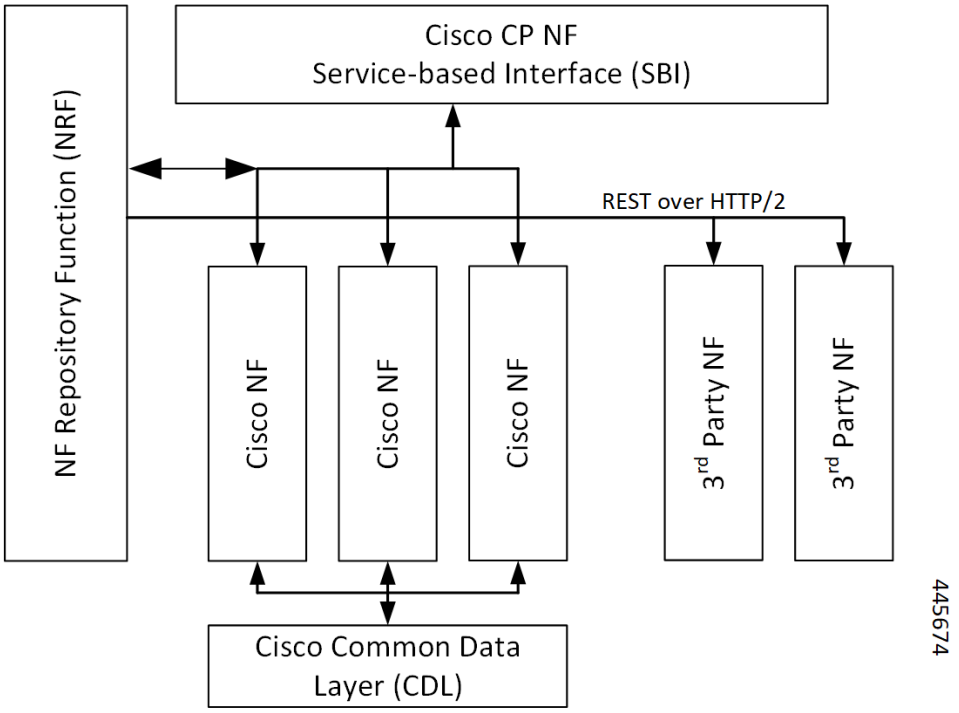
- Protocol Load Balancer Services—These are stateless microservices that are primarily responsible for dynamic discovery of application containers as well as for protocol proxy and termination. These include traditional 3GPP protocols and new protocols that are introduced with 5G.
- Applications Services—Responsible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

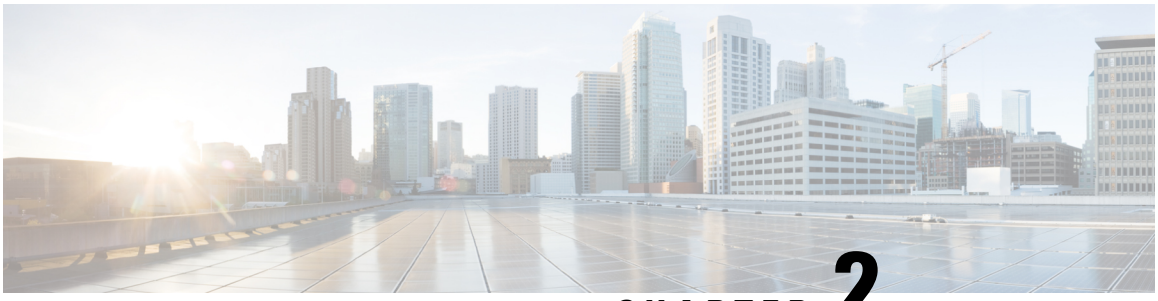


The three-tiered architecture on which Cisco CP NFs are designed fully support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

Figure 4: Cisco CP NF Service-based Architecture Support



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



CHAPTER 2

5G 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

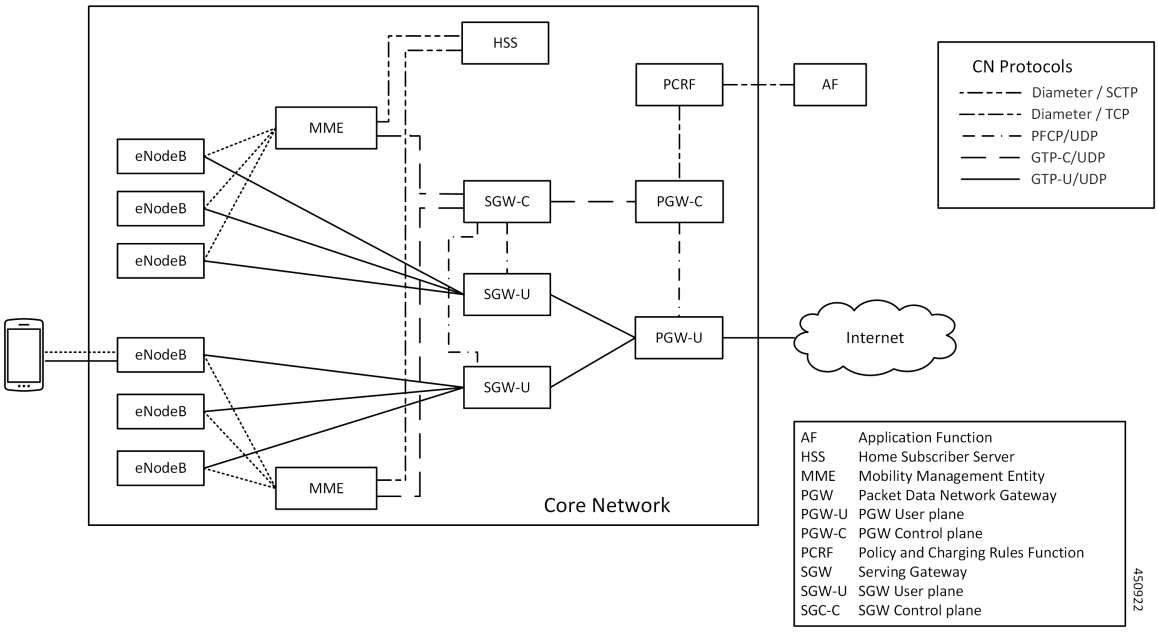
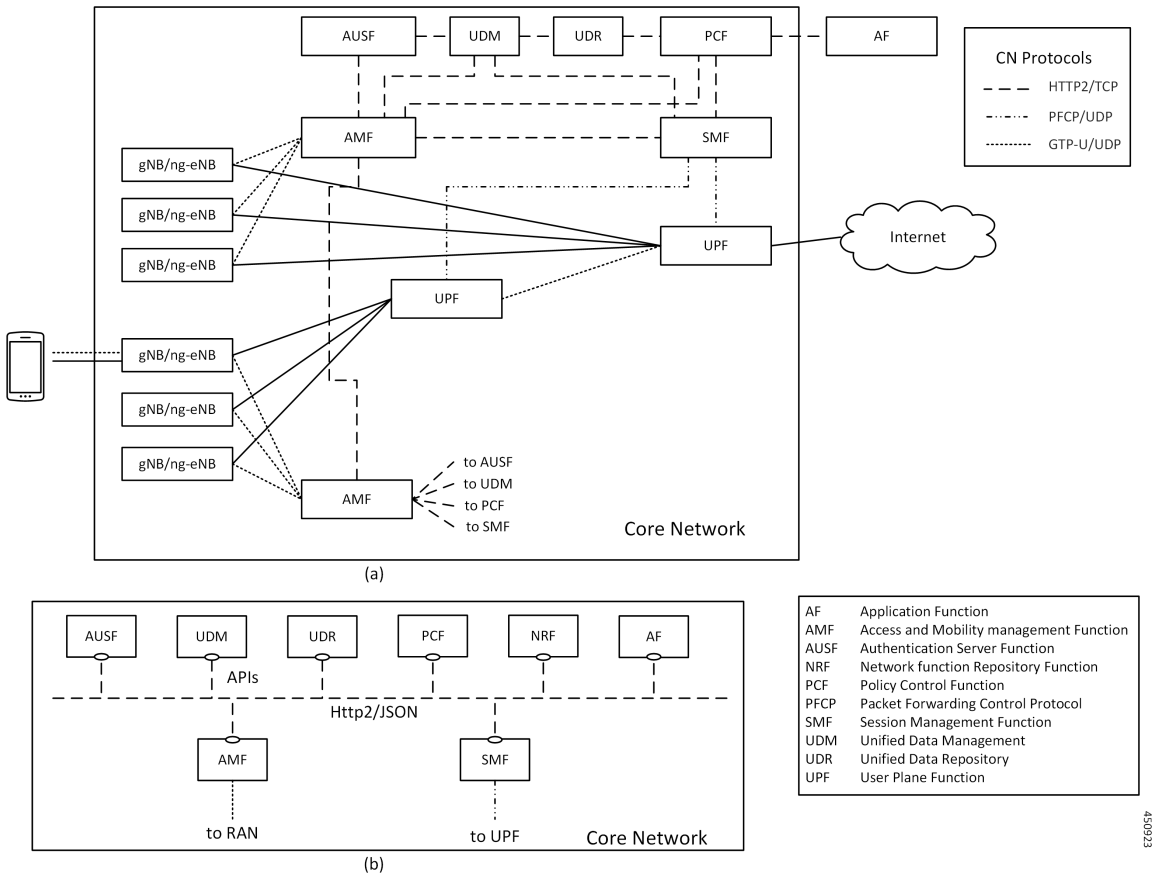


Figure 6: 5G Core Network - (a) Interface Representation, and (b) API Level Representation



Use Cases and Features

The main functions of AMF are to support:

- Connection management, registration, and mobility management with UE.
- It terminates the control plane of 5G Radio Access Network and manages the register/deregister status/mobility of UEs.

This section describes the use cases that AMF supports.

4G EPC Interworking with N26

The N26 interface is used to transfer mobiles authentication and session context as the mobile moves between the two systems (MME <-> AMF). This scheme provides seamless mobility to an UE's IP session and hence enables seamless mobility to voice sessions between 4G and 5G. Both Idle and Connected mode handovers are supported.

The following features are related to this use case:

- Internode Registration Support, on page 209

- N26-based Handover Procedures - EPC Interworking, on page 251
- N26 Stack Integration Support, on page 247

AN Release Procedure

The AMF supports procedure to release the logical NGAP signalling connection and the associated N3 User Plane connections and RAN RRC signalling and resources.

- AN-initiated—The AMF supports RAN initiated release because of inactivity, UE initiated connection release, link failure or any other reason.
- AMF-initiated—The AMF supports AMF-initiated release because of:
  - IE value received as a part of prior procedure.
  - Optional timer expiry

The following feature is related to this use case:

- Idle Entry Procedure, on page 205

Base AMF Configuration

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

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

The following feature is related to this use case:

- Deploying and Configuring AMF through Ops Center , on page 21

CMAS Support

The AMF supports interaction with Cell Broadcast Centre Function (CBCF) for public warning functionality and required messaging toward gNB as well as for realizing broadcast functionality.

The following feature is related to this use case:

- CMAS Service Support, on page 115

Encryption and Integrity Protection

The AMF supports both 5G-AKA and EAP-AKA' authentications. The following encryption and integrity protection algorithms enable encryption and integrity protection on the N1 interface:

- NEA0/NIA0
- 128-NEA1/128-NIA1
- 128-NEA2/128-NIA2

The following features are related to this use case:

- EAP and AKA Authentication, on page 161
- Encryption and Integrity Protection, on page 165

Handover Procedure

The AMF supports procedures to handover a UE from source NG-RAN to target NG-RAN.

- Xn Handover—The AMF supports Xn handover, used to handover a UE from source NG-RAN to target NG-RAN using Xn when the AMF is unchanged.
- N2 Handover—The AMF supports inter-AMF and intra-AMF N2 handovers. These can be triggered due to new radio conditions/load balancing, if there is no Xn connectivity between source and target NG-RAN or due to AMF change.

The following features are related to this use case:

- N2 Handover Procedure, on page 241
- Xn Handover, on page 481

Lawful Intercept

The Lawful Intercept (LI) feature enables law enforcement agencies (LEAs) to intercept subscriber communications. The LI functionality provides the network operator the capability to intercept and control messages of targeted mobile users.

For more details, contact your Cisco account representative.

NRF Register/Discovery

The AMF supports register/de-register/update with NRF. The AMF includes various query parameters, such as nf-type, plmn-info, slice-data, DNN, routing-indicator when it sends the NFDiscovery request towards the NRF during discovery of network elements. When AUSF, UDM, PCF, and SMF aren't locally configured, the AMF queries the NRF NF discovery API to discover them.

The following feature is related to this use case:

- NRF (Network Function Repository) Services, on page 287

OAM Support

The AMF provide counters and alarms/alerts for monitoring the AMF-specific functionality and features.

The following features are related to this use case:

- Application-based Alerts, on page 87
- Deploying and Configuring AMF through Ops Center , on page 21
- Pods and Services Reference, on page 27

- Smart Licensing, on page 43
- AMF Rolling Software Upgrade, on page 73
- Troubleshooting, on page 485

For more information, you can also see the following documents:

- *UCC 5G AMF - Metrics Reference*
- *UCC 5G AMF - CLI Reference*

PDU Session Establishment

The UE receives data services through a Protocol Data Unit (PDU) session, which is a logical connection between the UE and core network. In a PDU session establishment, the 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 establishes a PDU session when service is needed.

The following feature is related to this use case:

- Compliance to 3GPP Specifications, on page 123

PDU Session Modification

The PDU session modification procedure happens when one or several of the QoS parameters exchanged between the UE and the network are modified. Both UE- and SMF-initiated PDU session modifications are supported.

The following feature is related to this use case:

- Compliance to 3GPP Specifications, on page 123

PDU Session Release

The PDU session release procedure is used to release all the resources associated with a PDU Session. This can either be initiated by the UE or the SMF.

The following feature is related to this use case:

- Compliance to 3GPP Specifications, on page 123

Redundancy Support

The AMF support high availability for AMF specific pods and ensures session continuity in case of Pod failure.

The following feature is related to this use case:

- High Availability Services, on page 199

Roaming and Restriction Support

The AMF supports subscribers moving seamlessly in geographies beyond their network reach. Restriction control is also supported. Steering of Roaming (SoR) is supported at AMF.

The following feature is related to this use case:

- Roaming Support, on page 351

Service Request Procedure

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.

- UE Triggered—The AMF supports UE in Idle state initiating Service request procedure for sending uplink signalling messages, user data or other reasons.
- Network Triggered Service Request/Paging—The AMF supports procedure when the network needs to send Paging Request to RAN based on trigger(s) from UDM, SMF and other NF nodes. The paging request triggers the UE to initiate Service Request procedure.

The following features are related to this use case:

- Paging Support, on page 317
- Service Request Procedure, on page 375

SMS over NAS

The AMF supports registration and deregistration for SMS over NAS. MO/MT SMS are supported in CM-IDLE/CM-CONNECTED state.

The following feature is related to this use case:

- SMS over the Non-Access Stratum Procedures, on page 401

UE Configuration Update Procedure

The AMF supports UE Configuration Update procedure for access and mobility management related parameters, such as GUTI, TAI-list.

The following feature is related to this use case:

- UE Configuration Management Procedures, on page 451

Deregistration

To enable UE to deregister from 5GS network.

- UE-init Deregistration—The deregistration procedure allows the UE to inform the network that it doesn't want to access the 5G data services.
- Network-init Deregistration—The deregistration can be initiated by the UDM if the subscription is withdrawn for the UE or UE has moved to another node. It can also be initiated by AMF based on OAM requirements.

The following feature is related to this use case:

- Compliance to 3GPP Specifications, on page 123

Registration

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

- Initial Registration—The AMF supports initial UE registration to 5GS network.
- Mobility Registration Update—The AMF supports mobility registration update:
  - When changing to new Tracking Area (TA) outside the UE's Registration Area in Connected/Idle state.
  - When the UE needs to update its capabilities or negotiated parameters.

  AMF also supports registration with AMF change.
- Periodic Registration Update—The 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 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.
- Emergency Registration—The AMF supports Emergency Registration without authentication/subscription.

The following feature is related to this use case:

- Compliance to 3GPP Specifications, on page 123

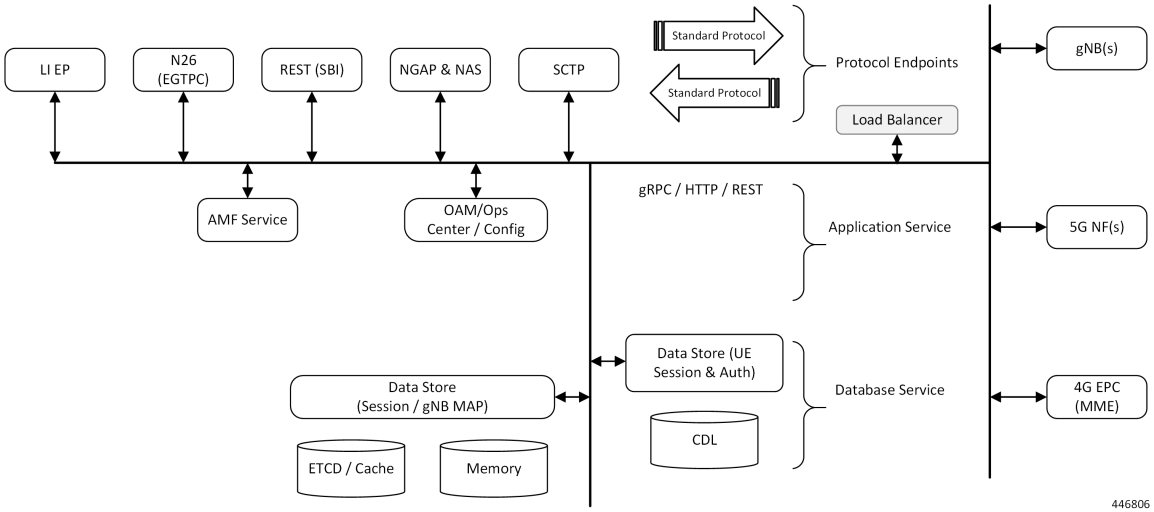
Deployment Architecture and Interfaces

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 the same namespace in Kubernetes.

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 an 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 8: End-to-End Registration by an UE Call Flow

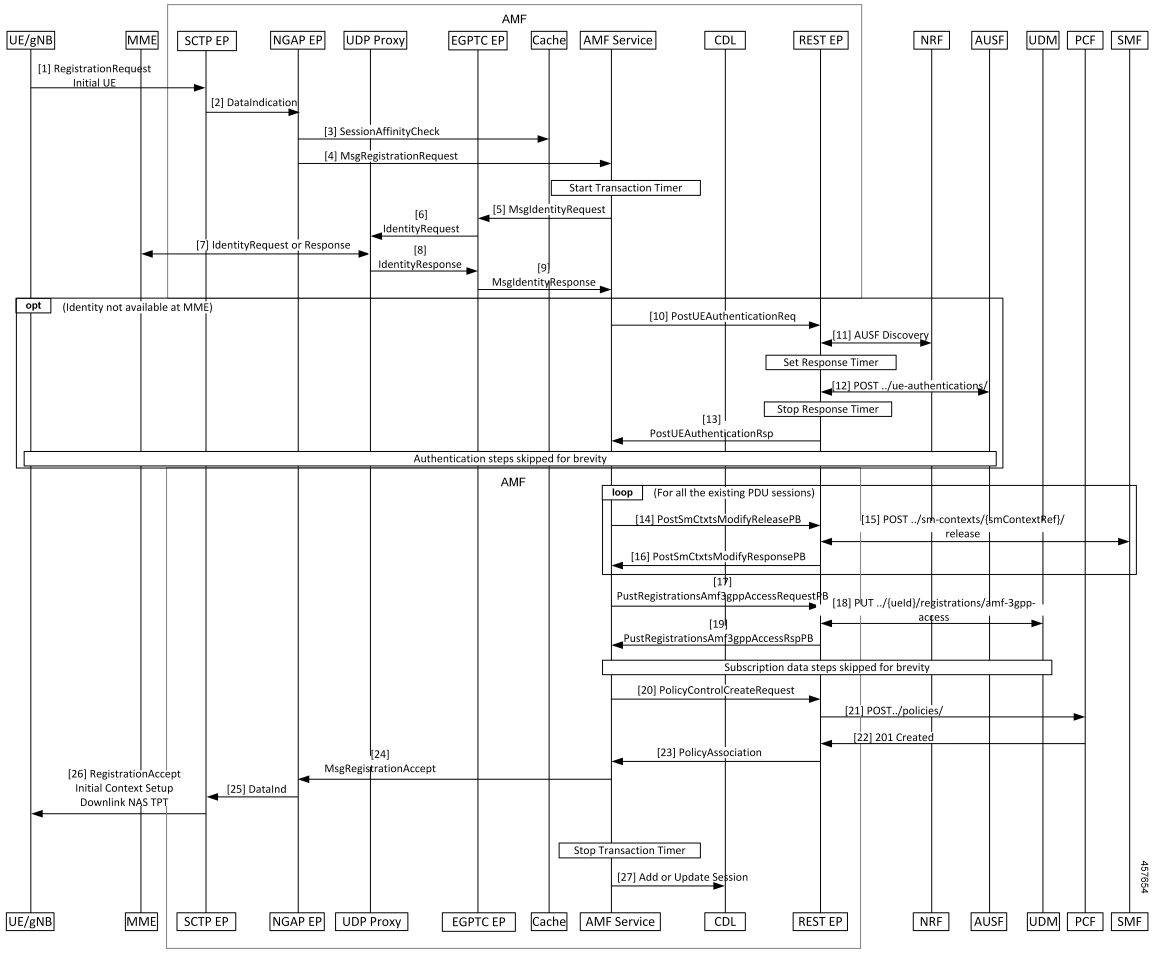


Table 1: End-to-End Registration by an UE Call Flow Description

Step	Description
1	The UE sends an Initial Registration Request to the gNB, which sends it to the AMF in an Initial UE message.
2	On the AMF, the message reaches the SCTP Endpoint (EP), which terminates the SCTP protocol and 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 are performed 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 the UE, the AMF maintains affinity of subscriber with service pod internally. If there's 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.
6	The EGTPC EP forwards the request to the UDP proxy after a transaction ID has been allocated.
7	The 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	The 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 are skipped.
12	The REST EP sends an Authentication Information Request 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	The REST EP uses the NRF to resolve UDM selection for this request and sends a request to the UDM.

Step	Description
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 the REST EP.
21	The 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	The NGAP encodes both the NAS message and the NGAP message and sends a message to the SCTP EP.
25	The SCTP EP sends the message out to the gNB.
26	The rest of the message has been excluded.
27	The AMF sends an Add or Update Session message to the CDL.

License Information

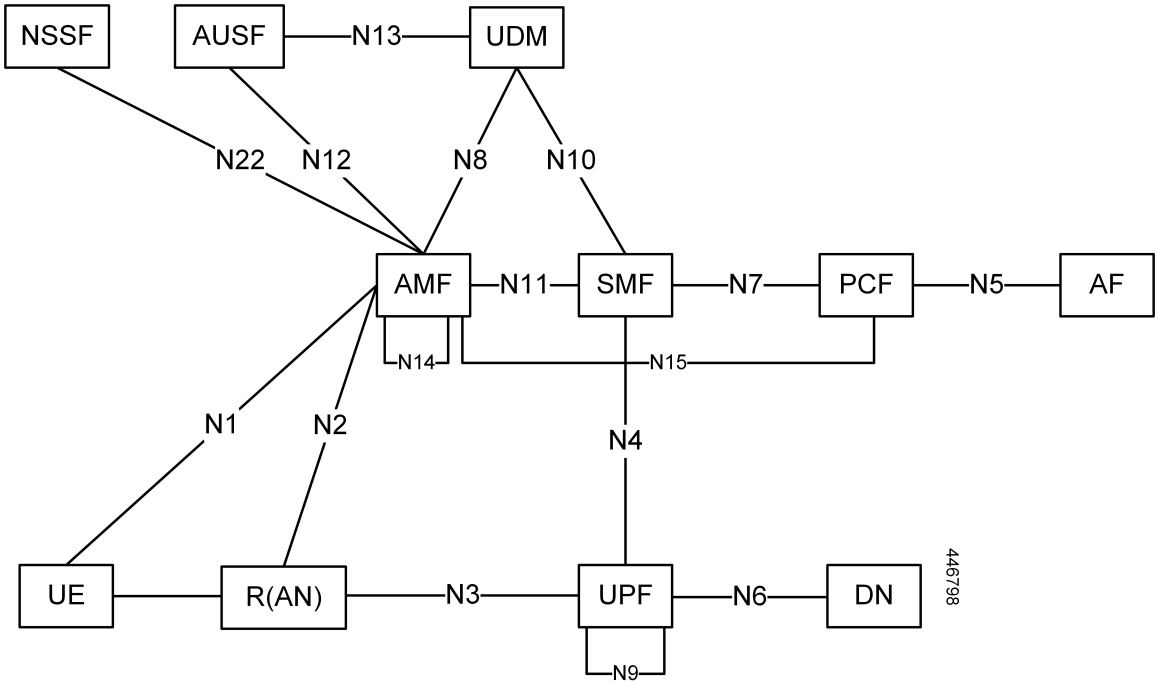
The AMF supports Cisco Smart Licensing. For more information, see the *Smart Licensing* chapter in this document.

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 9: 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

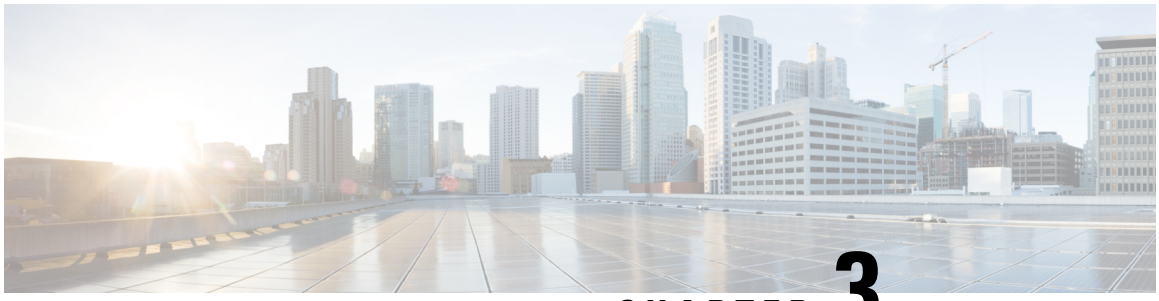
Interface	Relationship	3GPP Specification	Version
N1	Between UE and AMF	24.501	Compliance Support: 15.4.0
N2	Between R(AN) and AMF	38.413	Compliance Support: 15.4.0
N8	Between AMF and UDM	29.503	Compliance Support: 15.4.0
N11 (Namf)	Between AMF and SMF	29.518	Compliance Support: 15.5.1
N11 (Nsmf)	Between 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

Interface	Relationship	3GPP Specification	Version
N15	Between AMF and PCF	29.507	Compliance Support: 15.4.0

Limitations

The AMF has the following limitations:

- NGRAN location services are not supported.
- NSSF interactions are 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
      net.sctp.rto_max: 5000
```

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://209.165.200.230:9080/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 the 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*>

   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**

Note 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 the 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.

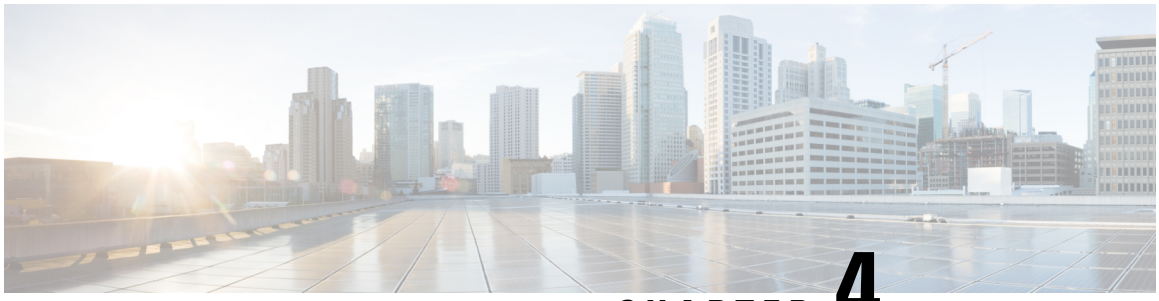
To check the sample configuration file, refer to Sample Configuration, on page 493.

Post Configuration Check

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

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

Also, log in to the Master node and check the AMF pod health and running state, using the following command: **kubectl get pod -n** *amf_namespace*.



CHAPTER 4

Pods and Services Reference

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	Enabled - Always-on For Multiple Service Pods on Multiple Nodes: Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 6: Revision History

Revision Details	Release
Multiple Service Pods on Multiple Nodes	2023.02.0
First introduced.	2021.04.0

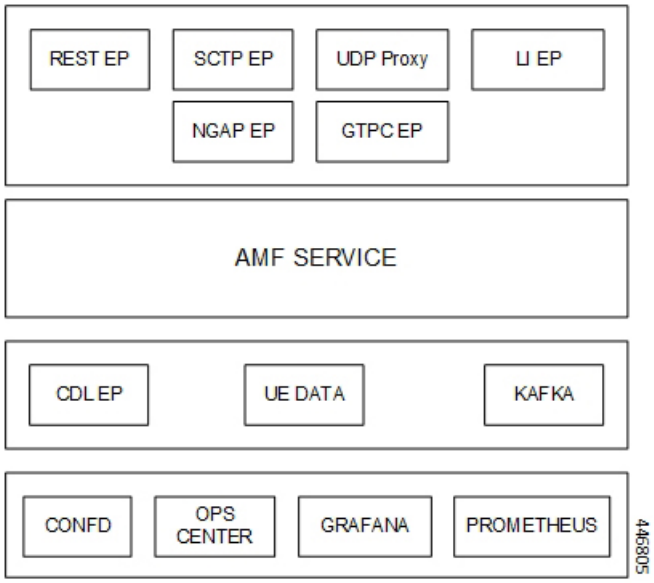
Feature Description

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 10: Communication Workflow of Pods



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 33.

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 7: 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
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-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	Operates as GTPC endpoint of AMF.	Protocol
kafka	Hosts the Kafka details for the CDL replication.	Protocol
nodemgr	Performs node level interactions, such as N4 link establishment, management (heart-beat). It also generates unique identifiers, such as NGAP-ID, TMSI, GUTI and so on.	Service

Pod Name	Description	Kubernetes Node Name
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-service	Contains main business logic of AMF.	Service
amf-rest-ep	Operates as REST endpoint of AMF for HTTP2 communication.	Protocol
amf-protocol-ep	Processes NGAP/NAS Protocol Messages.	Protocol
amf-gosctp-lb	Operates as SCTP endpoint for AMF.	Protocol
udp-proxy	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
li-ep	Responsible for handling LI-IRI events for AMF.	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 8: AMF Services and Pods

Service Name	Pod Name	Description
alert-frwd-ops-center	ops-center-amf-ops-center	Responsible for forwarding SNMP alerts.

Service Name	Pod Name	Description
amf-gosctp-lb	amf-gosctp-lb	Responsible for receiving 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.
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-cdl-cdl-amf	grafana-dashboard-cdl	Responsible for the default dashboard of CDL metrics in Grafana.

Service Name	Pod Name	Description
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.
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 9: 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.

Port	Service	Usage
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.
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.
3179	Tcpwrapped	SMI uses this TCP port for Calico(Kubernetes networking). Calico is used for routing the networking packets to pods.

In addition to the preceding ports, AMF uses the ports that are destined for SMI for routing information between hosts. For more information on SMI ports, see *Ultra Cloud Core Subscriber Microservices Infrastructure Operations Guide*.

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 protocol value. Example: For k8 label sctp-layer key value is smi.cisco.com/node-type-2 value protocol.

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

Viewing the Status and Pod Details

If the service requires extra pods, the AMF creates, and deploys those pods.

You can perform the following:

- View the list of pods that are participating in your deployment through the AMF Ops Center.
- 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 the pod is in the current state.

Sample Output:

```
kubectl get pod -n amf-ins cache-pod-0 -o yaml
apiVersion: v1
kind: Pod
metadata:
  annotations:
    cni.projectcalico.org/podIP: 209.165.201.3/32
    cni.projectcalico.org/podIPs: 209.165.201.3/32,4141:4141::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.209.165.201.29.nip.io/amf.2021.04.m0.i80/mobile-cnat-app-infra/cache-pod/main/
cache_pod:0.1.0-32e359a
    imageID:
docker-pullable://docker.209.165.201.29.nip.io/amf.2021.04.m0.i80/mobile-cnat-app-infra/
cache-pod/main/cache_pod@sha256:d2c82e1af506cf92c04d93f40ef8ca1dfcf830d457bfeabd4dc8aba7b63ce894

    lastState: {}
    name: cache-pod
    ready: true
    restartCount: 0
    started: true
    state:
      running:
        startedAt: "2021-10-16T18:03:49Z"
  hostIP: 209.165.201.29
  phase: Running
  podIP: 209.165.201.3
  podIPs:
  - ip: 209.165.201.3
  - 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-ins3 -o wide

NAME                                              READY   STATUS    RESTARTS
AGE     IP               NODE                      NOMINATED NODE   READINESS GATES
amf-ins3-amf-gosctp-lb-sctp-1-0                   1/1     Running   0
2d16h   209.165.201.29     amf-cndp-tb27d-master-1   <none>           <none>
amf-ins3-amf-gosctp-lb-sctp-1-1                   1/1     Running   0
2d16h   209.165.201.30                       amf-cndp-tb27d-master-2   <none>
  <none>
amf-ins3-amf-protocol-ep-default-0                2/2     Running   0
2d16h   192.203.42.85     amf-cndp-tb27d-master-2   <none>           <none>
amf-ins3-amf-protocol-ep-default-1                2/2     Running   0
2d16h   192.203.236.6     amf-cndp-tb27d-master-1   <none>           <none>
amf-ins3-amf-rest-ep-n0-0                         2/2     Running   0
2d19h   192.203.236.55    amf-cndp-tb27d-master-1   <none>           <none>
amf-ins3-amf-rest-ep-n0-1                         2/2     Running   0
2d19h   192.203.42.123    amf-cndp-tb27d-master-2   <none>           <none>
amf-ins3-amf-service-n0-0                         2/2     Running   1 (2d19h ago)
2d19h   192.203.211.179   amf-cndp-tb27d-master-3   <none>           <none>
amf-ins3-amf-service-n0-1                         2/2     Running   0
2d19h   192.203.211.131   amf-cndp-tb27d-master-3   <none>           <none>
amf-ins3-amf-service-n1-0                         2/2     Running   1 (2d19h ago)
```

```
2d19h   192.203.236.62    amf-cndp-tb27d-master-1   <none>           <none>
amf-ins3-amf-service-n1-1                           2/2     Running   0
2d19h   192.203.236.63    amf-cndp-tb27d-master-1   <none>           <none>
base-entitlement-amf-679fd785c-2zrnl                1/1     Running   0
3d12h   192.203.211.149   amf-cndp-tb27d-master-3   <none>           <none>
cache-pod-0                                         1/1     Running   0
2d19h   192.203.236.50    amf-cndp-tb27d-master-1   <none>           <none>
cache-pod-1                                         1/1     Running   0
2d19h   192.203.42.80     amf-cndp-tb27d-master-2   <none>           <none>
etcd-amf-ins3-etcd-cluster-0                        2/2     Running   0
3d11h   192.203.236.52    amf-cndp-tb27d-master-1   <none>           <none>
etcd-amf-ins3-etcd-cluster-1                        2/2     Running   0
3d11h   192.203.42.126    amf-cndp-tb27d-master-2   <none>           <none>
etcd-amf-ins3-etcd-cluster-2                        2/2     Running   0
3d11h   192.203.211.178   amf-cndp-tb27d-master-3   <none>           <none>
georeplication-pod-0                                1/1     Running   0
3d11h   209.165.201.31
                        amf-cndp-tb27d-master-2   <none>           <none>
grafana-dashboard-amf-774bdd8b6d-6t6kw              1/1     Running   0
3d11h   192.203.211.130   amf-cndp-tb27d-master-3   <none>           <none>
grafana-dashboard-etcd-amf-ins3-8597cf9fdc-72z7w    1/1     Running   0
3d11h   192.203.211.170   amf-cndp-tb27d-master-3   <none>           <none>
gtpc-ep-n0-0                                        2/2     Running   0
2d19h   192.203.236.22    amf-cndp-tb27d-master-1   <none>           <none>
gtpc-ep-n0-1                                        2/2     Running   0
2d19h   192.203.42.125    amf-cndp-tb27d-master-2   <none>           <none>
li-ep-n0-0                                          2/2     Running   0
3d11h   192.203.42.108    amf-cndp-tb27d-master-2   <none>           <none>
li-ep-n0-1                                          2/2     Running   0
3d11h   192.203.236.13    amf-cndp-tb27d-master-1   <none>           <none>
nodemgr-n0-0                                        2/2     Running   1 (2d19h ago)
2d19h   192.203.236.44    amf-cndp-tb27d-master-1   <none>           <none>
nodemgr-n0-1                                        2/2     Running   0
2d19h   192.203.211.150   amf-cndp-tb27d-master-3   <none>           <none>
oam-pod-0                                           2/2     Running   0
3d11h   192.203.211.146   amf-cndp-tb27d-master-3   <none>           <none>
ops-center-amf-ins3-ops-center-64479bd9d6-zqzzz     4/4     Running   0
3d12h   192.203.42.81     amf-cndp-tb27d-master-2   <none>           <none>
prometheus-rules-etcd-57688b5657-5gv5z              1/1     Running   0
3d11h   192.203.211.175   amf-cndp-tb27d-master-3   <none>           <none>
smart-agent-amf-ins3-ops-center-798d5f9884-zplrn    1/1     Running   0
3d12h   192.203.42.120    amf-cndp-tb27d-master-2   <none>           <none>
udp-proxy-0                                         1/1     Running   0
2d19h   198.51.100.10     amf-cndp-tb27d-master-1   <none>           <none>
udp-proxy-1                                         1/1     Running   0
2d19h   198.51.100.11     amf-cndp-tb27d-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 10: Pod States

State	Description
Running	The pod is healthy and deployed on a node. It contains one or more containers

State	Description
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 Summary and Details

Use the following commands to view the service summary:

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   209.165.202.130   <none>
8080/TCP                                      29d
amf-gosctp-lb                           ClusterIP   209.165.202.140   <none>
7084/TCP                                      36h
amf-nrf-service                         ClusterIP   209.165.202.151   209.165.200.241
9090/TCP                                      36h
amf-protocol-ep                         ClusterIP   209.165.202.142   <none>
9003/TCP,8080/TCP                             36h
amf-rest-ep                             ClusterIP   209.165.202.145   <none>
9003/TCP,8080/TCP,9201/TCP                    36h
amf-sbi-service                         ClusterIP   209.165.202.156   209.165.200.241
8070/TCP                                      36h
amf-service                             ClusterIP   209.165.202.144   <none>
9003/TCP,8080/TCP                             36h
base-entitlement-amf                    ClusterIP   209.165.202.137   <none>
8000/TCP                                      29d
bgpspeaker-pod                          ClusterIP   209.165.202.154   <none>
9008/TCP,7001/TCP,8879/TCP                    36h
datastore-notification-ep               ClusterIP   209.165.202.135   209.165.200.240
8012/TCP                                      36h
documentation                           ClusterIP   209.165.202.134   <none>
8080/TCP                                      29d
etcd                                    ClusterIP   None              <none>
2379/TCP,7070/TCP                             36h
etcd-amf-ins1-etcd-cluster-0            ClusterIP   209.165.202.143   <none>
2380/TCP,2379/TCP                             36h
etcd-amf-ins1-etcd-cluster-1            ClusterIP   209.165.202.139   <none>
2380/TCP,2379/TCP                             36h
etcd-amf-ins1-etcd-cluster-2            ClusterIP   209.165.202.131   <none>
2380/TCP,2379/TCP                             36h
grafana-dashboard-amf                   ClusterIP   209.165.202.138   <none>
```

```
9418/TCP                                          36h
grafana-dashboard-app-infra-amf-ins1     ClusterIP   209.165.202.133   <none>
9418/TCP                                          36h
grafana-dashboard-etcd-amf-ins1          ClusterIP   209.165.202.141   <none>
9418/TCP                                          36h
gtpc-ep                                  ClusterIP   209.165.202.149   <none>
9003/TCP,8080/TCP                                 36h
ldap-proxy-amf-ins1-oam-pod              ClusterIP   209.165.202.132   <none>
636/TCP,389/TCP                                   36h
li-ep                                    ClusterIP   209.165.202.150   <none>
9003/TCP,8080/TCP                                 36h
local-ldap-proxy-amf-ins1-ops-center     ClusterIP   209.165.202.148   <none>
636/TCP,369/TCP                                   29d
netconf-ops-center-amf-ins1-ops-center   ClusterIP   209.165.202.155   209.165.200.231
2024/TCP                                          29d
nodemgr                                  ClusterIP   209.165.202.153   <none>
9003/TCP,8884/TCP,8879/TCP,9201/TCP,8080/TCP      36h
oam-pod                                  ClusterIP   209.165.202.147   <none>
9008/TCP,7001/TCP,8879/TCP,10080/TCP,8080/TCP     36h
ops-center-amf-ins1-ops-center           ClusterIP   209.165.202.152   <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   209.165.202.129   <none>
8888/TCP                                          29d
ssh-ops-center-amf-ins1-ops-center       ClusterIP   209.165.202.136   209.165.200.231
2025/TCP                                          29d
```

Use the following commands to view the comprehensive service details:

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: 209.165.202.145
  clusterIPs:
  - 209.165.202.145
  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: {}
```

Multiple Service Pods on Multiple Nodes

Feature Description

This feature helps in bringing up service pods on two or more different nodes.

How it Works

To enable this feature, ensure the following:

- Set the configuration to two nodes and the number of replicas on each node, so that each node in an RU system has the number of configured amf-service replicas.
- When a node gets removed, the system won't be able to spawn a new service replica on the node that already has one.
- If one node (RU) gets removed from the three nodes and one replica configuration, the service pod previously running on the removed node (RU) respawns on the other available node (RU).
- The same changes can be configured for amf-rest-ep also.

Feature Configuration

To configure this feature, use the following sample configuration:

```
config
   instance instance-id instance-id
      endpoint { sbi | service }
         nodes number_of_nodes
         replicas number_of_replicas
         end
```

NOTES:

- **instance instance-id** *instance-id*—Specify the endpoint instance ID.
- **endpoint { sbi | service }**—Specify the endpoint that must be configured.

- **nodes** *number_of_nodes*—Specify the number of nodes that must be used for resiliency.
- **replicas** *number_of_replicas*—Specify the number of replicas that must be created for the endpoint, on each node.

Configuration Example

The following is an example configuration.

```
config
    instance instance-id 1
        endpoint service
            nodes 2
            replicas 2
        exit
    exit
exit
```

Configuration Verification

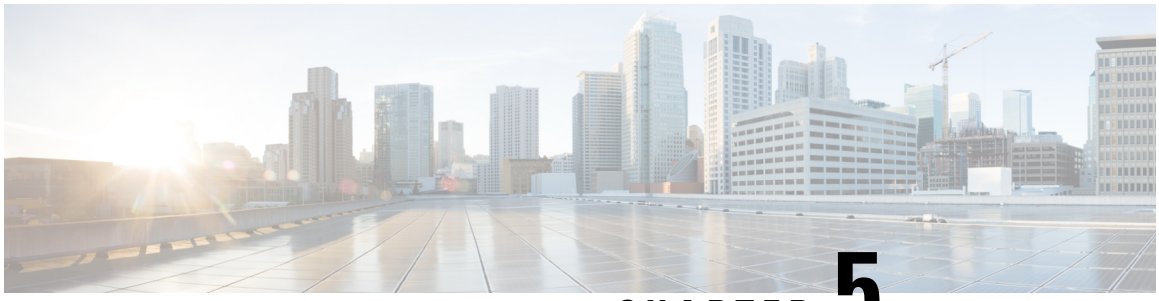
To verify the configuration:

```
show running-config instance instance-id 1 endpoint service
```

Note To allow the spawning of pods on the nodes, it's necessary to label the nodes appropriately in the cluster.

To verify the label:

```
show running-config k8 label service-layer
```



CHAPTER 5

Smart Licensing

Feature Summary and Revision History

Summary Data

Table 11: 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 12: Revision History

Revision Details	Release
First introduced.	2021.04.0

Smart Software Licensing

Cisco employs two types of license models - Legacy Licensing and Smart Software Licensing. Legacy Licensing consists of software activation by installing Product Activation Keys (PAK) on to the Cisco product. A Product Activation Key is a purchasable item, ordered in the same manner as other Cisco equipment and

used to obtain license files for feature set on Cisco Products. This traditional licensing does not need any online communication with the Cisco licensing server.

Smart Software Licensing is a cloud-based licensing of the end-to-end platform through the use of a few tools that authorize and deliver license reporting. Smart Software Licensing functionality incorporated into the NFs complete the product registration and authorization. AMF supports the Smart Software Licensing model.

Smart Licensing simplifies the purchase, deployment, and management of Cisco software assets. Entitlements are purchased through your Cisco account through Cisco Commerce Workspace (CCW) and immediately available in your Virtual Account for usage. This approach 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.

For information on setting up or managing the Smart Accounts, 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. To create a Cisco Smart Account, perform the following steps:

Step 1 Visit 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 appears.

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: Smart Transport
     Registration URL: null
     Utility URL: null

   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: Smart Transport
```

```
  Registration URL: null
  Utility URL: null

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: Smart Transport
     Registration URL: null
     Utility URL: null

   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: Smart Transport
  Registration URL: null
  Utility URL: null

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

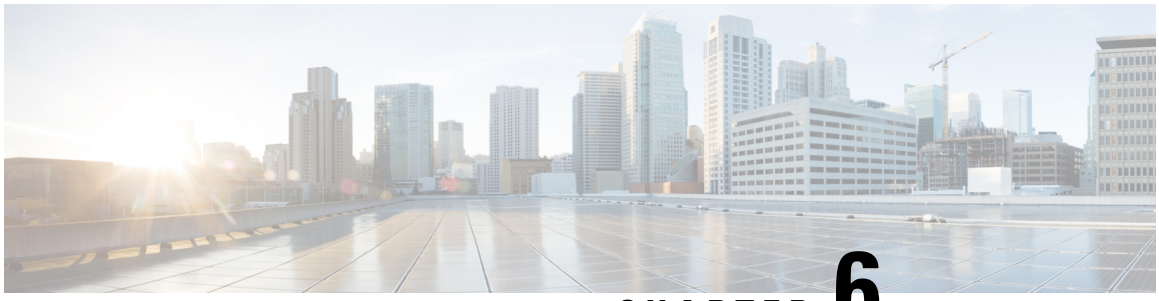
This section describes operations, administration, and maintenance information for this feature.

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 6

AMF Authentication and GUTI Reallocation Configuration Control

Feature Summary and Revision History

Summary Data

Table 13: Summary Data

Applicable Products or Functional Area	AMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	

Revision History

Table 14: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

AMF supports the authentication activities and the GUTI (Globally Unique Temporary Identity) reallocation configuration control for call flows.

GUTI

GUTI is used to keep the subscriber's IMSI confidential. AMF allocates a GUTI to the UE. It's composed of PLMN ID, AMF ID, and TMSI. As it's a temporary identifier, its associations aren't fixed to any specific subscriber or mobile. A single 5G-GUTI is used to access the Security Context of 3GPP and non-3GPP technologies within the AMF.

Supported Functions

AMF supports the following functions:

- Authentication and GUTI reallocation counter maintained as per the UE. For each supported type, separate counters are maintained.
- Time reference per UE for network-initiated GUTI reallocation
- GUTI reallocation attempted as per the configuration for a specific time interval.
- Includes the new GUTI in either Registration Accept or Configuration Update Command NAS message
- AMF shows the allocated GUTI and the allocated time in the **show subscriber** command output.

Note Collision of GUTI reallocation in Registration Accept or Configuration Update Command with other procedures isn't supported.

Supported Scenarios

This feature supports the following scenarios based on the UE on time and frequency of access attempts. These scenarios are part of the Registration and Service Request procedure:

- Selective authentication
- GUTI reallocation

The frequency supports access attempts per UE and not across UEs.

Unsupported Scenarios

The following scenario isn't supported:

- Authentication requirements dependent or based on EAP-AKA or EAPAKA' or EAPAKA Prime
- When the latest GUTI isn't acknowledged, the UE is paged simultaneously with the old and the new GUTI.

Note GUTI reallocation process takes place only for the successful procedure.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   call-control-policy ccp_name
      authenticate registration-request type { frequency frequency_count |
periodicity duration }
      no authenticate registration registration-request
      authenticate service-request type { frequency frequency_count |
periodicity duration }
      no authenticate registration service-request
     authenticate all-events { frequency frequency_count | periodicity duration
 }
      no authenticate all-events
      guti-reallocation type { frequency frequency_count | periodicity duration
 }
      no guti-reallocation
      end
```

NOTES:

- **call-control-policy** *ccp_name*—Specify the UE-specific name for call control policy. Must be a string.
- **authenticate registration-request** { normal | periodic | inter-rat | intra-rat }—Specify the required option to authenticate the registration process.
- **registration-type normal** —Specify the initial registration details with locally allocated GUTI.
- **authenticate service-request** { data | signaling }—Specify the option to authenticate the service type for the service request.
- **authenticate all-events** —Specify the option to authenticate all events. It's also the default or the fallback authentication option, when the configuration doesn't present for any type.
- **guti-reallocation** { periodic-registration | service-request }—Specify the options to authenticate the GUTI reallocation process.
- **no authenticate** { [registration-request] | [service-request] | [all-events] | [guti-reallocation] }—Specify the option for which the authentication isn't required.
- **frequency** *frequency_count*—Specify the required frequency duration or count for authenticating each option. The frequency range is 0–256. The disabled value is 0.
- **periodicity** *duration*—Specify the time, period, or duration for authenticating the selected option. The periodicity duration range is 0–10800 (minutes). The disabled value is 0.

Note

- The AMF does not maintain periodicity and frequency after the context is deleted. If UE context is not available, the frequency and periodicity triggers doesn't work.

  For example, if the mobile identifier in the NAS Attach is a foreign GUTI, the AMF doesn't trigger authentication/GUTI reallocation for the subscriber based on frequency/periodicity.

- Inter-rat ReAuth/SelectiveAuth is supported for frequency 1 and periodicity 0 only.
- If the GUTI reallocation and reauthentication need to be configured on the basis of only frequency or only periodicity, then the non-used or disabled configuration parameter (such as periodicity or frequency) must be set as 0.
- The periodicity values in minutes indicate that **Amf ReAuth** or **ReAllocateGuti** time difference between the two successive requests is more than the defined values.
- The periodicity timer configured for any procedure starts on the first occurrence of that procedure.
- The defined frequency value indicates that **Amf ReAuth** or **ReAllocateGuti** for every subscriber.
- When the AMF resets both frequency and periodicity, it indicates the expired value for either frequency or periodicity.
- The default GUTI reallocation is enabled for **periodic-registration**. The following commands are used to disable or enable this option.

```
config
    amf-global call-control-policy ccp-name
    guti-reallocation periodic-registration disabled
    end

config
    amf-global call-control-policy ccp-name
    no guti-reallocation periodic-registration disabled
    guti-reallocation periodic-registration { frequency count | periodicity
duration }
    end
```

Configuration Example

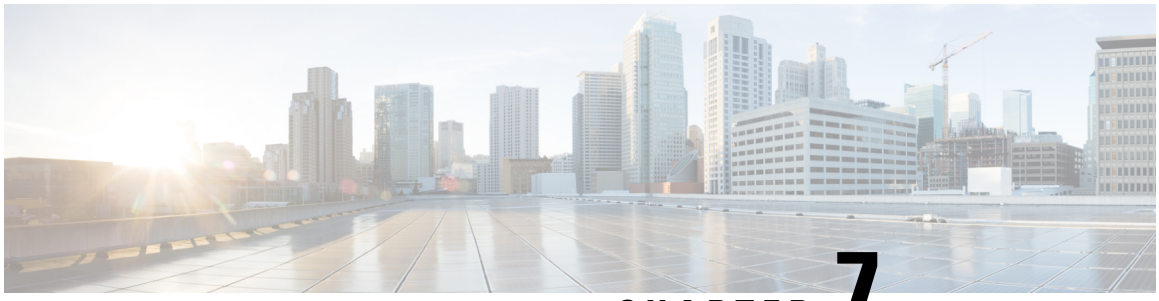
The following is an example configuration.

```
amf-global
   call-control-policy local
      guti-reallocation periodic-registration frequency 2 periodicity 1
      guti-reallocation service-request frequency 0 periodicity 1
      authenticate service-request signaling frequency 1 periodicity 20
      authenticate registration-request periodic frequency 1 periodicity 0
      end
```

Configuration Verification

To verify the configuration:

show call-control-policy *ccp_name*



CHAPTER 7

AMF Bulk Statistics and MME Equivalent KPI Support

Feature Summary and Revision History

Summary Data

Table 15: Summary Data

Applicable Products or Functional Area	AMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	

Revision History

Table 16: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

The bulk statistics and Key Performance Indicators (KPIs) are used for analyzing the AMF performance.

The following is a list of applicable bulk statistics:

- **Gauge:**
  - A snapshot value that shows the statistic at the time of reporting.
  - These statistics values can increment or decrement continuously.
  - **Example:** The number of current PDP contexts, simultaneous Active EPS Bearers, and so on
- **Counter:**
  - A historic value that shows the statistic accumulated for a specific time range.
  - These statistics values can only increment except in the following two scenarios:
    - **Rollover:** Where a counter exceeds its maximum value and rolls over to zero.
    - **Reset:** Where a counter is manually reset to zero.
  - **Example:** The total number of CSR requests received.

How it Works

This section describes how this feature works.

Bulk statistics allows you to configure various schemas for collecting statistics from the system. It also offloads those statistics to a collector for offline review and analysis. They are further processed for the following scenarios:

- Controlling the statistics gathering and reporting
- Collecting and transferring on both the active and the standby chassis
- Providing specific requirements for more selective statistics obtained on standby
- Acting as a subset of the total statistics collected over a specific timeline

OAM Support

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

Supported Service Request Counters

All scenarios are supported as per the required references. The following table lists various supported service request counters and their descriptions.

Table 17: Supported Service Request Counters

Name	Description	Trigger
Sctp Outgoing SCTPPacket stats	The total number of SCTP packets sent. Retransmitted DATA chunks are included.	Increments when the AMF sends the SCTP packet to the gNB.
Sctp Incoming SCTPPacket stats	The total number of SCTP packets received. Duplicates are included.	Increments when the AMF receives the SCTP packet from the gNB.
Sctp Init stats	The total number of times that AMF received SCTP INIT and association reached to established state.	Increments when the AMF received SCTP INIT and SCTP association is successfully established.
Sctp Shutdowns stats	The total number of times that associations terminated gracefully from AMF side or gNB.	Increments when the gNB is disconnected from the AMF.
Sctp Fragmented Message stats	The total number of user messages that needs to be fragmented due to the presence of the MTU.	Increments when the SCTP message is fragmented, due to the presence of the MTU.
Sctp Reassembled Message stats	The total number of user messages reassembled, after converting into DATA chunks.	Increments when the SCTP message is reassembled, due to the data fragment received from the gNB.
Ausf Ue eapaka rsp	The total number of EAPAKA or EAP-AKA or EAP-AKA-Prime responses received by the AMF.	Increments when the AMF receives an EAPAKA or EAP-AKA or EAP-AKA-Prime response for the eap-session request.
Ausf Ue eapaka cfm	The total number of EAPAKA or EAP-AKA or EAP-AKA-Prime authorization confirmation sent by the AMF.	Increments when the AMF sends AUSF EAPAKA or EAP-AKA or EAP-AKA-Prime CFM to AUSF.
Ausf Autentication Cfm Rsp Stats	The total numbers of 5g-aka confirm response received from the AUSF.	Increments when the AMF receives 5g-aka authentication confirm response.
Ausf Autentication Cfm Stats	The total numbers of 5g-aka confirm requests sent to the AUSF.	Increments when the AMF sends 5g-aka authentication confirm request to the AUSF.
Ausf Autentication Req Stats	The total number of AUSF authentication requests sent by the AMF.	Increments when the AMF receives authentication request.
Ausf Autentication Rsp Stats	The total number of AUSF authentications responses received by the AMF.	Increments when the AMF receives authentication response from the AUSF.

Name	Description	Trigger
Authentication Mac Failed	The total number of authentication MAC failures received during UE authentications.	Increments when the N1 authentication rejection is sent due to the MAC failure.
Authentication Reject	The total number of authentication rejections sent by the AMF.	Increments when the 5g-aka authentication fails.
Authentication Sync Failed	The total number of AMF authentication rejections due to the sync failure.	Increments when the N1 authentication rejection is sent due to the sync failure.
Ebi Fail Bearers Not Found	The total number of failures in EPS Bearer ID setup failed due to Bearer ID not found.	Increments when the EPS bearer ID allocation fails as the bearer ID isn't found.
Ebi Fail Invalid Pdu Session	The total number of failures due to PDU session ID not found.	Increments when the EPS bearer ID allocation fails as the PDU session ID isn't present.
Ebi Rejected No N26	The total number of failures due to the restriction of EPS bearer ID allocation.	Increments when the EBI allocation failure happens, due to the EBI allocation restriction.
Gnb Ics Fail Stats	The total number of initial context setup requests failed.	Increments when the AMF ICS fails.
Gnb Ics Req Stats	Total number of initial context setup requests sent by the AMF.	Increments when the AMF sends ICS requests.
Gnb Ics Rsp Stats	The total number of initial context setup responses received.	Increments when the AMF receives ICS responses.
Pcf Delete Req Stats	The total numbers of PCF delete requests sent during the PDU release deregistration procedure. It's triggered during clear subscriber process.	Increments when the AMF tried to clear the subscriber requests towards the UDM and the PCF.
Pcf Delete Rsp Stats	The total numbers of PCF delete responses received during the PDU release deregistration procedure.	Increments when the AMF tries to clear the subscriber response towards the UDM and the PCF.
Udm Pcscf Restor Req Stats	The total number of PCSCF restoration requests sent to the UDM.	Increments when the AMF sends the PCSCF restoration request to the UDM.
Udm Pcscf Restor Rsp Stats	The total number of PCSCF restoration responses received from the UDM.	Increments during the PDU modification process, when the PDU map doesn't have an entry, when the AMF receives the PCSCF restoration notification from the UDM.

Name	Description	Trigger
Udm Registration Req Stats	The total number of UDM registration requests sent.	Increments when the AMF sends the UDM registration request.
Udm Registration Rsp Stats	The total number of UDM registration responses received by the AMF.	Increments when the AMF receives the UDM registration response.
Udm Subscriber Data Req Stats	The total number of subscriber data requests sent to the UDM.	Increments when the AMF sends the subscriber data request to the UDM.
Udm Subscriber Data Rsp Stats	The total number of subscriber data response received from the UDM.	Increments when the AMF receives the subscriber data response.
Udm Subscriber Notify Req Stats	The total numbers of subscriber notify requests sent to the UDM.	Increments when subscriber notify requests are sent to the UDM, during the UDM registration procedure.
Udm Subscriber Notify Rsp Stats	The total number of subscribers notify responses received by the AMF.	Increments when the AMF receives the UDM subscriber notify response.
Udm Unsubscriber Notify Req Stats	The total numbers of UDM unsubscriber notify requests sent to the UDM.	During deregistration process, it's the total number of unsubscribe requests sent to the UDM.
Udm Unsubscriber Notify Rsp Stats	The total numbers of UDM response unsubscriber notify statistics received by the UDM.	During deregistration process, it's the total number of unsubscribe responses received from the UDM.
Ue Authentication Req Stats	The total number of UE authentication requests sent.	During the UE authentication procedure, this is incremented, when the UE authentication request is sent.
Ue Authentication Rsp Stats	The total number of UE authentication responses received.	During the UE authentication procedure, this is incremented, when the UE authentication response is received.
Ue Configuration Update Cmd	The total number of UE configuration update commands sent by the AMF.	Increments when the AMF sends the UE configuration update command.
Ue Configuration Update Complete	The total number of UE configuration update responses received with completion note of the procedure.	Increments when the AMF receives the UE config update response, for completion.
Ue Security Cmd Req Stats	The total number of security mode CMD sent from the AMF towards the UE.	Increments when the AMF sends the security mode command to the UE.

Name	Description	Trigger
Ue Security Cmd Rsp Stats	The total number of security mode complete messages received by the AMF.	Increments when the AMF receives the security mode completed messages.
Gtpc Rx Context Ack	The total number of GTPC contexts ACK received from the MME.	Increments when the AMF receives the context ACK from the MME.
Gtpc Rx Context Req	The total number of GTPC context requests received from the MME.	Increments when the AMF receives the GTPC context request from the MME.
Gtpc Rx Context Rsp	The total number of GTPC context request responses received from the MME.	Increments when the AMF receives the GTPC context response from the MME.
Gtpc Rx Fwd Reloc Cmp Ack	The total number of GTPC forward relocations complete ACK received from the MME.	Increments when the AMF receives the GTPC forward relocation complete ACK is received from the MME.
Gtpc Rx Fwd Reloc Req	The total number of GTPC forward relocation requests received from the MME.	Increments when the AMF receives the GTPC forward relocation request from the MME.
Gtpc Rx Fwd Reloc Rsp	The total number of GTPC forward relocation responses received from the MME.	Increments when the AMF receives the GTPC forward relocation response from the MME.
Gtpc Rx Identification Req	The total number of GTPC identification requests received from the MME.	Increments when the AMF receives the GTPC identification requests from the MME.
Gtpc Rx Identification Rsp	The total number of GTPC identification responses received from the MME.	Increments when the AMF receives the GTPC identification response from the MME.
Gtpc Rx Reloc Cancel Req	The total numbers of GTPC cancel requests received from the MME.	Increments when the AMF receives the GTPC cancel request from the MME.
Gtpc Rx Reloc Cancel Rsp	The total numbers of GTPC cancel response received from the MME.	Increments when the AMF receives the GTPC cancel response from the peer MME.
Gtpc Tx Context Ack	The total number of GTPC contexts ACK sent to the MME.	Increments when the AMF sends the GTPC context ACK to the MME.
Gtpc Tx Context Req	The total number of GTPC context requests sent to the MME.	Increments when the AMF sends the GTPC context request to the MME.
Gtpc Tx Context Rsp	The total number of GTPC context responses sent to the MME.	Increments when the AMF sends the GTPC context response to the MME.

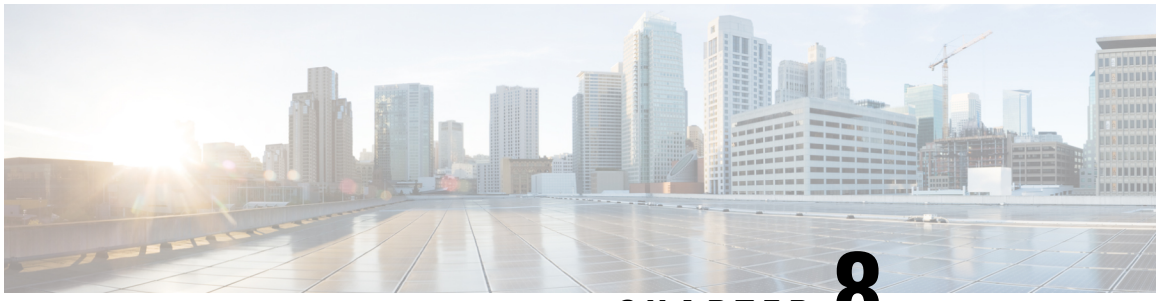
Name	Description	Trigger
Gtpc Tx Fwd Reloc Cmp Ack	The total number of GTPC forward relocations complete ACK sent to the MME.	Increments when the AMF sends the GTPC forward relocation complete ACK to the MME.
Gtpc Tx Fwd Reloc Cmp Notf	The total number of GTPC forward relocation complete notifications sent to the MME.	Increments when the AMF sends the GTPC forward relocation complete notification to the MME.
Gtpc Tx Fwd Reloc Req	The total number of GTPC forward relocation requests sent to the MME.	Increments when the AMF sends the GTPC forward relocation request to the MME.
Gtpc Tx Fwd Reloc Rsp	The total number of GTPC forward relocation responses sent to the MME.	Increments when the AMF sends the GTPC forward relocation response to the MME.
Gtpc Tx Identification Req	The total number of GTPC identification requests sent to the MME.	Increments when the AMF sends the GTPC identification request to the MME.
Gtpc Tx Reloc Cancel Req	The total numbers of GTPC cancel relocation requests sent to the MME.	Increments when the AMF sends the GTPC relocation cancel request to the MME.
Gtpc Tx Reloc Cancel Rsp	The total number of GTPC relocations cancel response sent to the MME.	Increments when the AMF sends the GTPC relocation cancel response to the MME.
Gtpc Tx Req	The total number of context requests or identification request failures towards the MME.	Increments when there's a failure in sending the GTPC context request or identification request, due to the peer MME not ready, or epsnas container not present, and so on.
Nas In Identity Response	The total number of identity responses received from the UE.	Increments when the AMF recieves an identity response from the UE.
Nas In Ue Deregistration Accept	The total number of network initiated deregistration received.	Increments when the network initiated deregistration is received.
Nas Out Identity Request Imei	The total number of identity requests with IMEI as matching value.	Increments when the IMEI-based identity request is sent.
Nas Out Identity Request Suci	The total number of identity requests with SUCI as matching value.	Increments when the SUCI-based identity request is sent.
Ngap Dl Handover Command Msg	The total number of handover commands sent to the source gNB.	Increments when the AMF sends the handover command to the source gNB.

Name	Description	Trigger
Ngap Dl Handover Preparation Failure Msg	The total number of handovers prepare failure sent by the AMF.	Increments when the AMF sends the handover preparation failure to the gNB.
Ngap Dl Handover Request Msg	The total number of handover request messages sent to the gNB.	Increments when the AMF sends the handover request message to the gNB.
Ngap Ul Handover Cancel Msg	The total numbers of handover cancel requests received from the gNB.	Increments when the AMF receives the handover cancel request from the gNB.
Ngap Ul Handover Request Ack Msg	The total number of handover ACK messages received by the AMF.	Increments when the AMF recieves the handover ACK message from the gNB.
Ngap Ul Handover Required Msg	The total number of handover required messages received by the AMF.	Increments when the AMF receives the handover required message from the gNB.
Smf Sm Ctxt Create Req	The total numbers of SMF SM context create request sent to the SMF.	Increments when the AMF sends the SM context create request to the SMF.
Smf Sm Ctxt Create Rsp	The total number of SM contexts create response received from the SMF.	Increments when the AMF receives the SM context create response from the SMF.
Smf Sm Ctxt Retrieve Req	The total number of SM contexts retrieve request sent to the SMF.	Increments when the AMF sends the message to retrieve the context.
Smf Sm Ctxt Update Req	The total number of SMF context updates request sent to the SMF.	Increments when the AMF sends the SM context update request to the SMF.
Smf Sm Ctxt Update Rsp	The total number of SM context update responses received for the update contexted data from the SMF.	Increments when the AMF receives the SM context update response from the SMF.
Udm Initiated Dereg Request	The total number of UDM initiated deregistration request received.	Increments when the AMF receives the UDM initiated deregistration request.
Udm Initiated Dereg Response	The total number of UDM initiated deregistration responses sent to the UDM.	Increments when the AMF sends the UDN-initiated deregistration responses to the SMF.

Bulk Statistics Support

The following are supported bulk statistics in AMF for Attempted, Success, and Failure scenarios:

- Registration
- All procedures and features



CHAPTER 8

AMF Rolling Software Upgrade

Feature Summary and Revision History

Summary Data

Table 18: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	

Revision History

Table 19: Revision History

Revision Details	Release
CDL 1.10.3 related updates.	2023.01.0
First introduced.	2022.01.0

Feature Description

The AMF consists of a three-tier architecture as the following:

- Protocol

- Service
- Session

Each tier from this list includes a set of microservices (pods) for a specific functionality. Within these tiers, a Kubernetes Cluster exists. It comprises K8s or Kubernetes nodes such as master node and worker node (which also includes OAM nodes).

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

The following is a list of 12 nodes in the AMF K8s cluster:

- Three master nodes
- Three OAM worker nodes
- Two protocol worker nodes
- Two service worker nodes
- Two session (data store) worker nodes

The K8s cluster supports the following nodes:

- OAM worker nodes—Hosts the Ops Center pods for configuration management and metrics pods for statistics and Key Performance Indicators (KPIs).
- Protocol worker nodes—Hosts the AMF protocol-related pods for the following interfaces:
  - Service-based interfaces (such as N8, N11, N12, N14, N15, NRF)
  - UDP-based protocol interfaces (such as N26)
- Service worker nodes—Hosts the AMF application-related pods that help in processing the perform session management.
- Session worker nodes—Hosts the database-related pods that store the data for the subscriber session.

Upgrading AMF

This section describes how to upgrade the rolling software for AMF.

Rolling Software Upgrade for AMF

The rolling software upgrade uses one of the following processes:

- Upgrading or migrating the build from an older version to a newer version
- Upgrading the patch for the required deployment set of application pods

For more information on the supported CDL versions, contact your Cisco account representative.

The applications must be available all the time, where:

- Any new version (or even multiple newer versions) is expected to get deployed with a new build version or patch.
- Any unstable deployment upgrade is reverted to a previous stable version.
- Rolling upgrade process gets activated with a zero downtime, by incrementally updating pod instances with new ones.

Note The rolling software upgrade is supported from an older version to a newer version within the same major release.

Prerequisites

The prerequisites for upgrading AMF must not have changes to the following functions:

- Set of features supported in the old and new builds
- Addition, deletion, or modification of the existing CLI behavior
- Interface changes within the peer or across the pods

Recommendations

The following is a list of recommendations:

- Configuration changes aren't recommended during the upgrade process.
- All the required configuration changes must be performed, when the upgrade process gets completed.

Failure Handling

It's recommended to use the manual process to downgrade the system to a previous healthy build. The following are some of the failure scenarios:

- Crash, pods deployment, and others during the processes
- New events or procedures after the successful upgrade

Rolling Software Upgrade Using the SMI Cluster Manager

The AMF software upgrade or in-service upgrade procedure uses the K8s rolling strategy to upgrade the pod images. The pods of a StatefulSet are upgraded sequentially to ensure that the ongoing process remains unaffected.

Initially, a rolling upgrade on a StatefulSet causes a single pod instance to terminate. A pod with an upgraded image replaces the terminated pod. This process continues until all the replicas of the StatefulSet are upgraded.

The terminating pods exit gracefully after completing all the ongoing processes. Other in-service pods continue to receive and process the traffic to provide a seamless software upgrade.

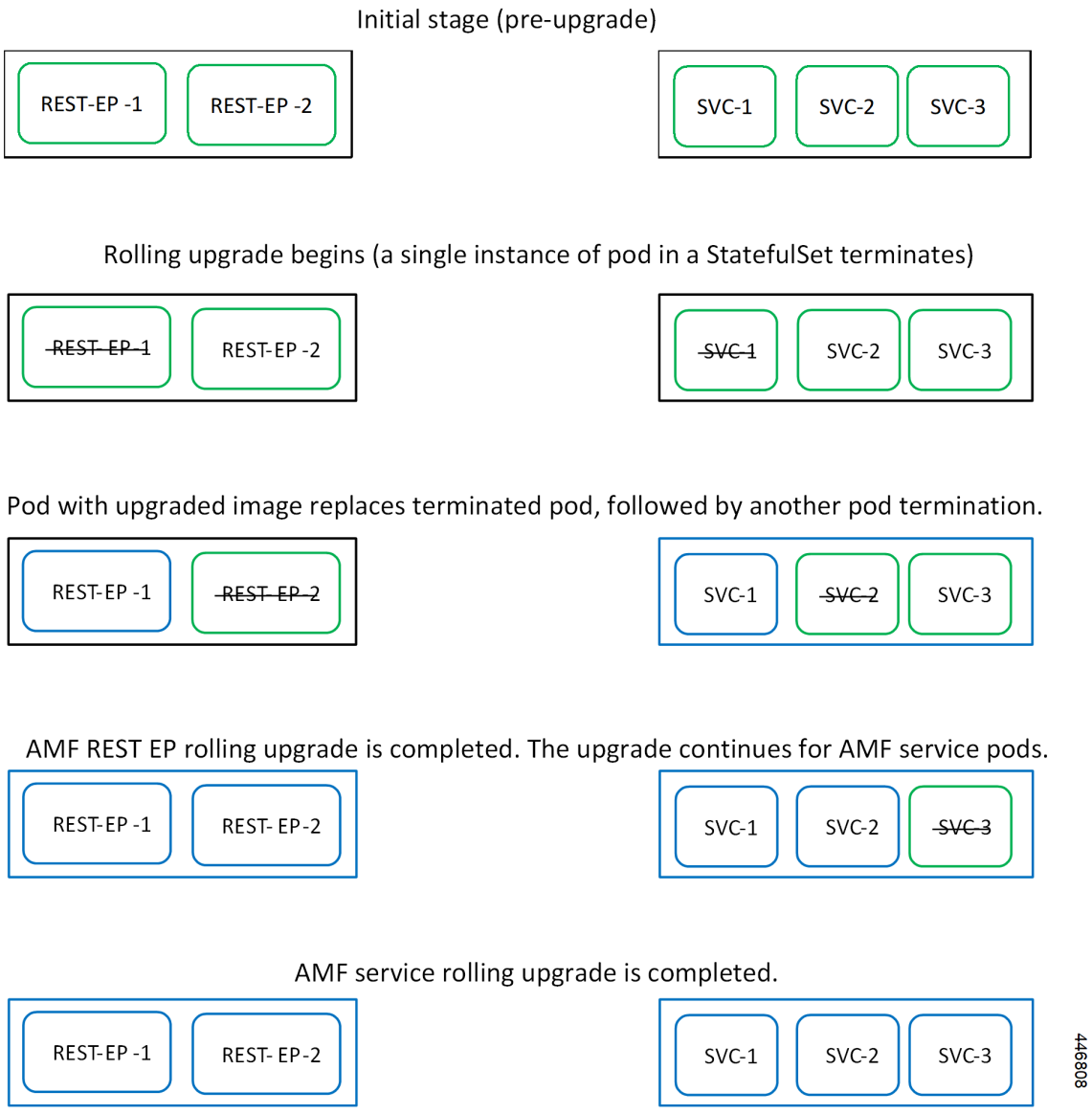
You can control the software upgrade process through the Ops Center CLI.

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

The following figure illustrates the following:

- The AMF rolling upgrade for AMF REST endpoint pods (two replicas) on protocol worker nodes
- Along with AMF service pods (three replicas) on service worker nodes

Figure 11: AMF Rolling Upgrade



Important ETCD v3.5.x does not support in-service downgrade to 3.4.x. If you're downgrading from 2023.04.0 builds to previous releases. perform system mode shutdown before downgrade.

Prerequisites

The following is a list of prerequisites for updating AMF:

- All the nodes that include all the pods in the node must be up and running.
- A patch version of the AMF software

Note Currently, major versions don’t support the rolling upgrade. The major version represents the release year, release number, and maintenance number. The version format is YYYY.RN.MN. For example: 2020.03.0

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

AMF Health Check

To perform a health check and to ensure that all the services are running, and nodes are in the ready state:

- Log on to the Master node.
- Use the following configuration:

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

Important Ensure that all the nodes are in the ready state before you proceed further. Use the command `kubectl get nodes` to display the node states.

Performing the Deployment File Back Up

Before upgrading, back up the configuration, logs, and deployment files.

To back up the deployment files, perform the following steps:

1. Log on to the SMI Cluster Manager Node as a Ubuntu user

2. Create a new directory for deployment.

   Example:

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

3. Move the `amf` deployment files into the newly created deployment directory.
4. Untar the `amf` deployment file.

   Example:

   ```
   test@smi1amf01-cm01:~/temp_08072019_T1651$ tar -xzvf amf.2020.01.0-1.SPA.tgz
   ./
   ./amf_REL_KEY-CCO_RELEASE.cer
   ./cisco_x509_verify_release.py
   ./amf.2020.01.0-1.tar
   ./amf.2020.01.0-1.tar.signature.SPA
   ./amf.2020.01.0-1.tar.SPA.README
   ```

5. Verify the downloaded image.

   Example:

   ```
   test@smi1amf01-cm01:~/temp_08072019_T1651$ cat amf.2020.01.0-1.tar.SPA.README
   ```

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

Performing the Ops Center Configuration Back Up

To back up the Ops Center configurations, perform the following steps:

1. Log on to SMI Cluster Manager node as an Ubuntu user
2. To back up the SMI Ops Center configuration to the `/home/ubuntu/smiops.backup` file, use the following command:

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

3. To back up the CEE Ops Center configuration to the `/home/ubuntu/ceeops.backup` file, use the following command:

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

4. To back up the AMF Ops Center configuration to the `/home/ubuntu/amfops.backup` file, use the following command:

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

Performing CEE Back Up and AMF Ops Center Configuration

To back up the CEE and AMF Ops Center configuration, perform the following steps:

1. Log on to the Master node as an Ubuntu user

2. Create a directory to back up the configuration files as the following:

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

3. Back up the AMF Ops Center configuration and verify the line count of the backup files as the following:

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

   Example:

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

4. Back up the CEE Ops Center configuration and verify the line count of the backup files as the following:

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

   Example:

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

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

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

   Example:

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

6. Verify the line count of the backup files.

   Example:

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

Staging a New AMF Image

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

To stage the new AMF image, perform the following steps:

1. Download and verify the new AMF image.
2. Log on to the SMI Cluster Manager node as an Ubuntu user
3. Copy the images to the `uploads` directory.

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

Note The SMI uses the new image present in the `uploads` directory to upgrade.

4. Verify whether the image is picked up by the SMI for processing from the `uploads` directory.

   sleep 30; ls /data/software/uploads

   Example:

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

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

   Example:

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

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

Triggering the Rolling Software Upgrade

AMF utilizes the SMI Cluster Manager to perform a rolling software upgrade.

To upgrade AMF using SMI Cluster Manager, use the following configuration procedures:

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

1. Log on to the SMI Cluster Manager Ops Center
2. Download the latest tarball from the URL, as the following:

   software-packages download *url*

   NOTES:

   - **software-packages download** *url*—Specify the software packages to be downloaded through HTTP/HTTPS.

   Example:

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

3. Verify whether the tarball is loaded.

   software-packages list

   NOTES:

   - **software-packages list**—Specify the list of available software packages.

   Example:

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

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

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

   ```
   config
     cluster cluster_name
      ops-centers app_name instance_name
          repository url
           exit
         exit
   ```

   NOTES:

   - **cluster** *cluster_name*—Specify the K8s cluster name.
   - **ops-centers** *app_name instance_name*—Specify the product Ops Center and instance.

     app_name is the application name.

     instance_name is the name of the AMF instance.
   - **repository** *url*—Specify the local registry URL for downloading the charts.

   Example:

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

5. Update the latest version of the product chart using the following command:

   clusters *cluster_name* **actions sync run**

   NOTES:

   - **actions**—Specify the actions performed on the cluster.
   - **sync run**—Triggers the cluster synchronization.

   Example:

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

Important

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

Monitoring the Upgrade

You can monitor the status of the upgrade through SMI Cluster Manager Ops Center.

To monitor the upgrade status, use the following configurations:

```
config
   clusters cluster_name actions sync run debug true
   clusters cluster_name actions sync logs
   monitor sync-logs cluster_name
   clusters cluster_name actions sync status
   exit
```

NOTES:

- **clusters** *cluster_name*—Specify the information about the nodes to be deployed. *cluster_name* is the name of the cluster.
- **actions**—Specify the actions performed on the cluster.
- **sync run**—Trigger the cluster synchronization.
- **sync logs**—Display the current cluster synchronization logs.
- **sync status**—Display the current status of the cluster synchronization.
- **debug true**—Enter the debug mode.
- **monitor sync logs**—Monitor the cluster synchronization process.

Example:

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

Important

You can view the pod details after the upgrade through the CEE Ops Center.

For more information on pod details, see Viewing the Pod Details, on page 83 section.

Viewing the Pod Details

You can view the details of the current pods through the CEE Ops Center.

To view the pod details, use the following command in the CEE Ops Center CLI:

cluster pods *instance_name pod_name* **detail**

NOTES:

- **cluster pods**—Specify the current pods in the cluster.
- *instance_name*—Specify the name of the instance.
- *pod_name*—Specify the name of the pod.
- **detail**—Display the details of the specified pod.

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

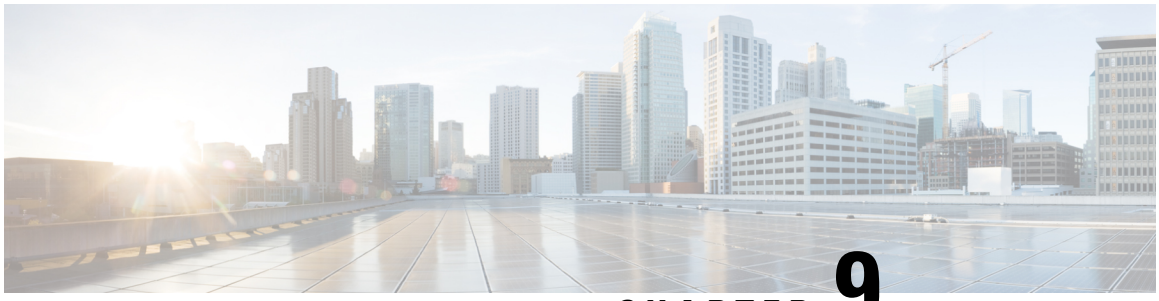
Example:

```
cluster pods amf-data alertmanager-0 detail
details apiVersion: "v1"
kind: "Pod"
metadata:
  annotations:
    alermanager.io/scrape: "true"
    cni.projectcalico.org/podIP: "<ipv4address/subnet>"
    config-hash: "5532425ef5fd02add051cb759730047390b1bce51da862d13597dbb38dfbde86"
  creationTimestamp: "2020-02-26T06:09:13Z"
  generateName: "alertmanager-"
  labels:
    component: "alertmanager"
    controller-revision-hash: "alertmanager-67cdb95f8b"
    statefulset.kubernetes.io/pod-name: "alertmanager-0"
  name: "alertmanager-0"
  namespace: "amf"
  ownerReferences:
  - apiVersion: "apps/v1"
    kind: "StatefulSet"
    blockOwnerDeletion: true
    controller: true
    name: "alertmanager"
    uid: "82a11da4-585e-11ea-bc06-0050569ca70e"
  resourceVersion: "1654031"
  selfLink: "/api/v1/namespaces/amf/pods/alertmanager-0"
  uid: "82aee5d0-585e-11ea-bc06-0050569ca70e"
spec:
  containers:
  - args:
    - "/alertmanager/alertmanager"
    - "--config.file=/etc/alertmanager/alertmanager.yml"
    - "--storage.path=/alertmanager/data"
    - "--cluster.advertise-address=$(POD_IP):6783"
    env:
    - name: "POD_IP"
      valueFrom:
        fieldRef:
          apiVersion: "v1"
          fieldPath: "status.podIP"
    image: "<path_to_docker_image>"
    imagePullPolicy: "IfNotPresent"
    name: "alertmanager"
```

```
    ports:
    - containerPort: 9093
      name: "web"
      protocol: "TCP"
    resources: {}
    terminationMessagePath: "/dev/termination-log"
    terminationMessagePolicy: "File"
    volumeMounts:
    - mountPath: "/etc/alertmanager/"
      name: "alertmanager-config"
    - mountPath: "/alertmanager/data/"
      name: "alertmanager-store"
    - mountPath: "/var/run/secrets/kubernetes.io/serviceaccount"
      name: "default-token-kbjnx"
      readOnly: true
  dnsPolicy: "ClusterFirst"
  enableServiceLinks: true
  hostname: "alertmanager-0"
  nodeName: "for-smi-cdl-1b-worker94d84de255"
  priority: 0
  restartPolicy: "Always"
  schedulerName: "default-scheduler"
  securityContext:
    fsGroup: 0
    runAsUser: 0
  serviceAccount: "default"
  serviceAccountName: "default"
  subdomain: "alertmanager-service"
  terminationGracePeriodSeconds: 30
  tolerations:
  - effect: "NoExecute"
    key: "node-role.kubernetes.io/oam"
    operator: "Equal"
    value: "true"
  - effect: "NoExecute"
    key: "node.kubernetes.io/not-ready"
    operator: "Exists"
    tolerationSeconds: 300
  - effect: "NoExecute"
    key: "node.kubernetes.io/unreachable"
    operator: "Exists"
    tolerationSeconds: 300
  volumes:
  - configMap:
      defaultMode: 420
      name: "alertmanager"
    name: "alertmanager-config"
  - emptyDir: {}
    name: "alertmanager-store"
  - name: "default-token-kbjnx"
    secret:
      defaultMode: 420
      secretName: "default-token-kbjnx"
status:
  conditions:
  - lastTransitionTime: "2020-02-26T06:09:02Z"
    status: "True"
    type: "Initialized"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "Ready"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "ContainersReady"
```

```
  - lastTransitionTime: "2020-02-26T06:09:13Z"
    status: "True"
    type: "PodScheduled"
  containerStatuses:
  - containerID: "docker://821ed1a272d37e3b4c4c9c1ec69b671a3c3fe6eb4b42108edf44709b9c698ccd"

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



CHAPTER 9

Application-based Alerts

Feature Summary and Revision History

Summary Data

Table 20: 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 21: 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

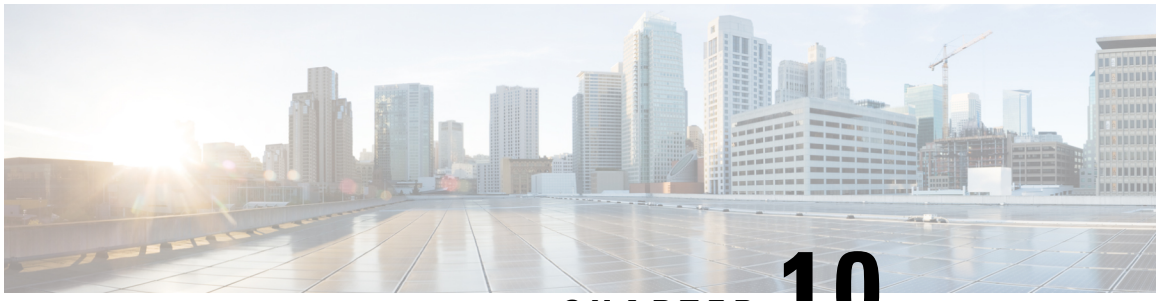
To configure alerts related to the N15 AM Policy Control Create Request, use the following configuration:

```
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 10

Attach Rate Throttling

Feature Summary and Revision History

Summary Data

Table 22: 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 23: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

Attach rate limit is the maximum number of new connections that AMF can process. The new connections include Initial Registration Request, Namf_Communication_CreateUEContext Request, and N26 Forward Relocation Request.

Setting the rate limit enables the operators to manage the traffic and reduce the signaling on the external nodes.

Note AMF does not throttle emergency, periodic, and mobility registration.

How it Works

This section describes how this feature works.

When you enable the attach rate throttling feature, AMF buffers and queues new connection requests (excluding Emergency Registration). The AMF prioritizes the processing of these requests in the FIFO (first in, first out) order.

If the queue is full, AMF drops or rejects packets with a cause code which is based on the configured action.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   amf-global
      network-protection-overload
         attach-rate
            rate-limit permitted_connection_count
            queue-size queue_size
            action
               drop
               initial-registration reject-with-cause { congestion |
protocol_error_unspecified }
               in14-create-ue-context reject-with-http-code {403}
               in26-fwd-reloc reject-with-cause { gtpc-entity-congestion
 | relocation-failure | no-resources-available }
               end
```

NOTES:

- **amf-global**—Enter the AMF global configuration mode.
- **attach-rate**—Configure the attach rate feature.
- **rate-limit** *permitted_connection_count*—Specify the number of new connections that AMF accepts per second. *permitted_connection_count* must be an integer in the range 50—5000.

- **queue-size** *queue_size*—Specify the size of queue that AMF uses for buffering the packets. AMF uses this queue when the new connection requests exceed the value that you have specified for **rate-limit**.

  queue_size must be an integer in the range 50—1000. The default *queue_size* is 50.

- **action**—Configure the action that AMF takes when the queue is full. The default action is Reject for all requests with #default reject cause.

  The following options are available for Action:

  - **drop**—Configure to drop all the new connection requests.
  - **initial-registration reject-with-cause { congestion | protocol_error_unspecified }**—Configure AMF to reject the UE-initiated Initial Registration Request with the one of the following causes in the reject message:
    - **congestion**—The message is congestion (22).
    - **protocol_error_unspecified**—The message is protocol_error_unspecified (111) #default.
  - **n14-create-ue-context reject-with-http-code {403}**—Configure AMF to reject the new Namf_Communication_CreateUEContext Request with the HTTP error code. The AMF receives this request in the source AMF during the UE-initiated inter-AMF N2 handover. With the error code as 403, the Cause attribute of the ProblemDetails is set to HANDOVER_FAILURE #default.
  - **n26-fwd-reloc reject-with-cause { gtpc-entity-congestion | relocation-failure | no-resources-available }**—Configure AMF to reject the new MME-initiated forward relocation requests through the N26 interface.

    If AMF rejects the inbound forward-relocation requests, it uses one of the following cause codes:

    - No resources available (73)
    - gtpc-entity-congestion (120)
    - relocation-failure (81) #default

Note

- AMF does not support dynamic change configuration.
- The configured rate-limit and queue-size are applied to each amf-service pod and not at the aggregation of all service pods.

Configuration Example

The following is an example configuration.

```
amf-global
network-protection-overload attach-rate
  rate-limit 100
  queue-size 100
  action
   initial-registration reject-with-cause congestion
   n14-create-ue-context reject-with-http-code 403
   n26-fwd-reloc reject-with-cause relocation-failure
```

```
  exit
exit
exit
amf-global
network-protection-overload attach-rate
  rate-limit 100
  queue-size 100
  action
   drop
  exit
exit
exit
```

OAM Support

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

Bulk Statistics Support

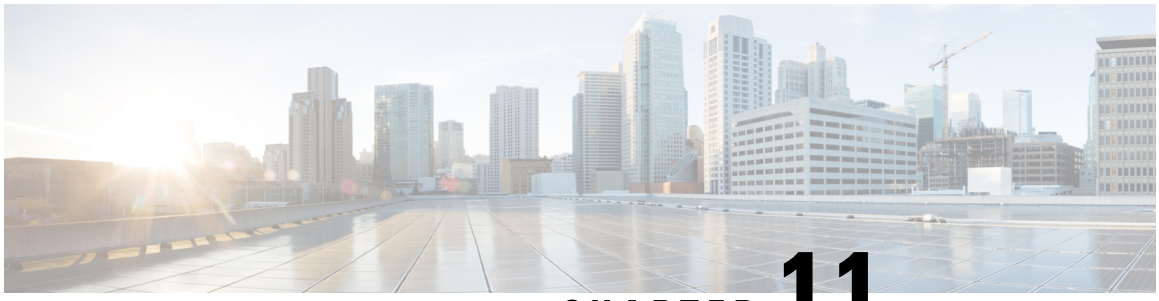
AMF supports the following statistics for the Attach Rate Throttling feature.

attach_rate_trottle

Description: The message-level statistics that AMF uses to reject or drop connection requests when the queue is full.

Labels:

- app_name
- message_type: GTPCFwdRelocReq, N14UeContextCreateReq, N1RegistrationRequest
- action: drop, reject



CHAPTER 11

Common Data Layer

Feature Summary and Revision History

Summary Data

Table 24: 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 25: 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 AMF.

The following are the two different deployment possibilities for CDL pods:

- CDL created locally in the same namespace as that of AMF namespace

- CDL created in a different namespace

Architecture

AMF consists of the following layers as part of the cloud native architecture:

- 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

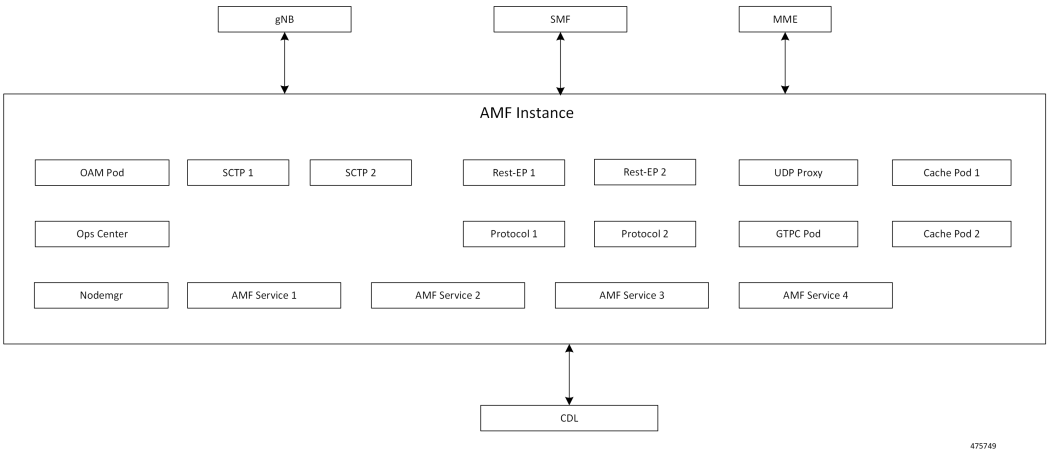
- Datastore Layer—Supports session storage

  Example: CDL

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

The following figure explains the architecture of AMF instance with separate namespace of CDL.

Figure 12: AMF Instance Architecture



The CDL is deployed as an independent entity which acts as a session store for AMF. The AMF instance performs the following:

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

- Provides instance ID by enhancing 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 105.
- 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 107.

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 example configuration:

```
cdl label-config session
   endpoint key key_value
   endpoint value endpoint_value
   slot map  no_of_slot_maps
      key key_value
      value value
   end
   index map map_number
      key key_value
      value value
   end
cdl logging default-log-level log_level
cdl datastore session
   cluster-id cluster_id
   label-config session
      slice-names cdl_slice_name
      endpoint replica replica_number
      index replica replica_number
      index map map_number
         index write-factor write_factor
      end
      slot replica replica_number
      slot map map_number
         slot write-factor write_factor
      end
   end
```

```
end
cdl kafka replica replica_number
cdl kafka storage storage_value
```

NOTES:

- **endpoint key** *key_value*—Specify the key for the endpoint configuration.
- **endpoint value** *endpoint_value*—Specify the value associated with the endpoint key.
- **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.
- **key** *key_value*—Specify the key for the slot map.
- **value** *value*—Specify the value associated with the slot map key.
- **index map** *map_number*—Specify the number of partitions to be created for index. Must be an integer in the range of 1–1024.
- **key** *key_value*—Specify the key for the index map.
- **value** *value*—Specify the value associated with the index map key.
- **cdl logging default-log-level** *log_level*—Specify the default logging level for the system.
- **cluster-id** *cluster_id*—Specify the the cluster ID for the datastore session.
- **slice-names** *cdl_slice_name*—Specify the CDL slice names. cdl_slice_name must be an alphanumeric string from 1 to 16 characters in length.
- **endpoint replica** *replica_number*—Specify the number of replicas to be created. The default value is 1. Must be an integer in the range of 1–16.
- **index replica** *no_of_replicas_per_map*—Specify the number of replicas to be created. The default value is 2. num_replica must be an integer in the range of 1–16.
- **index write-factor** *write_factor*—Specifythe number of copies to be written before successful response. The default value is 1. write_factor must be an integer in the range of 0–16.
- **slot replica** *replica_number*—Specify the number of replicas to be created. The default value is 1. num_replica must be an integer in the range of 1–16.
- **slot map** *map_number*—Specify the number of partitions in a slot. The default value is 1. num_map/shards must be an integer in the range of 1–1024.
- **slot write-factor** *write_factor*—Specify the number of copies to be written before successful response. The default value is 1. *write_factor* must be an integer in the range of 0–16. Make sure that the value is lower than or equal to the number of replicas..

Configuration Example

Use the `show running-config cdl` command to verify the configuration. The following is an example configuration in CDL Ops Center.

```
cdl label-config session
 endpoint key smi.cisco.com/node-type-4
 endpoint value cdl
 slot map 1
```

```
  key   smi.cisco.com/node-type-4
  value cdl
 exit
 slot map 2
  key   smi.cisco.com/node-type-4
  value cdl
 exit
 index map 1
  key   smi.cisco.com/node-type-4
  value cdl
 exit
exit
cdl logging default-log-level error
cdl datastore session
 cluster-id   1
 label-config session
 slice-names  [ 1 ]
 endpoint replica 2
 index replica 2
 index map    1
 index write-factor 1
 slot replica 2
 slot map     2
 slot write-factor 1
 slot notification dynamic-provisioning true
exit
cdl kafka replica 3
cdl kafka storage 1
```

Configuring the CDL in different namespace as AMF

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

```
cdl label-config session
   endpoint key key_value
   endpoint value endpoint_value
   slot map  no_of_slot_maps
      key key_value
      value value
   end
   index map map_number
      key key_value
      value value
   end
cdl logging default-log-level log_level
cdl datastore session
   cluster-id cluster_id
   label-config session
      slice-names cdl_slice_name
      endpoint replica replica_number
      index replica replica_number
      index map map_number
         index write-factor write_factor
      end
      slot replica replica_number
      slot map map_number
         slot write-factor write_factor
```

```
        slot notification dynamic-provisioning true
      end
    end
end
cdl kafka replica replica_number
cdl kafka storage storage_value
```

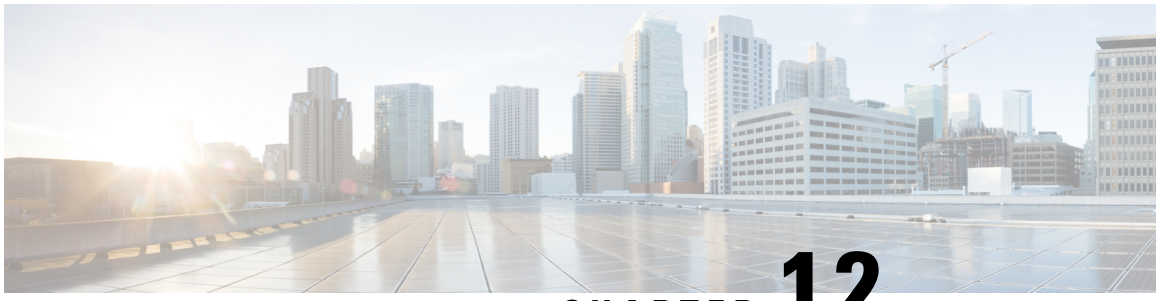
NOTES:

- **endpoint key** *key_value*—Specify the key for the endpoint configuration.
- **endpoint value** *endpoint_value*—Specify the value associated with the endpoint key.
- **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.
- **key** *key_value*—Specify the key for the slot map.
- **value** *value*—Specify the value associated with the slot map key.
- **index map** *map_number*—Specify the number of partitions to be created for index. Must be an integer in the range of 1–1024.
- **key** *key_value*—Specify the key for the index map.
- **value** *value*—Specify the value associated with the index map key.
- **cdl logging default-log-level** *log_level*—Specify the default logging level for the system.
- **cluster-id** *cluster_id*—Specify the the cluster ID for the datastore session.
- **slice-names** *cdl_slice_name*—Specify the CDL slice names. cdl_slice_name must be an alphanumeric string from 1 to 16 characters in length.
- **endpoint replica** *replica_number*—Specify the number of replicas to be created. The default value is 1. Must be an integer in the range of 1–16.
- **index replica** *no_of_replicas_per_map*—Specify the number of replicas to be created. The default value is 2. num_replica must be an integer in the range of 1–16.
- **index write-factor** *write_factor*—Specifythe number of copies to be written before successful response. The default value is 1. write_factor must be an integer in the range of 0–16.
- **slot replica** *replica_number*—Specify the number of replicas to be created. The default value is 1. num_replica must be an integer in the range of 1–16.
- **slot map** *map_number*—Specify the number of partitions in a slot. The default value is 1. num_map/shards must be an integer in the range of 1–1024.
- **slot write-factor** *write_factor*—Specify the number of copies to be written before successful response. The default value is 1. *write_factor* must be an integer in the range of 0–16. Make sure that the value is lower than or equal to the number of replicas..

Configuration Example

Use the `show running-config cdl` command to verify the configuration. The following is an example configuration in CDL Ops Center.

```
cdl label-config session
 endpoint key smi.cisco.com/node-type-4
 endpoint value cdl
 slot map 1
  key   smi.cisco.com/node-type-4
  value cdl
 exit
 slot map 2
  key   smi.cisco.com/node-type-4
  value cdl
 exit
 index map 1
  key   smi.cisco.com/node-type-4
  value cdl
 exit
exit
cdl logging default-log-level error
cdl datastore session
 cluster-id   1
 label-config session
 slice-names  [ 1 ]
 endpoint replica 2
 index replica 2
 index map    1
 index write-factor 1
 slot replica 2
 slot map     2
 slot write-factor 1
 slot notification dynamic-provisioning true
exit
cdl kafka replica 3
cdl kafka storage 1
```



CHAPTER 12

Collision Handling

Feature Summary

Summary Data

Table 26: Summary Data

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

Feature Description

The AMF interacts and supports multiple nodes. A few of the nodes are as the following:

- UE/GNB
- UDM
- AUSF
- SMF

When multiple nodes send simultaneous request towards the AMF, there's a possibility of collision at the AMF node.

The AMF collision handling feature supports handling the collision between different procedures at the AMF node.

How it Works

When a collision is detected, any of the following AMF collisions resolver-based procedures get activated:

- Aborts an ongoing procedure and performs peer node cleanup when required.
- Aborts an ongoing procedure and cleans locally without informing peer nodes.
- Discards an incoming message without responding and paving a way for its timeout.
- Allows both procedures to continue and execute one at a time in the FIFO manner.

Examples:

The following are a few examples:

1. The AMF receives a note of the UE-initiated deregistration process, while the initial registration procedure activity is still in progress.

   In this case, the AMF aborts the initial registration procedure locally, without informing peer nodes such as UDM, PCF, and so on.

2. The AMF receives a note of another initial registration process, while the current one is still in progress.

   In this case, the AMF aborts the older initial registration procedure, and performs the peer node cleanup activity, if required (such as the `AMPolicyControl_Delete` activity).

OAM Support

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

Bulk Statistics Support

The following statistics is used in the AMF collision handling.

amf_collision_stats

Description:

This set of statistics is used for tracking and debugging the AMF collision. The statistics include the name of the colliding procedure and the action taken by the collision resolver.

Sample Query:

```
amf_collision_stats{action_type="abort_proc1",
app_name="amf",cluster="clu001",data_center="sys001",
instance_id="0",proc1="UERegistration",
proc2="Deregistration",service_name="amf-service"} 1
```

When the AMF receives the De-Registration while the UE Registration procedure is in progress, the collision resolver aborts the registration procedure. It includes the names of two colliding procedures and collision resolver actions.

Labels:

- Label: **action_type**

  Label Description: Type of the action associated with the AMF collision statistics

  Example: **abort_proc1**

- Label: **app_name**

  Label Description: The name of the NF-app associated with the AMF collision statistics

  Example: **amf**

- Label: **cluster**

  Label Description: The name of the cluster associated with the AMF collision statistics

  Example: **clu001**

- Label: **data_center**

  Label Description: The name of the data center associated with the AMF collision statistics

  Example: **sys001**

- Label: **instance_id**

  Label Description: The instance ID associated with the AMF collision statistics

  Example: **0**

- Label: **proc1**

  Label Description: The procedure type associated with the AMF collision statistics This label refers as one of the procedures or as the primary procedure.

  Example: **UERegistration**

- Label: **proc2**

  Label Description: The procedure type associated with the AMF collision statistics This label refers as one of the procedures or as the secondary procedure.

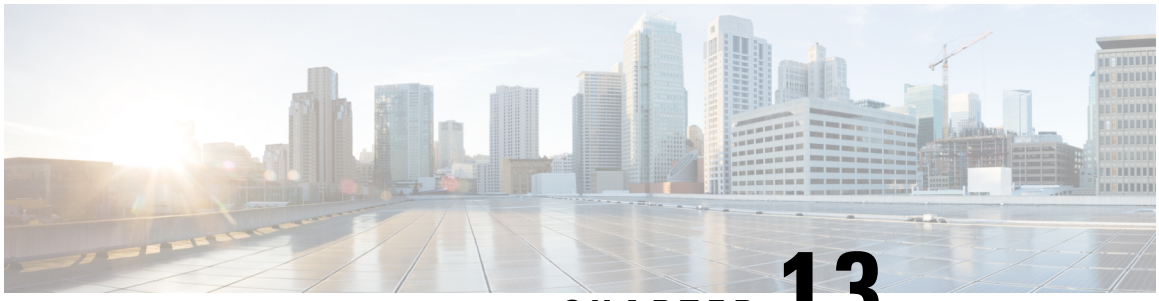
  Example: **Deregistration**

- Label: **service_name**

  Label Description: Name of the NF service associated with the AMF collision statistics

  Example: **amf-service**

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



CHAPTER 13

CMAS Service Support

Feature Summary and Revision History

Summary Data

Table 27: 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 28: 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, and Notification Call Flow

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

Figure 13: CMAS Subscription, Message Delivery, and Notification Call Flow

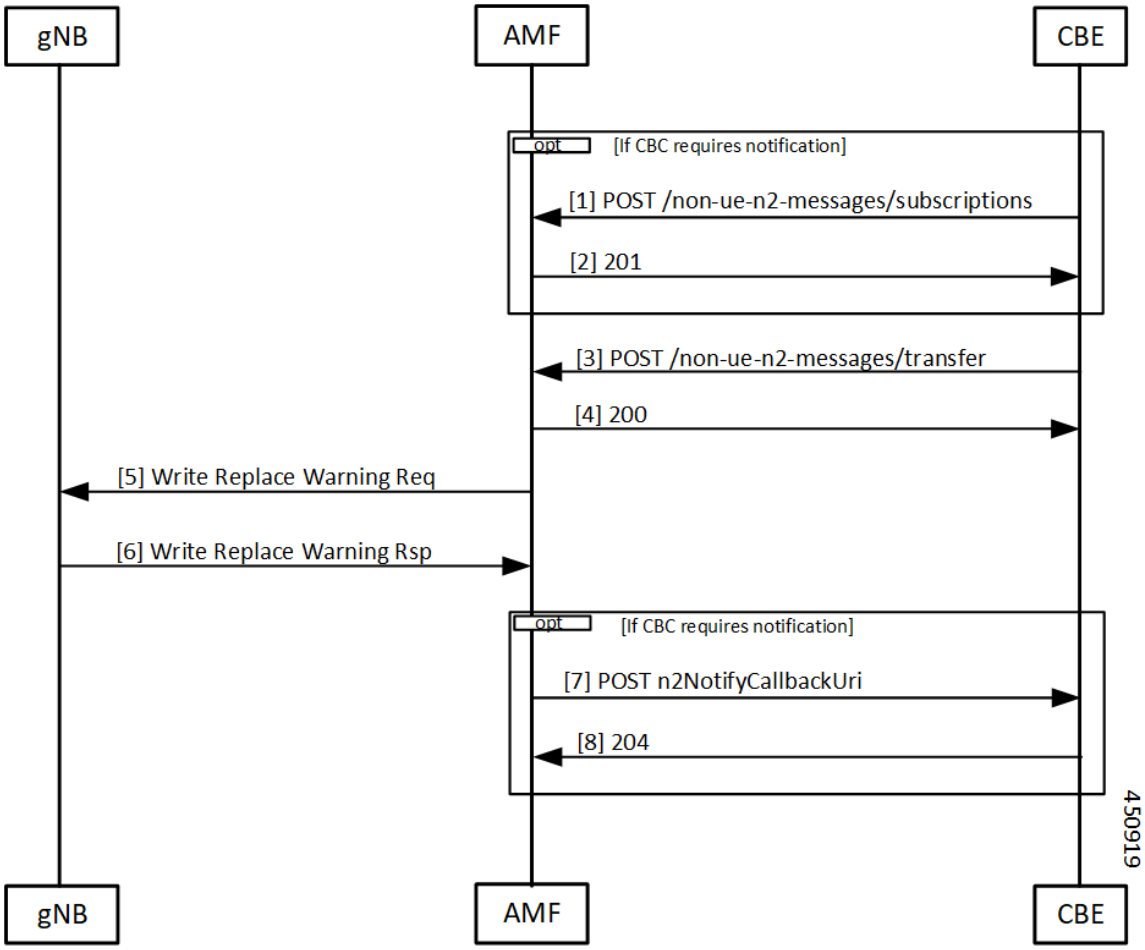


Table 29: CMAS Subscription, Message Delivery, and Notification Call Flow Description

Step	Description
1	The Cell Broadcast Center (CBC) creates and sends a NonUeN2InfoSubscribe to the AMF to be notified by the NG-RANs for the UE coverage of warning messages sent. The message type is the subscription parameter. The Cell Broadcase Entity (CBE) cannot subscribe 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 the following: • Message Identifier • Serial Number • List of NG-RAN TAIs • Warning Area List NG-RAN • 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 a list of TAI or a 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.
5	The AMF determines the set of gNB that need the message to send. This could be a list of gNB (if the CBCF sends the list), all gNB in a list of TAI, or all the gNB that are connected to the AMF. The AMF doesn't 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 multiple binary payloads are not allowed 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 14: Non-UE N2 Messages Subscription Call Flow

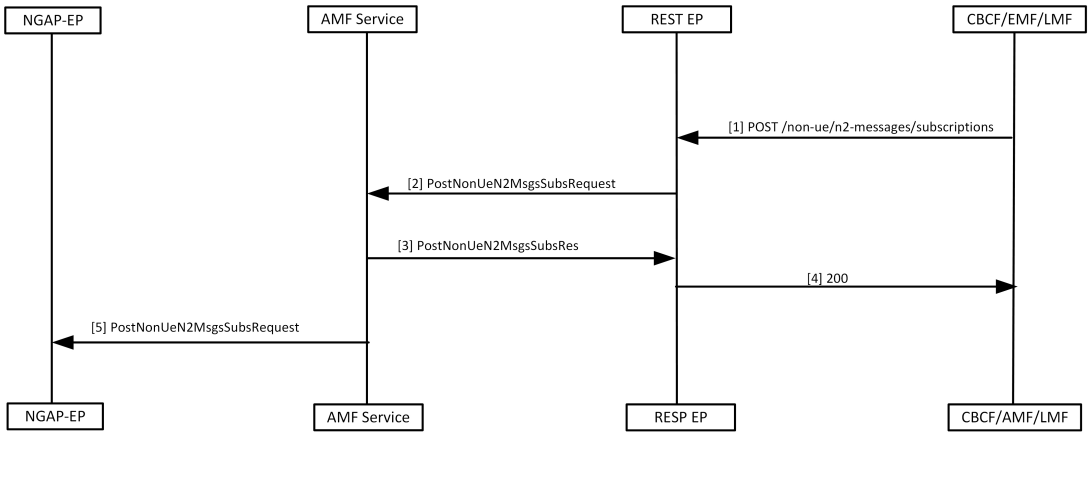


Table 30: Non-UE N2 Messages Subscription Call Flow Description

Step	Description
1	The 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 Canceled Area List) or PWS-RF (Restart Indication or Failure Indication).
2	The REST-EP forwards this message to the AMF service.
3	The AMF service saves the subscription to the database and sends a 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	The REST-EP responds with a 201 message to the peer node.
5	The 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 15: Non-UE N2 Messages Transfer Call Flow

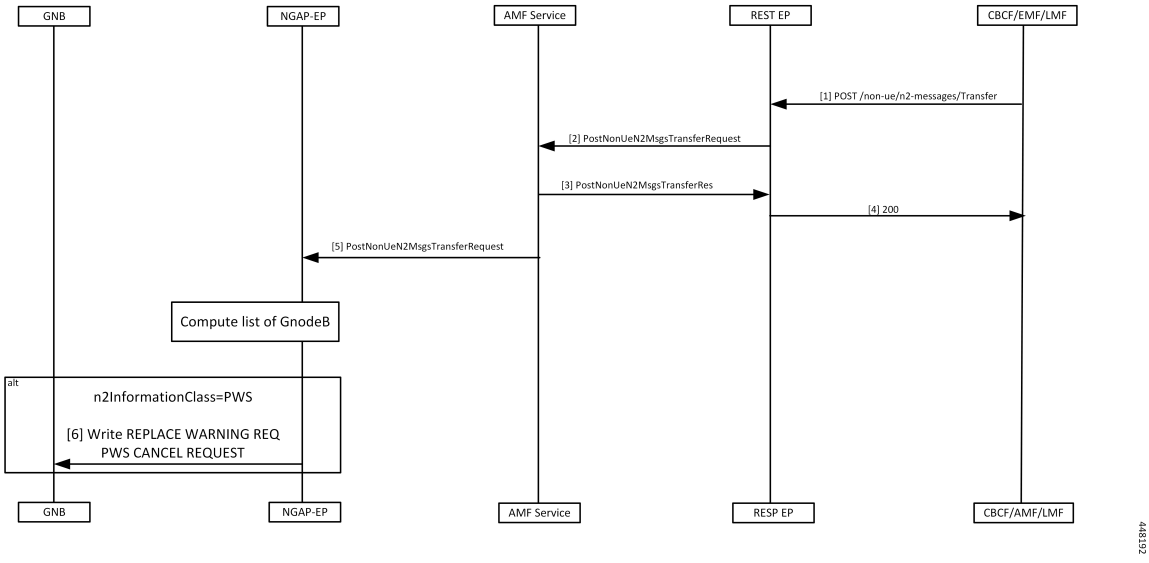


Table 31: Non-UE N2 Messages Transfer Call Flow Description

Step	Description
1	The peer node sends a NonUEN2MsgeTransferRequest to the AMF. The REST-EP receives this request and forwards the message to the AMF service.
2	AMF does the following while handling the warning messages (these messages may contain filters, for example, gNB or TAIs that must match): • On receiving the warning message, AMF service checks for protocol errors and returns error response, if there is any. • If the warning message contains filters, the AMF forwards the message to all NG-RANS that match the filters. • If the warning message doesn't contain filters, the AMF forwards the message to all NG-RANs connected to this AMF. • If the warning message contains filters but no matching NG-RANs, the AMF doesn't send any message.
3	The AMF sends NonUEN2MsgeTransferResponce to the REST-EP. • The AMF saves PWS messages to obtain correlation in responses, if the CBCF requests the responses to be send.
4	The REST-EP sends the response to the peer that sent the request.
5	The AMF service forwards the NonUEN2MsgeTransferRequest to the NGAP-EP. The NGAP-EP uses the parameters of the request to find the list of gNodeB to send these messages.

Step	Description

6	The NGAP-EP forwards the message to gNB with the following scenarios:
	• The NGAP copies the N2 payload without any changes and forwards it to the gNB, when the message has the N2InformationClass set to PWS.
	• The AMF performs the following actions, when the sendRanResp field in PWS information is set to true.
	  • Saves the msgIdentifier and the 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 16: Non-UE Message Notification Call Flow

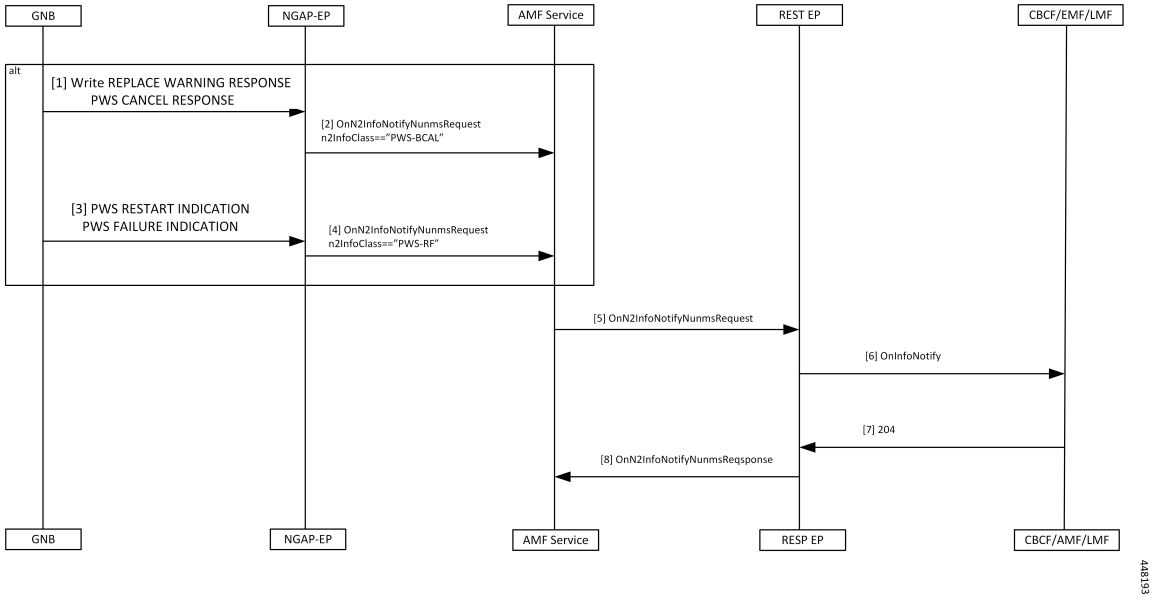


Table 32: Non-UE Message Notification Call Flow description

Step	Description
1	The gNB sends a Write Replace Warning Response or PWS Cancel Response to NGAP-EP.
2	The 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.

Step	Description
4	If there's a subscription for notification of the PWS events, the NGAP-EP generates a callback with n2InfoClass set to PWS-RF.
5	The AMF service forwards the onN2InfoNotifyRequest to REST-EP.
6	The REST-EP sends the message to the peer node.
7	The peer node responds with a 204 OK.
8	The REST-EP forwards the onN2InfoNotifyResponse to the AMF.

Non-UE Notification Subscription Deletion Call Flow

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

On receiving the non-UE events notification in the AMF, the existing subscription gets deleted.

Figure 17: Non-UE-Notification Subscription Deletion Call Flow

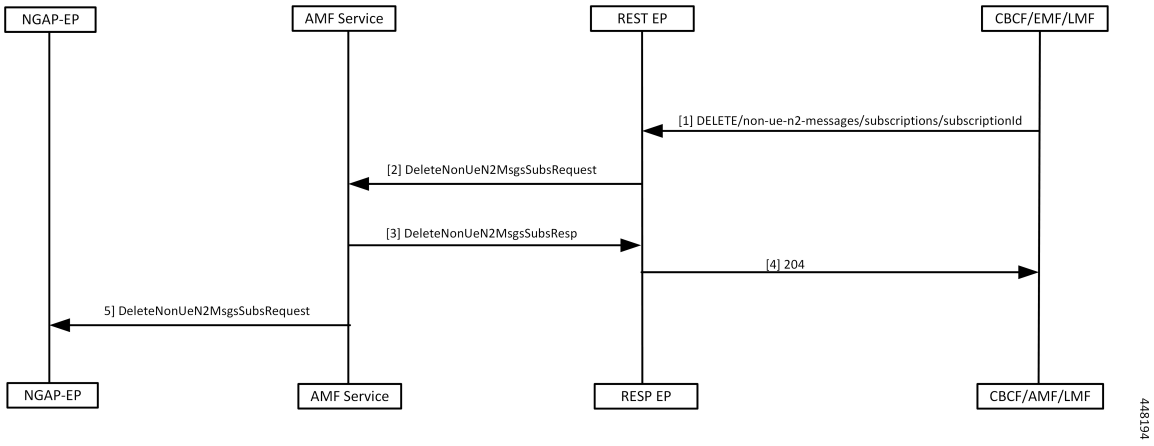
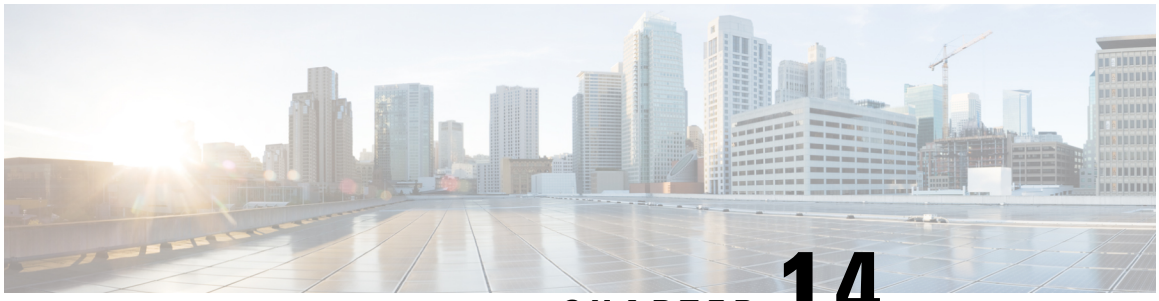


Table 33: Non-UE Notification Subscription Deletion Call Flow Description

Step	Description
1	The peer node sends a Delete message to the AMF with the ID assigned during the subscription process .
2	The REST-EP forwards the request to the AMF service.
3	The AMF service deletes the subscription information from the database before sending the response to the REST-EP.
4	The REST-EP forwards the response as 204 to the peer node.
5	The AMF service sends the request to NGAP-EP to remove the existing subscription from the NGAP-EP.



CHAPTER 14

Compliance to 3GPP Specifications

Feature Summary and Revision History

Summary Data

Table 34: 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 35: Revision History

Revision Details	Release
First introduced.	2021.04.0

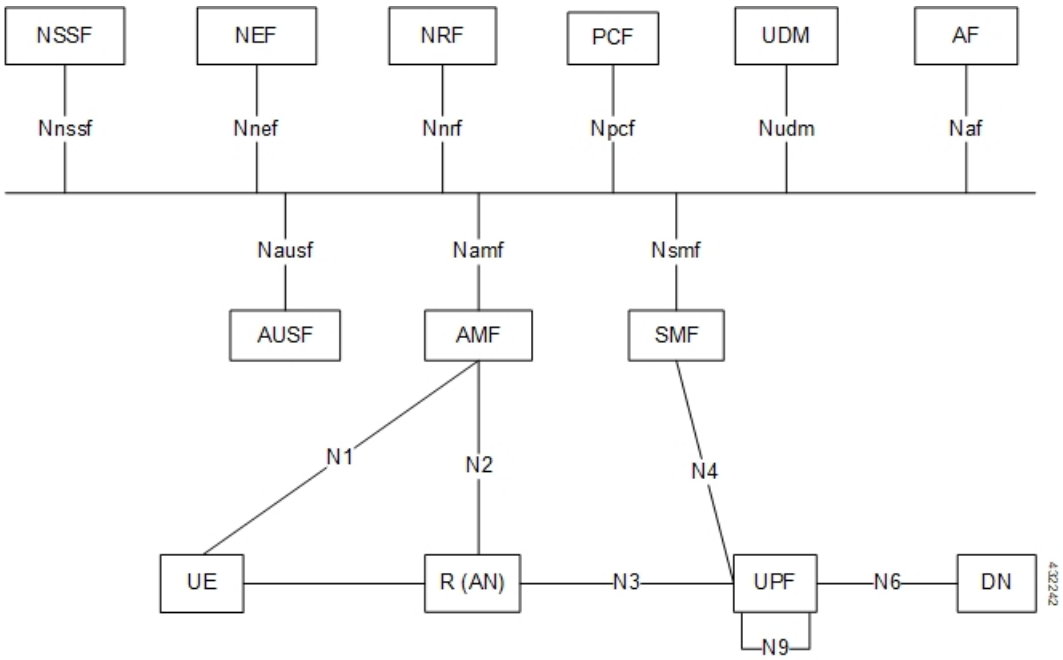
Feature Description

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 17.

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 18: Initial Registration Request Call Flow

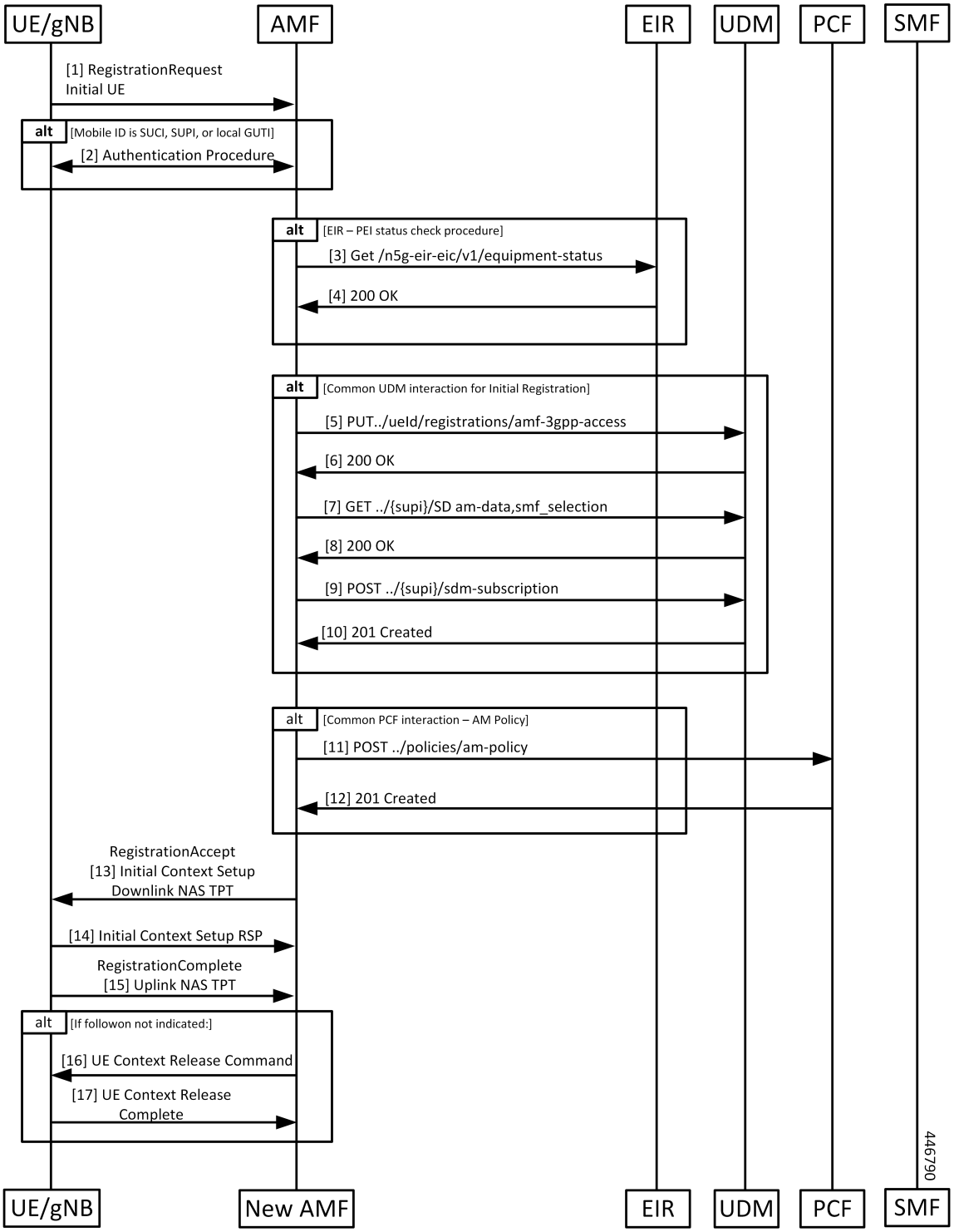


Table 36: Initial Registration Request Call Flow Description

Step	Description
1	An UE which wants to register itself with the 5G core sends a Registration-Request N1 message towards AMF with the following 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, or GUTI allocated by this AMF, the AMF authenticates the UE as presented in the authentication procedure.
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 exit 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.

Step	Description
10	The UDM registers the AMF and responds to the AMF.
11	The 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 the integrity check passes and PCF subscription data already exit 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 an Initial Context Setup Request, the gNB responds with an 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 without AMF Change Call Flow

This section describes the Mobility Updating or Periodic Registration without AMF Change call flow.

Figure 19: Mobility Updating or Periodic Registration without AMF Change Call Flow

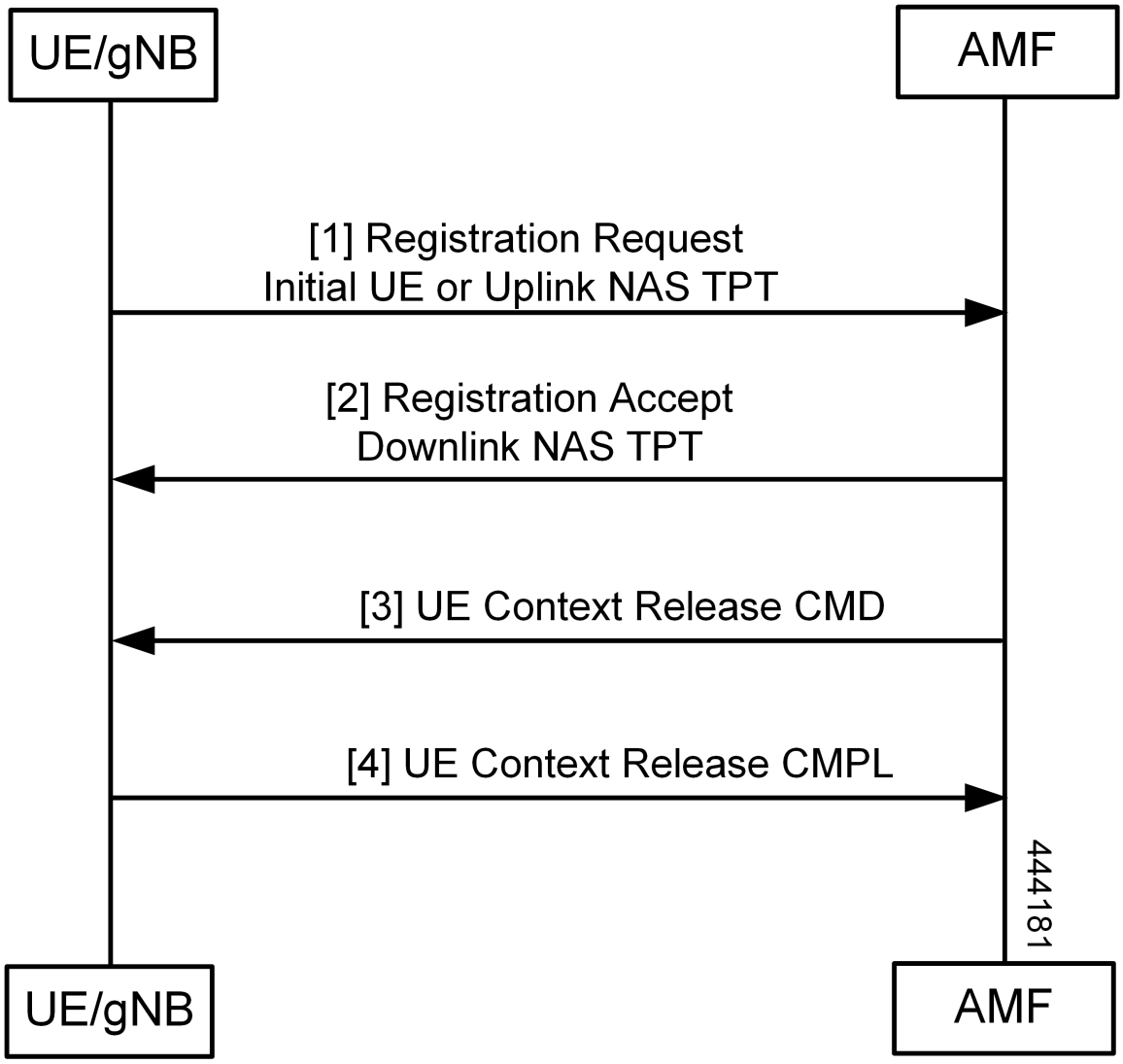


Table 37: Mobility Updating or Periodic Registration without AMF Change Call Flow Description

Step	Description
1	The UE triggers the Mobility Updating or Periodic Registration 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 doesn't 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.

The UE receives data services through a PDU session, which is a logical connection between the UE and core network.

During the 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 the service is needed.

Figure 20: PDU Session Establishment Call Flow

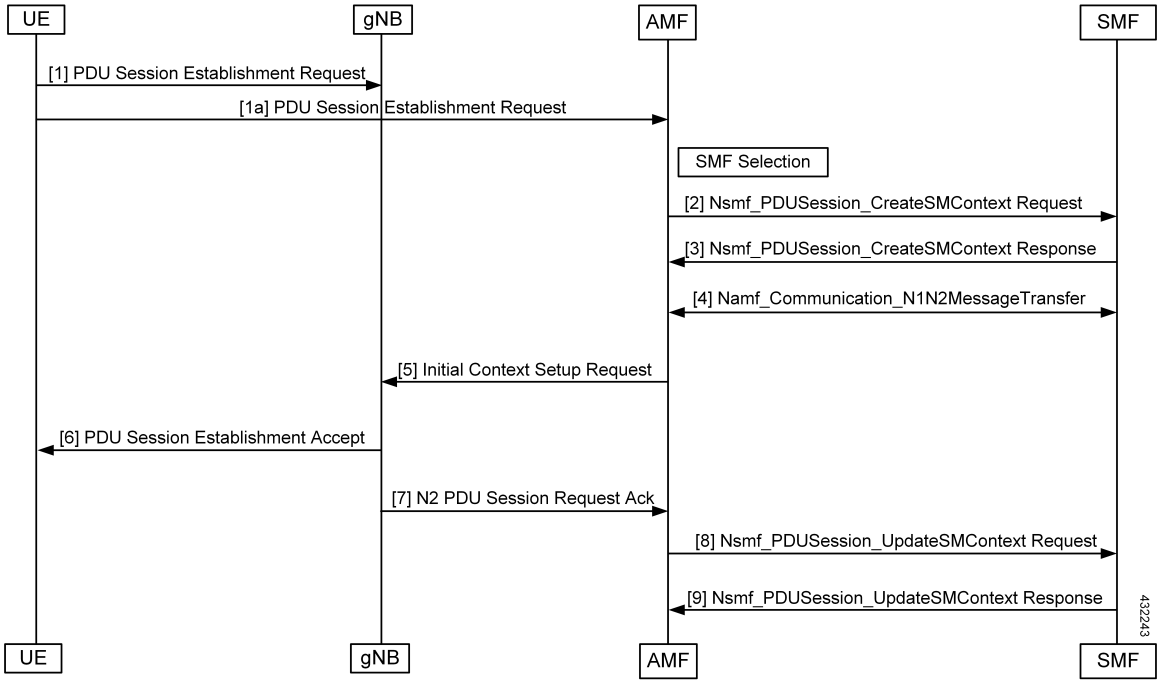


Table 38: PDU Session Establishment Call Flow Description

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, Requested SSC mode, 5GSM Capability PCO, SM PDU DN Request Container, and 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, single or multiple S-NSSAIs, 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. The AMF-service stickiness is maintained for the subscriber for the PDU establishment transaction.
3	The 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)).
4	The SMF sends Namf_Communication_N1N2MessageTransfer to the 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.

Step	Description
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	The RAN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) to the UE.
7	The gNB sends the N2 PDU Session Request Ack to the AMF. The N2 PDU Session Response included 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	The AMF sends the Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type) to the SMF. The AMF forwards the N2 SM information received from the RAN to the SMF.
9	The SMF sends the Nsmf_PDUSession_UpdateSMContext Response to the AMF.

PDU Session Establishment with Initial Context Call Flow

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

Figure 21: PDU Session Establishment with Initial Context Call Flow

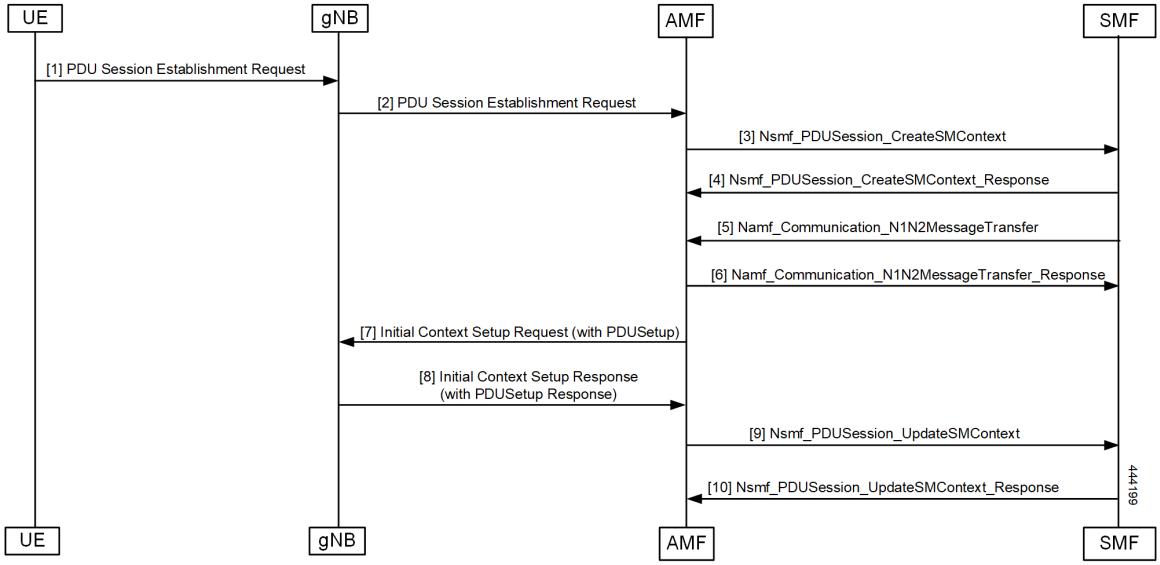


Table 39: PDU Session Establishment for Existing PDU Call Flow Description

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 the following: • PDU session ID • Requested PDU Session Type • Requested SSC mode • 5GSM Capability PCO • SM PDU DN Request Container • Number of Packet Filters
2,3,4	If the 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. The AMF invokes the Nsmf_PDUSession_CreateSMContext Request towards SMF with SUPI, DNN, S-NSSAIs, 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. The AMF service stickiness is maintained for the subscriber for the PDU establishment transaction. The 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)). The SMF sends Namf_Communication_N1N2MessageTransfer to the AMF. The N2 SM information carries information that the AMF forwards 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. The SMF receives Namf_Communication_N1N2MessageTransfer response from the AMF.
7	The gNB sends the Initial Context Setup Request to the AMF. The RAN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) to the UE.
8	The AMF responds with the Initial Context Setup Response to the gNB. The response includes the 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)).

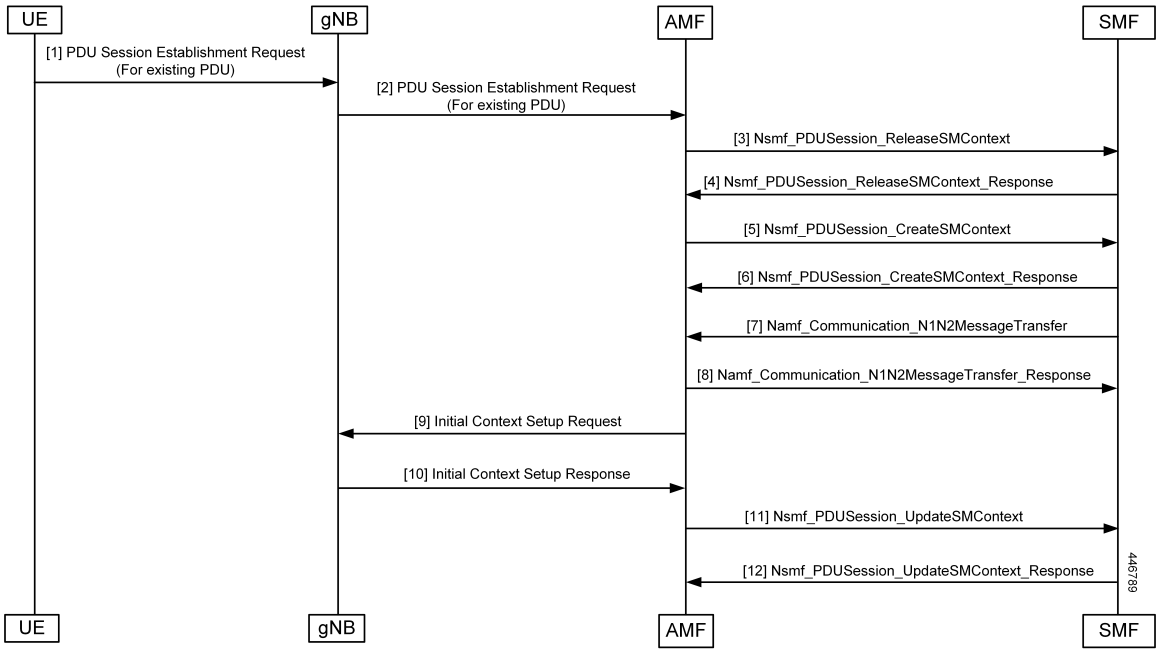
Step	Description
9	The AMF sends Nsmf_PDUSession_UpdateSMContext Request to the SMF The Nsmf_PDUSession_UpdateSMContext Request includes the N2 SM information and Request Type. The AMF forwards the N2 SM information received from RAN to the SMF.
10	The SMF sends the Nsmf_PDUSession_UpdateSMContext Response to the AMF.

PDU Session Establishment for Existing PDU Call Flow

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

If the UE starts the PDU Establishment Request for an existing PDU, the AMF performs local PDU release and sends the PDU release to SMF. It also initiates PDU Resource Setup Request. If the PDU release fails at SMF, the AMF sends the PDU reject.

Figure 22: PDU Session Establishment for Existing PDU Call Flow



The UE receives data services through a PDU session, which is a logical connection between the UE and the core network. The 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 40: 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 starts 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 the following: • PDU session ID • Requested PDU Session Type • 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 Session Establishment procedure is performed.
5	The AMF selects SMF based on slice-info and plmn-info provided by UE. The SMF is selected by NRF query or static configuration. The AMF invokes the Nsmf_PDUSession_CreateSMContext Request towards the SMF with SUPI, DNN, S-NSSAIs, 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, and DNN Selection Mode. The subscriber data store is modified to store the PDU information. The AMF service stickiness is maintained for the subscriber for the PDU establishment transaction.
6	The 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)).
7	The SMF sends Namf_Communication_N1N2MessageTransfer to AMF. The N2 SM information carries information that the AMF forwards 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 the Initial Context Setup is incomplete, the AMF sends the NAS message information as a part of the Initial Context Setup Request.
9	The AMF sends the Initial Context Setup Request to the gNB. The RAN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) to the UE.

Step	Description
10	The gNB sends the Initial Context Setup Response to the AMF with the N2 PDU Session Response (PDU Session ID, Cause, N2 SM information (PDU Session ID, AN Tunnel Info, List of accepted or rejected QFIs, User Plane Enforcement Policy Notification)).
11	The AMF forwards the N2 SM information received from RAN to the SMF. The Nsmf_PDUSession_UpdateSMContext Request includes the N2 SM information and Request Type.
12	The SMF responds with the Nsmf_PDUSession_UpdateSMContext_Response to the AMF.

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. The 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.

The 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 23: UE-Initiated PDU Session Modification Call Flow

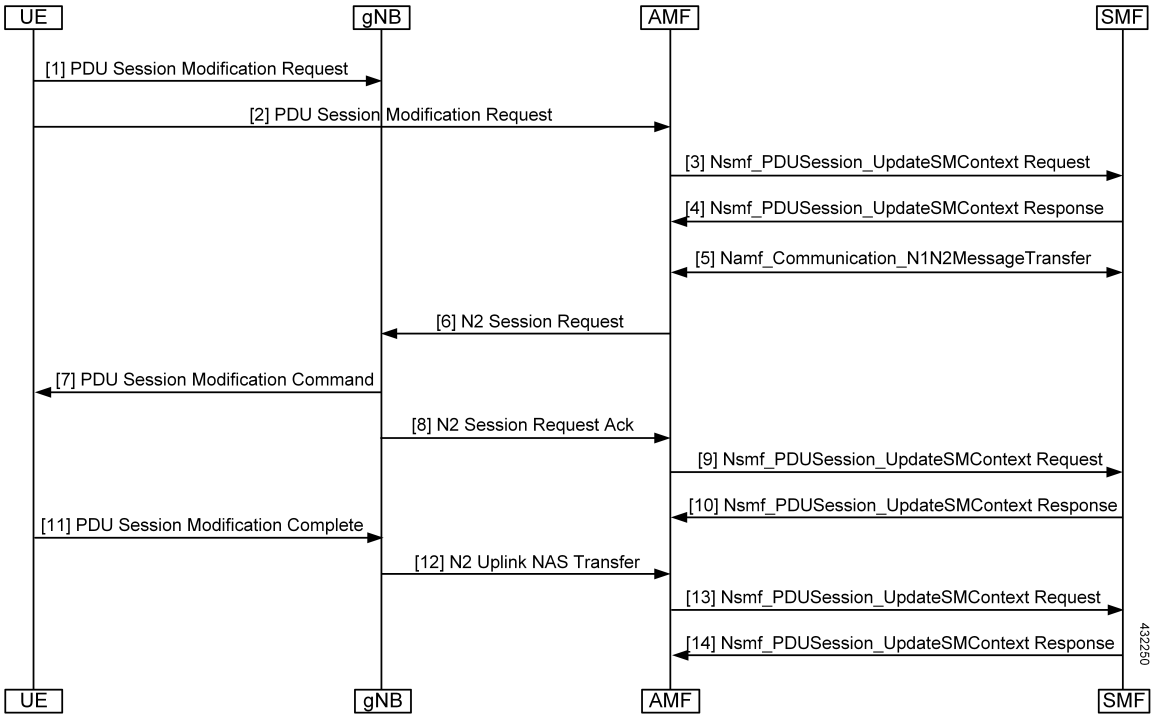


Table 41: UE-Initiated PDU Session Modification Call Flow Description

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)), and PDU Session ID) message. The AMF invokes the Nsmf_PDUSession_UpdateSMContext Request towards the 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 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, and 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.
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 through 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 through 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.

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

Figure 24: SMF-Initiated PDU Session Modification Call Flow

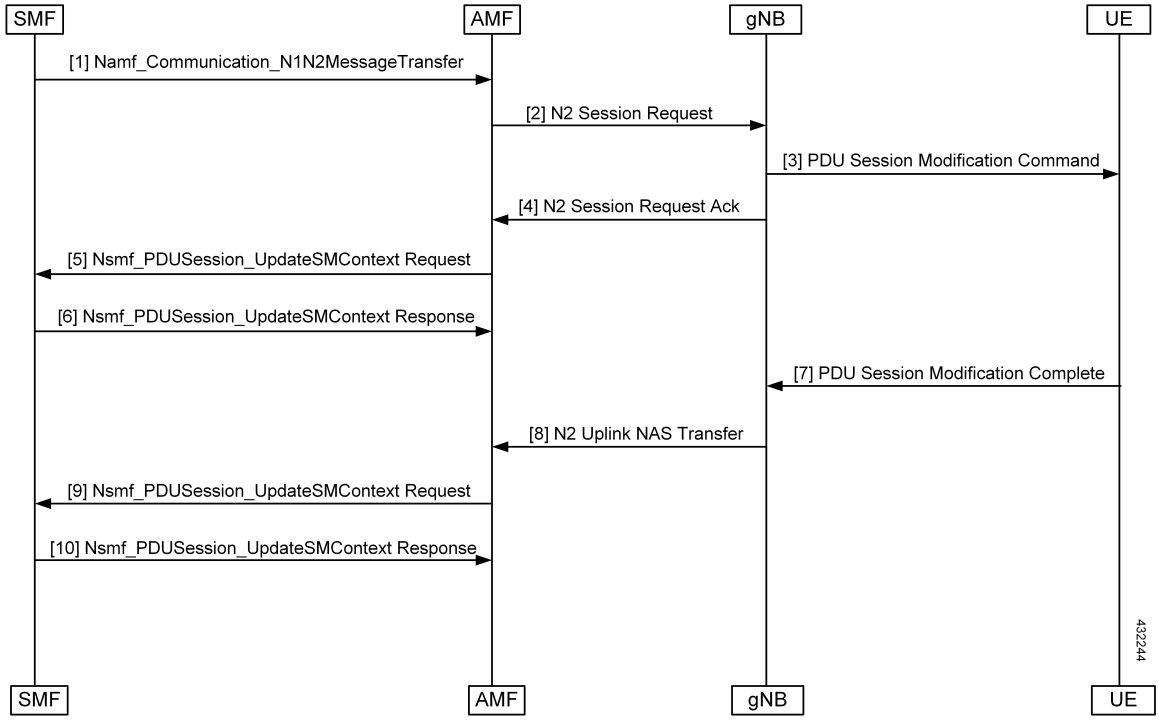


Table 42: SMF-Initiated PDU Session Modification Call Flow Description

Step	Description
1	The SMF starts the 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 the 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.

Step	Description
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 through 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 one or more QoS Flows associated with one or more QoS rules 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 through 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 25: UE-Initiated PDU Session Release Call Flow

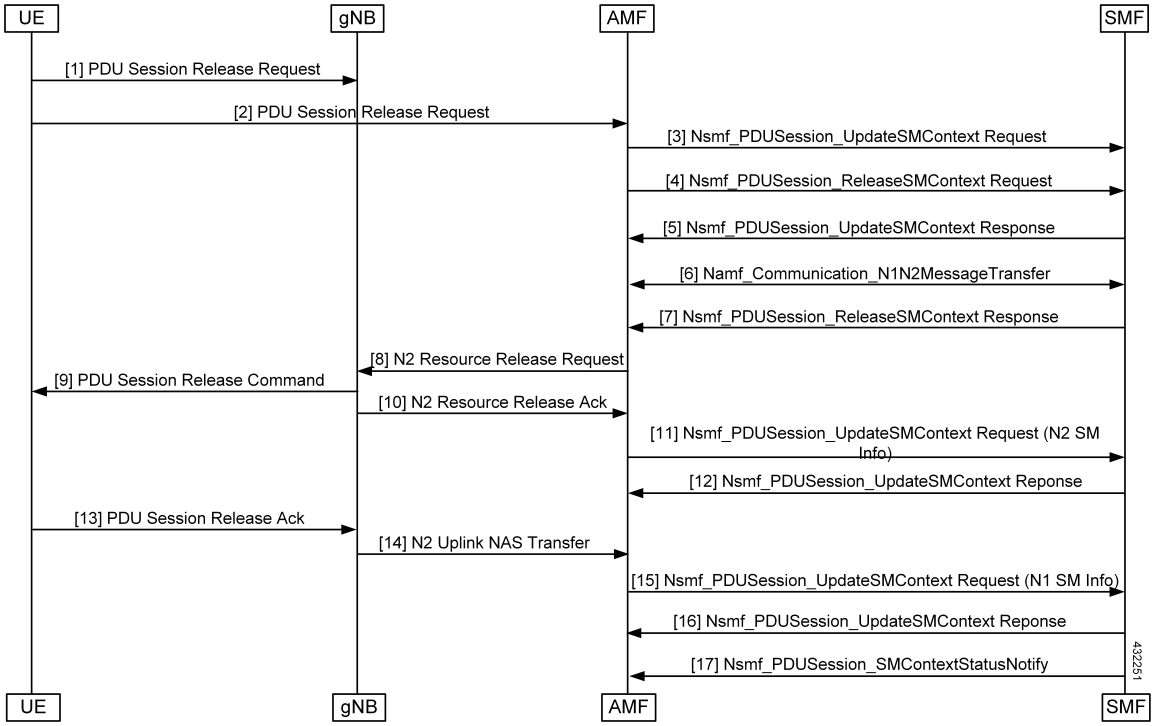


Table 43: UE-Initiated PDU Session Release Call Flow Description

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 through 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)).
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	The SMF responds to the AMF with the Nsmf_PDUSession_ReleaseSMContext response.

Step	Description
8	The 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 exchanges with the UE to release the corresponding AN resources.
10	The 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, and S-NSSAI.

SMF-Initiated PDU Release Call Flow

This section describes the SMF-Initiated PDU Release call flow.

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

Figure 26: SMF-Initiated PDU Release Call Flow

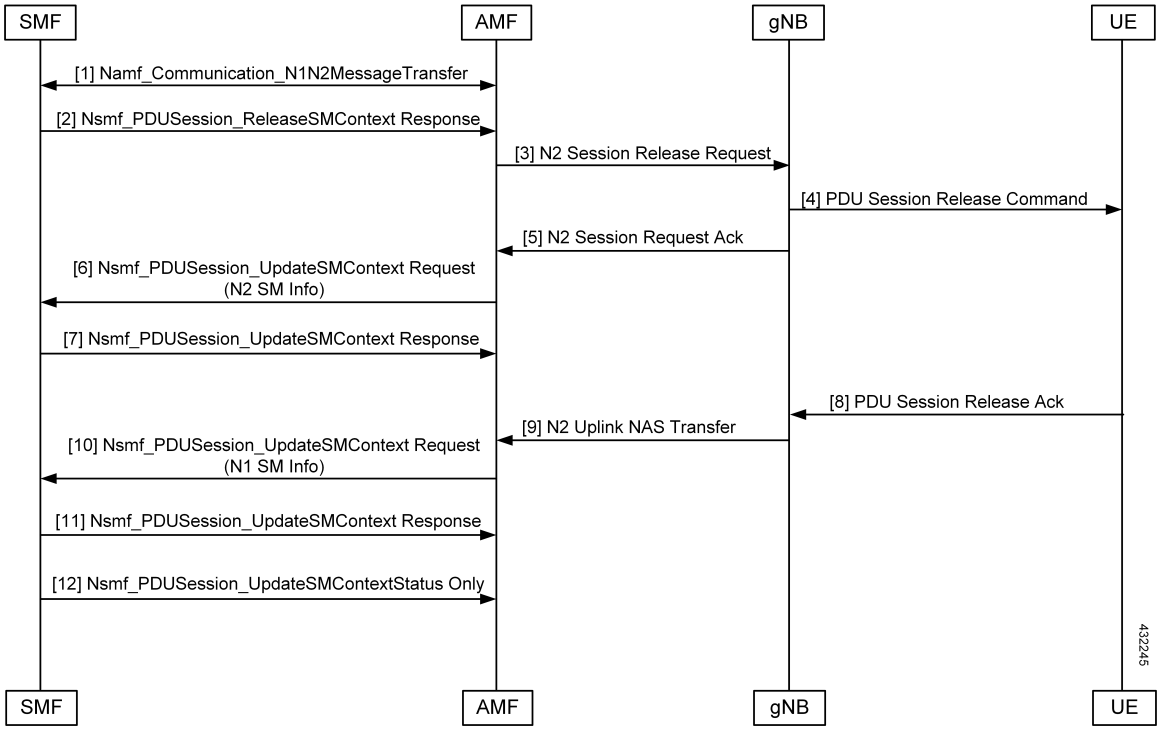


Table 44: SMF-Initiated PDU Release Call Flow Description

Step	Description
1	If the UP connection of the PDU session is active, the SMF includes the N2 Resource Release Request (PDU Session ID) in the Namf_Communication_N1N2MessageTransfer, to release the RAN resources associated with the PDU session.
2	The SMF responds to the AMF with the Nsmf_PDUSession_ReleaseSMContext response.
3	The 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 exchanges with the UE to release the corresponding AN resources.
5	The 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, and 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 27: UE-Initiated Deregistration Call Flow

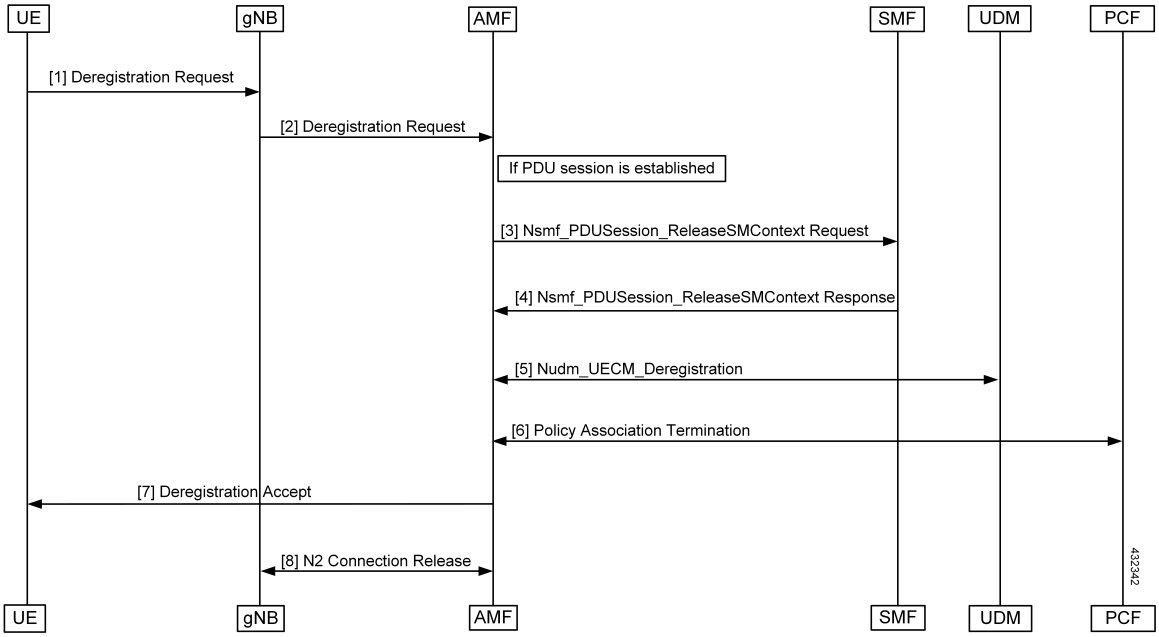


Table 45: UE-Initiated Deregistration Call Flow Description

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

Step	Description
3	If the PDU session has been established, the AMF sends Nsmf_PDUSession_ReleaseSMContext (SUPI and PDU Session ID) to SMF. All the 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 or 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	The gNB exchanges the N2 UE Context Release with the AMF.

UDM-Initiated Deregistration Call Flow

This section describes the UDM-Initiated Deregistration call flow.

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

Figure 28: UDM-Initiated Deregistration Call Flow

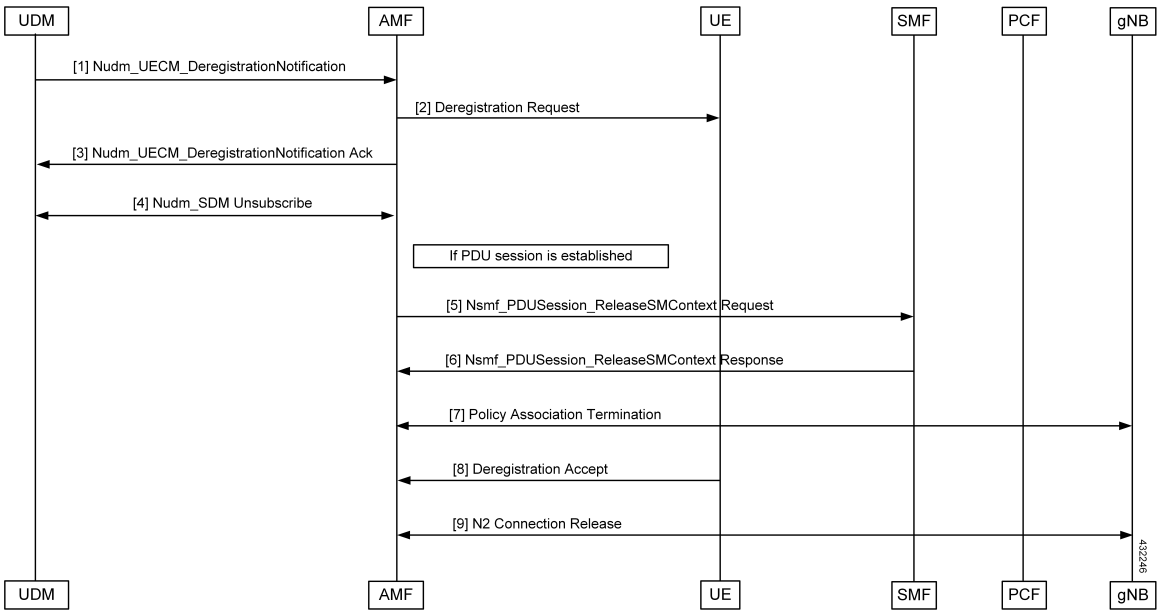


Table 46: UDM-Initiated Deregistration Call Flow Description

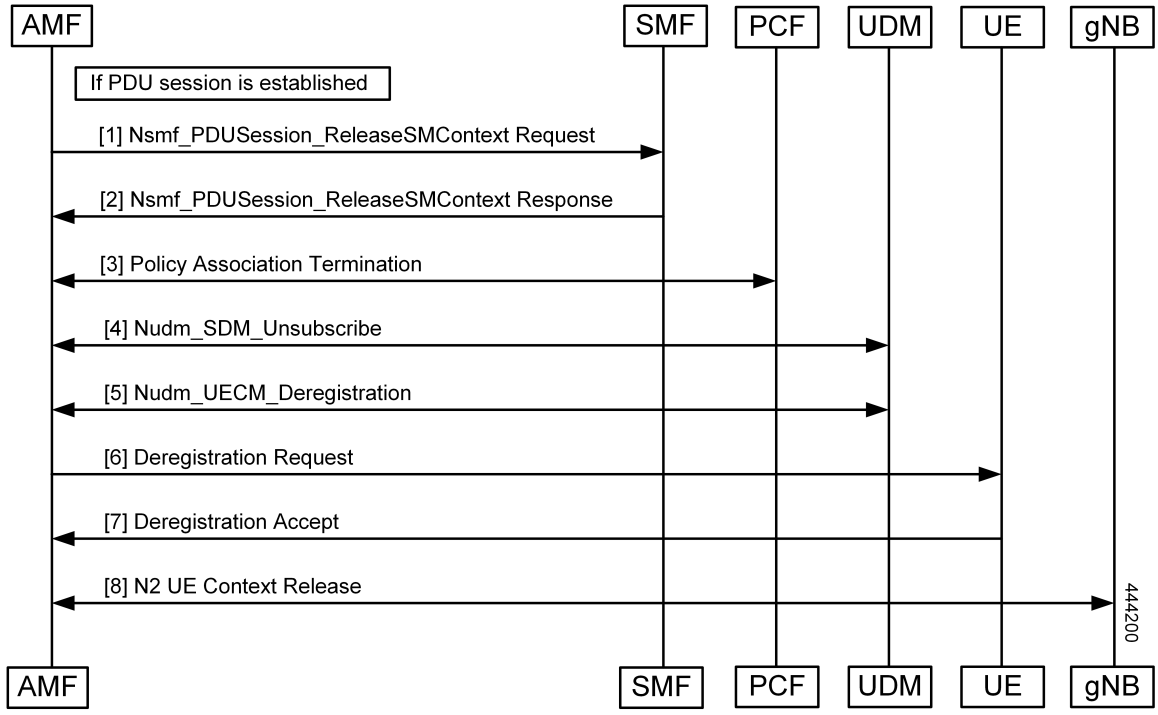
Step	Description
1	If the UDM wants to request the immediate deletion of a subscriber's contexts and PDU sessions, the UDM sends a Nudm_UECM_DeregistrationNotification (SUPI, Access Type, Removal Reason) message with Removal Reason set to Subscription Withdrawn to the registered AMF. If the AMF receives Nudm_UECM_DeregistrationNotification with Removal Reason as Subscription Withdrawn, the AMF executes the 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 Reregistration in which case the UE should reregister 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 unsubscribes with the UDM using Nudm_SDM_Unsubscribe service operation.
5, 6	If the UE has any established PDU sessions, the 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 and cell identity of the cell which the UE is using.
9	The AMF exchanges the N2 UE Context Release with gNB.

AMF-Initiated Deregistration Call Flow

This section describes the AMF-Initiated Deregistration call flow.

If implicit detach timer expires, the AMF performs deregistration.

Figure 29: AMF-Initiated Deregistration Call Flow



In case of a clear subscriber, the AMF starts a deregistration procedure.

Table 47: AMF-Initiated Deregistration Call Flow Description

Step	Description
1	If the PDU session is established, the AMF sends Nsmf_PDUSession_ReleaseSMContext (SUPI, PDU, and 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 the UDM using the 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 reregistration in which case the UE should reregister 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.

Step	Description
7	After 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 and cell identity of the cell which the UE is using.
8	The AMF and gNB exchanges the N2 UE Context Release.

UE Identity Procedure for Authentication Failure Call Flow

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

When the authentication fails at the Step 5 mentioned in the following call flow, the AMF triggers the Identity Request towards UE. Authentication is proceeded with the new UE identity.

Figure 30: UE Identity Procedure for Authentication Failure Call Flow

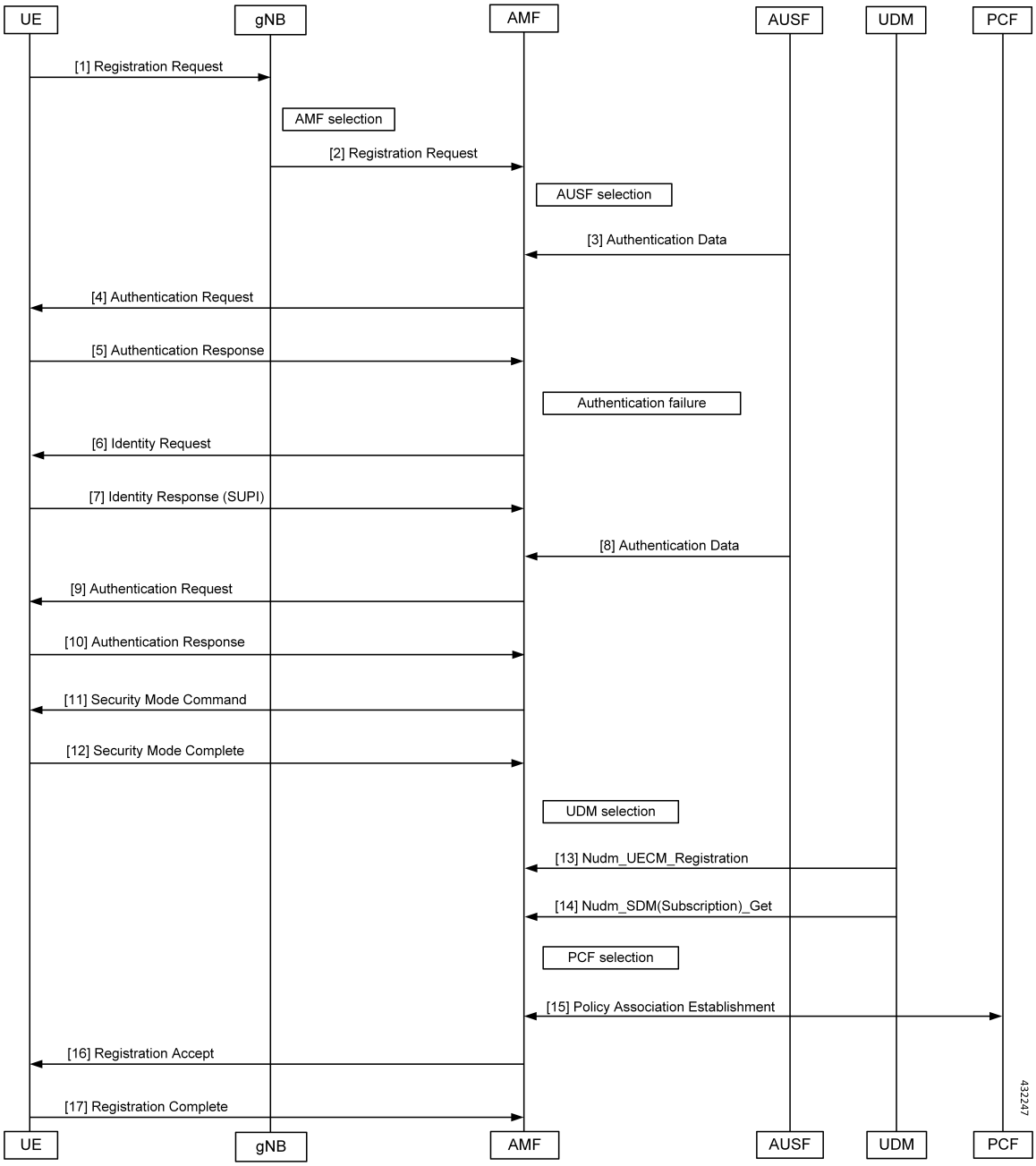


Table 48: UE Identity Procedure for Authentication Failure Call Flow Description

Step	Description
1	The UE sends a Registration Request to the gNB.
2	The gNB forwards the Registration Request with the AMF selection to the AMF.
3	The AUSF sends the authentication data along with the AUSF selection to the AMF.

Step	Description
4	The AMF sends an Authentication Request to the UE.
5	During the registration procedure when Authentication Response is received from the UE, the AMF examines the Authentication Response parameters and confirms that the authentication has failed. In such a case, the AMF triggers Identity Request to UE asking for its SUCI.
6	The UE sends the Identity Request message to 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 that the result received and if the result is as expected then the registration procedure starts.
11	The NAS security initiation is performed.
12	After the NAS security function setup is complete, the AMF starts the NGAP procedure to provide the 5G-AN with security context. The 5G-AN stores the security context and notifies it 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 info through the NRF query or 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	The AMF selects 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. The policies are not applied for UE and are stored in AMF.
16	The AMF sends a Registration Accept message to the UE indicating that the Registration Request is accepted. Registration Accept contains the following: • 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

Step	Description
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 a Registration Request is received with unknown GUTI then AMF triggers an Identity Request towards UE and requests for an UE identity. Registration proceeds with the new UE identity.

Figure 31: UE Identity Procedure for Unknown Subscribers Call Flow

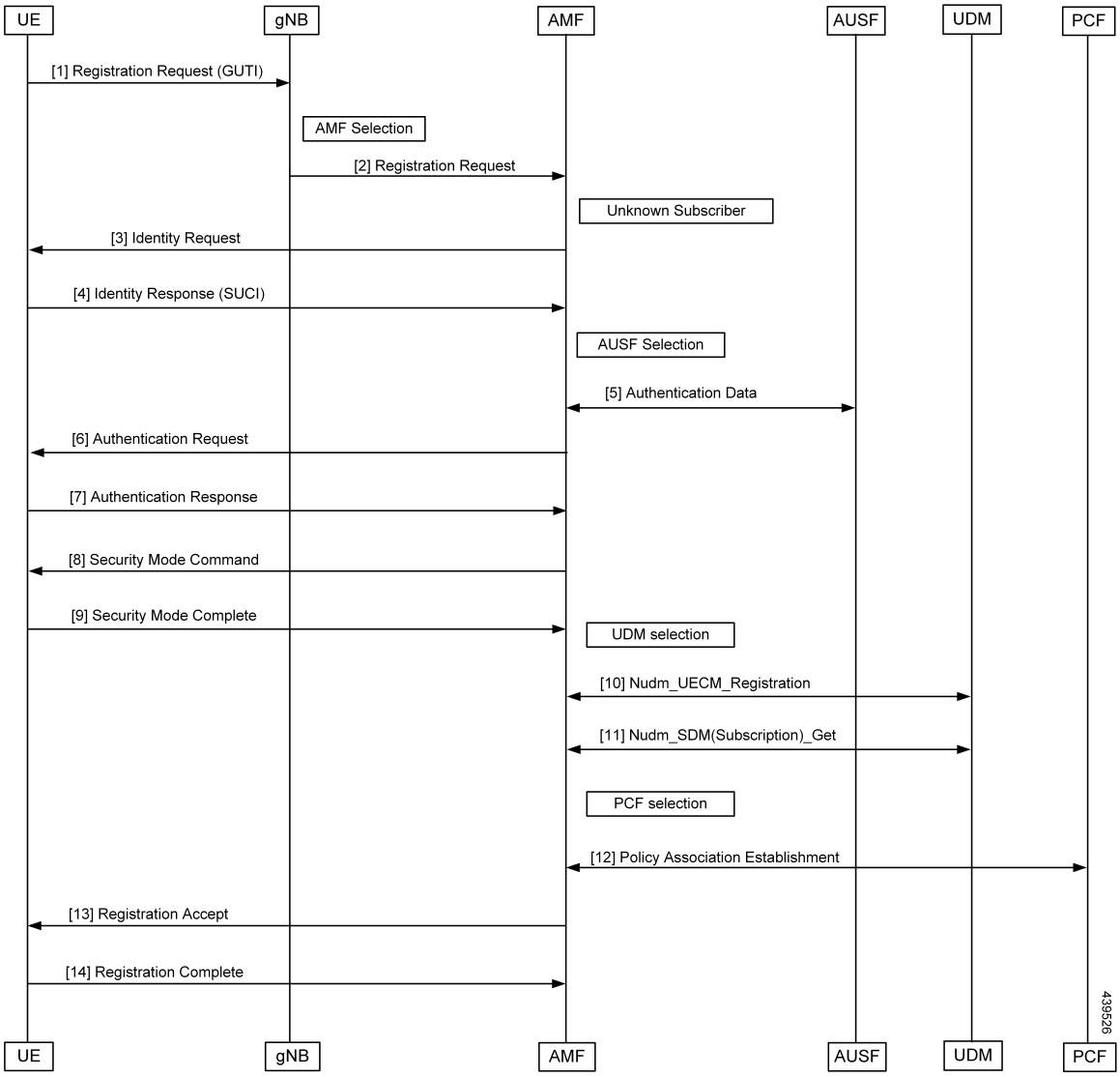


Table 49: UE Identity Procedure for Unknown Subscribers Call Flow Description

Step	Description
1	The UE sends the Registration Request with the GUTI to the gNB.
2	During the registration procedure, the AMF determines that the received GUTI is of a subscriber who is not present in AMF. In such case, AMF triggers an identity-request to UE asking for its SUCI.
3	The UE sends the identity-request message to the AMF.
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 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 that the result received and if the result is as expected then the registration procedure is proceeded.
8	The NAS security initiation is started.
9	After the NAS security function is set up, the AMF initiates the NGAP procedure to provide the 5G-AN with security context. The 5G-AN stores the security context and notifies it to 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 info through the NRF query or 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 PCF based on PLMN-info and slice-info and performs a Policy Association Establishment. The PCF sends policy data to AMF with restrictions and other policies to be applied for the UE. Currently the policies are not applied for UE and are stored in AMF.

Step	Description
13	The AMF sends a Registration Accept message to the UE indicating that the Registration Request has been accepted. The Registration Accept contains the following: • 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
```

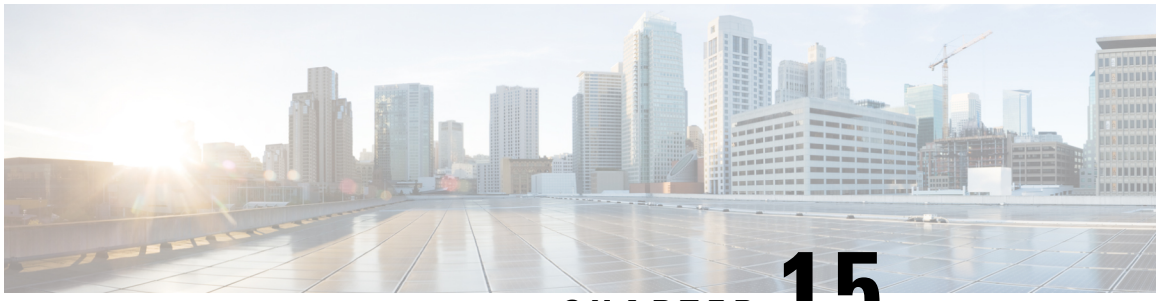
```
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 <Peer AMF IP Address>
      primary ip-address port <Peer AMF Port number>
     exit
    exit
   exit
  exit
 exit
exit
exit

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 15

Dynamic Configuration Change Support for SCTP and SBI Endpoints

Feature Summary and Revision History

Summary Data

Table 50: 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 51: 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 156 and Configuring the SCTP VIP-IP Port Removal , on page 157.
- 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 157.
- 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 160.

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:

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.
- The change in the SCTP IP address isn't supported dynamically but the port change is supported.
- For any addition, deletion, or update of a new IP to the existing SCTP service requires the AMF restart.

Configuration Example

The following is an example configuration for IPv4.

```
config
   instance instance-id 1
      endpoint sctp
         vip-ip 209.165.200.226 offline
         vip-ip 209.165.200.228 vip-port 1000
         end
```

The following is an example configuration for IPv6.

```
config
   instance instance-id 1
      endpoint sctp
         vip-ip 209.165.202.158 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 158.

- 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 158.
- 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 159.

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 209.165.200.226 offline
      vip-ip 209.165.200.225
      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 159.
- Slice Addition—This configuration enables the addition of a slice. For more information, refer to Configuring the Slice Addition, on page 159.
- Slice Removal—This configuration enables the removal of a slice. For more information, refer to Configuring the Slice Removal, on page 160.

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.

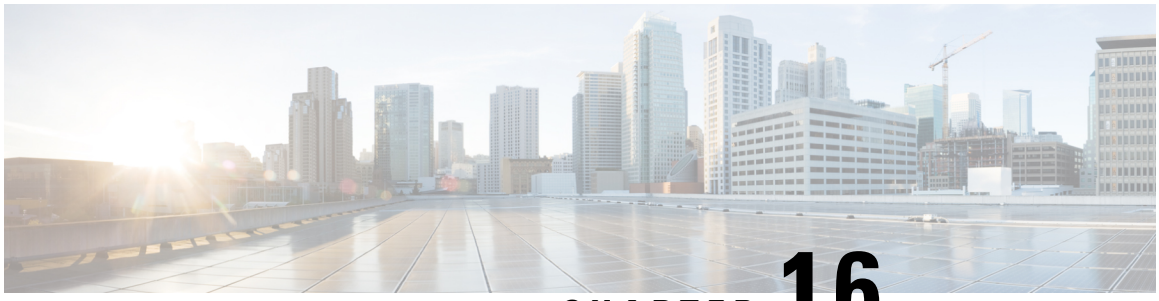
Note The VIP-IP doesn't support dynamic change. To update a VIP-IP, reconfigure the VIP-IP.

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 16

EAP and AKA Authentication

Feature Summary and Revision History

Summary Data

Table 52: 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 53: 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

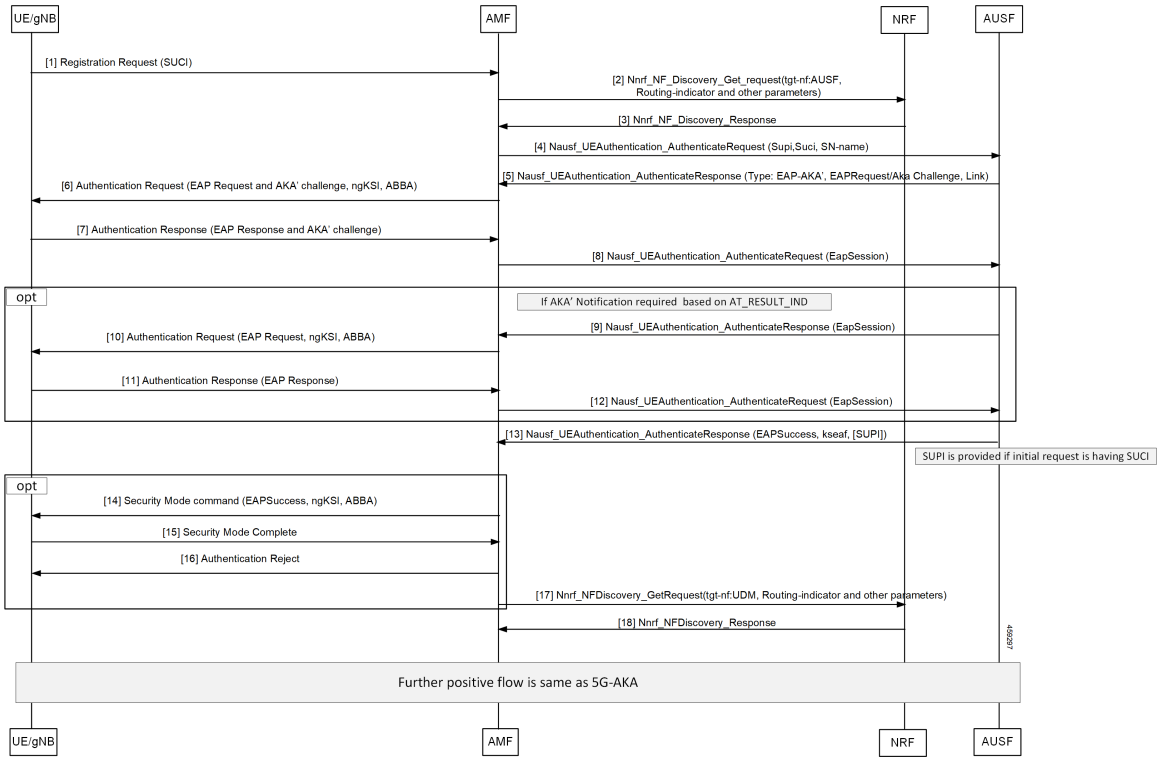
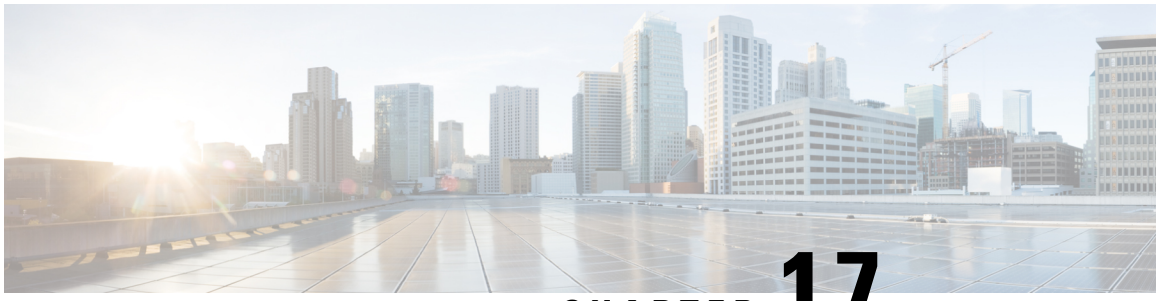


Table 54: EAP-AKA'-based Authentication basic Call Flow Description

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



CHAPTER 17

Encryption and Integrity Protection

Feature Summary and Revision History

Summary Data

Table 55: 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 56: 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:

- NEA0/NIA0
- 128-NEA1/128-NIA1
- 128-NEA2/128-NIA2

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

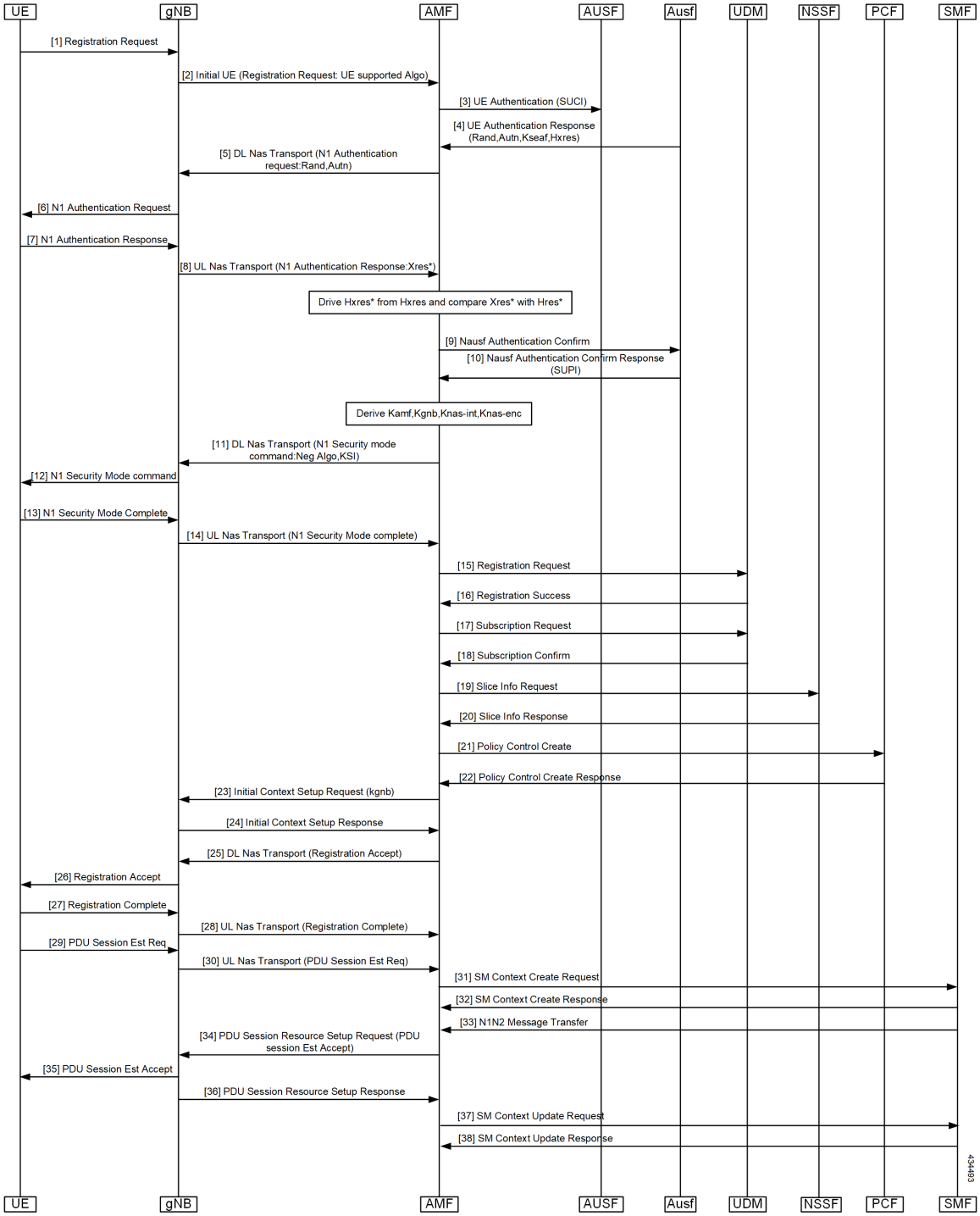


Table 57: UE Registration with Encryption/Integrity Protection Call Flow Description

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

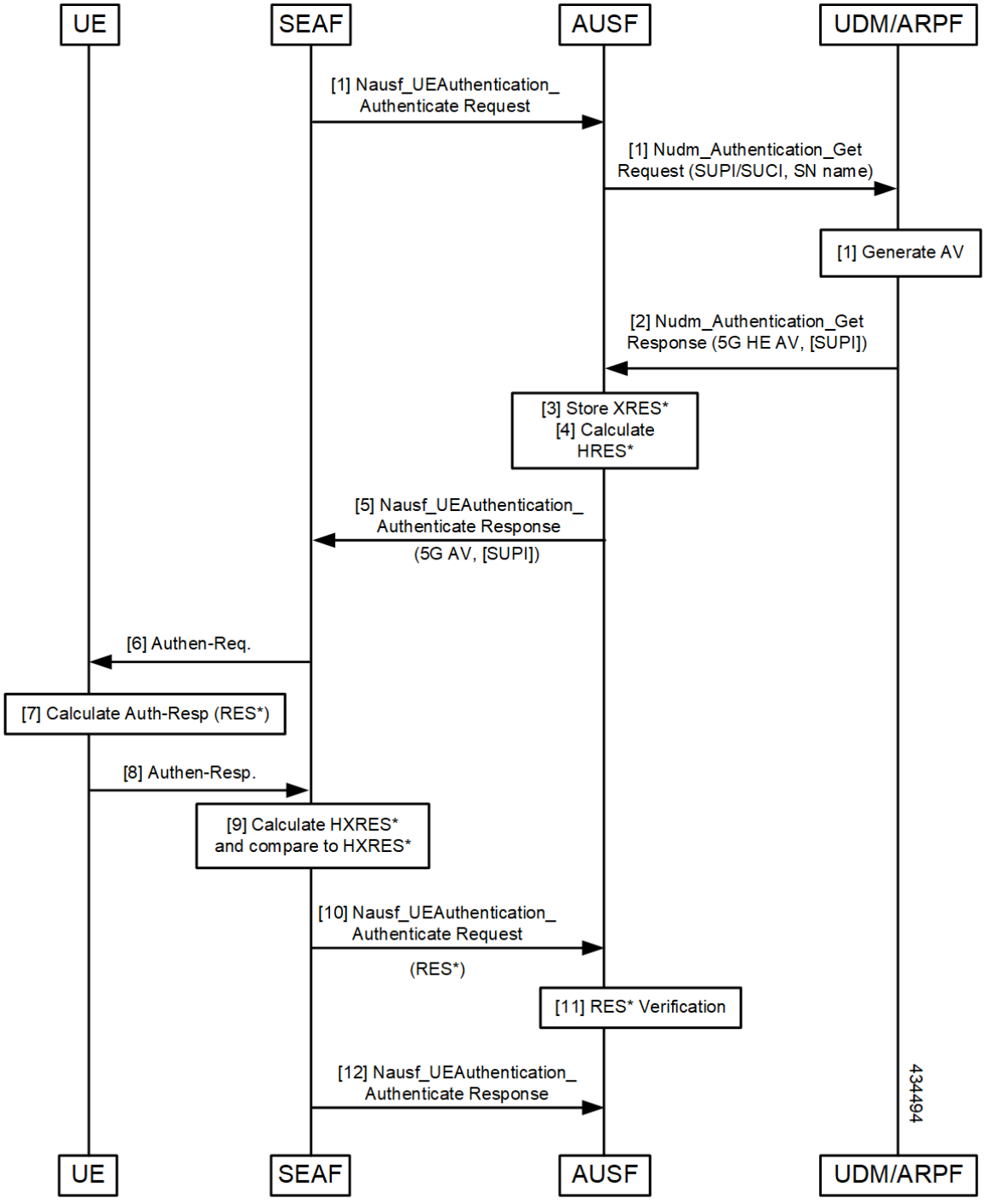


Table 58: UE Access and Authentication Request Call Flow Description

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.
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
```

OAM Support

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

Bulk Statistics Support

The following statistics are supported for this feature.

amf_nas_security_algos_total

Description: Captures the integrity and confidentiality algorithms that are used in AMF for processing the NAS messages and failure or errors that are associated with the security algorithms.

Labels:

- Label: algos_lang

  Label Description: The language type as go or c.

- Label: algos_type

Label Description: The algorithm type. Example: 128-5G-EA1

- Label: message_direction

  Label Description: The message direction as inbound or outbound.

- Label: message_type

  Label Description: The message type.

- Label: reason

  Label Description: The reason for the failure.

- Label: status

  Label Description: The status as success or failure.

amf_nas_security_algos_seconds_total

Description: Captures the time spent processing the security algorithms.

Labels:

- Label: algos_lang

  Label Description: The language type as go or c.

- Label: algos_type

  Label Description: The algorithm type. Example: 128-5G-EA1

- Label: message_direction

  Label Description: The message direction as inbound or outbound.

- Label: message_type

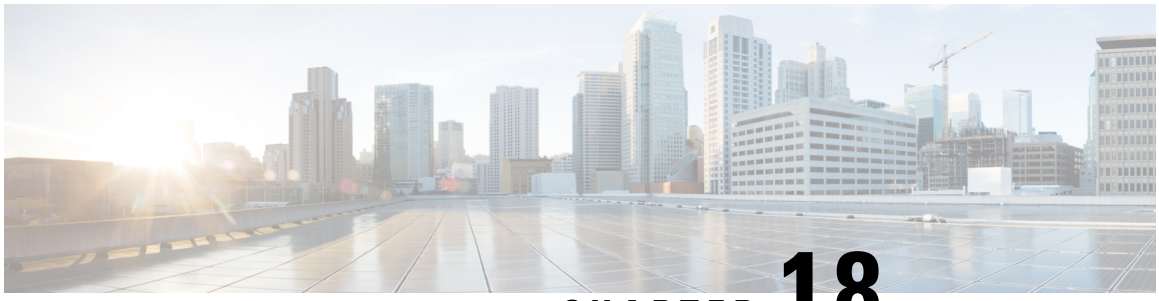
  Label Description: The message type.

- Label: reason

  Label Description: The reason for the failure.

- Label: status

  Label Description: The status as success or failure.



CHAPTER 18

Evolved Packet System Fallback Support

Feature Summary and Revision History

Summary Data

Table 59: Summary Data

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

Revision History

Table 60: 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 an action sent only to RAN, which is based on the value of CLI, and the capability of UE.

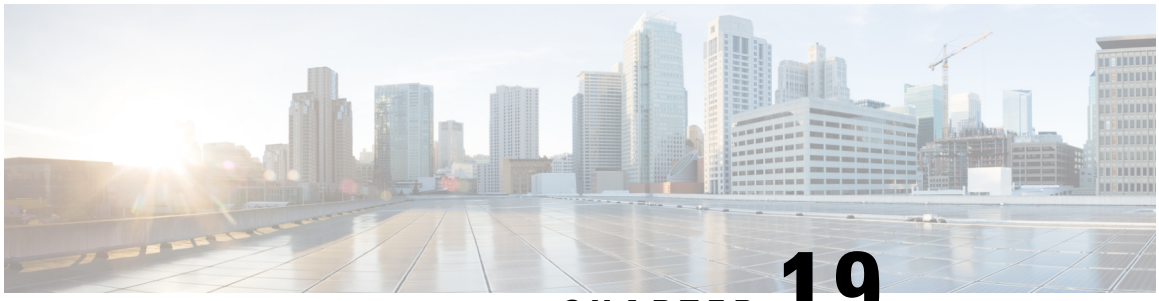
NOTES:

- **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 "Interworking without N26" indicator supported within the 5GS network functionality support. It gets applied only when the "Interworking without N26" indicator in the 5GS network functionality is in a supported state. When not supported, the "unsupported status" doesn’t have a reference to the 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 nonsupported option indicates the disabled 5G VoPS 3GPP support.
- **5G IMS Voice over Packet-Switched (VoPS) 3GPP Sessions**—Specify if the UE capability support gets enabled or not. Also, to specify, if the enabled UE configuration is 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 19

Failure and Error Handling Support

Feature Summary and Revision History

Summary Data

Table 61: 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 62: Revision History

Revision Details	Release
Supported the following failure handing message types: • UdmSdmGetUeAmSubscriptionData • AmfCommReleaseUeContext	2023.03.0
Introduced local cause code support for the ims-vops-failure condition.	2022.02.0

Revision Details	Release
First introduced.	2022.01.0

Feature Description

AMF supports the error handling for the following interfaces:

- SBI—AMF interaction across various 5G NF's
- REST-EP—AMF interaction to NGAP, and NAS (towards UE)

AMF validates the syntax and semantic errors for each attribute during SBI message validation. It evaluates the mandatory, conditional, and optional attributes in the following:

- NGAP content
- NAS content
- Each SBI interface message

Note You can define the local cause code-mapping values for Mobility-Management, while rejecting the NAS messages under failure scenarios.

Validation of the NGAP and NAS optional IEs aren't supported.

How it Works

This section describes how this feature works.

Error Handling on SBI Interface

AMF supports the failure handling for SBI interfaces to continue or to terminate the call. This failure handling is supported as per the actions defined under each service, message-type, and status code.

NRF library provides the failure handling template for each NF to handle statistical and dynamical endpoint information. This library integrates with the REST endpoint to handle SBI message requests or responses.

AMF performs failure handling in the following scenarios:

- When the remote SBI endpoint responds with HTTP error code, it performs the retry procedure as per the failure handling template configuration.
- When the remote SBI endpoint does not respond within the timeout value, it considers it as an error and proceeds with failure handing.
- When failure is detected, the REST endpoint checks for retry count in the Failure Handing profile and performs retries.
- When retries are exhausted or retries aren't configured, it performs the failure action as configured.

Retransmit happens to the same configured URI.

You can configure response timeout under Failure Handling profile. The default timeout value is 2000 ms.

When multiple status codes are received, the number of retries defined for the first received status code is considered.

For terminate process, the UE context is cleared without any peer communication.

Note

- AMF supports the primary, secondary, and tertiary IP addresses that are defined in NF-client profile. If the primary address returns an error or times out, try the secondary address. If the secondary address returns an error or times out, try the tertiary address.
- **Retry-and-ignore** is supported only for the SMSF interface.

The peer NFs send cause codes to the AMF for each SBI interface. The AMF handles these cause codes received from any SBI interface in each response message as per UE context.

Table 63: SBI Supported Failure Actions

Parameter	Failure Action
continue	• Continues the session • Rejects the call
terminate	• Terminates the session • Rejects the call
retry-and-terminate	Perform retry as configured • If retries are not exhausted, continues the session and the call. • If retries are exhausted, terminates the session and rejects the call.
retry-and-continue	Perform retry as configured • If retries are not exhausted, continues the session and the call. • If retries are exhausted, terminates the session and rejects the call.
retry-and-ignore	Perform retry as configured • If retry is passed, continues the session, and continues the call. • If retries are exhausted, continues the session, and continues the call (provided no dependency).

SBI Supported Interfaces and Messages

Table 64: Feature History Table

Feature Name	Release Information	Description
New Failure Handling Messages	2023.03	AMF supports the following new message types as part of the failure handling template configuration. • UdmSdmGetUeAmSubscriptionData • AmfCommReleaseUeContext

Table 65: SBI Supported Interfaces and Messages

Interface	Messages
AMF	Service: namf-comm • AmfCommUeContextTransfer • AmfCommUeContextTransferUpdate • AmfCommCreateUeContext • AmfCommReleaseUeContext
AUSF	Service: nausf-auth • AusfAuthenticationReq • AusfAuthenticationCfm
PCF	Service: npcf-am-policy-control • PcfAmfPolicyControlCreate • PcfAmfPolicyControlDelete
SMF	Service: nsmf-pdusession • SmfSmContextCreate • SmfSmContextUpdate • SmfSmContextDelete
SMSF	Service: nsmsf-sms • SmsfActivationReq • SmsfDeactivationReq • SmsfSendSms

Interface	Messages
UDM	Service: nudm-sdm • UdmSubscriptionReq • UdmUnSubscriptionReq • UdmSdmGetUeAmSubscriptionData Service: nudm-uecm • UdmRegistrationReq • UdmDeRegistrationReq

SBI Message Validation

AMF performs the message validation for the SBI interfaces.

Table 66: Handling of Inbound Request Messages

Action	Inbound Request Message
Lookup	• Performs look up for the presence of mandatory or conditional attributes. • REST endpoint fills the appropriate cause code and sends to the peer NF when inbound message isn’t qualified. • REST endpoint doesn't forward the failure request process to the AMF-service pod.
Validation	• Validates syntax and semantic errors in mandatory or conditional attributes. • REST endpoint fills the appropriate cause code and sends to the peer NF, when any failure of message parsing or decoding occurs. • REST endpoint doesn't forward the failure request process to the AMF-service pod.
Optional Attributes	• Validates optional attributes in SBI messages. • Checks the syntax and semantic errors of optional attributes present in the SBI message. • REST endpoint ignores the validation of failed optional attributes and forwards the request to the AMF-service pod. The AMF-service pod handles the requested message as per the call model.

Note Validation of incoming inbound request message from UDM, SMF, and SMSF to AMF is supported on the REST endpoint.

Error handling on NGAP and NAS

NGAP error handling:

- Mandatory IE's presence and length checks are performed for the NGAP message validation.

NAS error handling:

- Mandatory IE's presence and length checks are performed for NAS message validation. Conditional IE validations for NAS are also performed.

Local Cause Code Mapping

You can ignore the default EPS Mobility Management (EMM) cause code and configure a preferred EMM cause code to send to a UE in response to a procedural failure.

For example, you can instruct the AMF to return one of the six different EMM cause codes other than the default value, when the AMF receives an authentication error from an AUSF. A list local cause code mappings are created at the global configuration level. A desired list name is specified in the Call Control Profile or in the AMF services or both.

The order of Cause Code selection is as follows:

- Call Control Profile
- AMF Services
- Default

You can configure the local cause codes either or both in the AMF-service or in the Call Control profile.

Table 67: Local Cause Code Mapping condition and 5GMM Cause Codes, on page 185 explains the local cause code-mapping conditions, and 5GMM cause codes with its default value.

Table 67: Local Cause Code Mapping condition and 5GMM Cause Codes

Local Cause Code Mapping Condition	5GMM Cause Codes
auth-failure	• illegal-ms • no-suitable-cells-in-tracking-area • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: illegal-ms
clear-subscriber	• plmn-not-allowed • 5GS-services-not-allowed • no-suitable-cells-in-tracking-area • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: plmn-not-allowed
ctxt-xfer-fail	• ue-identity-not-derived • no-suitable-cells-in-tracking-area • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: ue-identity-not-derived
ims-vops-failure	• redirection-to-epc-required • no-suitable-cells-in-tracking-area Default Value: redirection-to-epc-required

Local Cause Code Mapping Condition	5GMM Cause Codes
peer-node-unknown	• ue-identity-not-derived • no-suitable-cells-in-tracking-area • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: ue-identity-not-derived
registration-restriction	• plmn-not-allowed • 5GS-service-not-allowed • no-suitable-cells-in-tracking-area • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: plmn-not-allowed
rat-type-restriction	• plmn-not-allowed • no-suitable-cells-in-tracking-area • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: plmn-not-allowed
restricted-zone-code	• no-suitable-cells-in-tracking-area • 5GS-services-not-allowed • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: no-suitable-cells-in-tracking-area

Local Cause Code Mapping Condition	5GMM Cause Codes
udm-unavailable	• no-suitable-cells-in-tracking-area • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: no-suitable-cells-in-tracking-area

Feature Configuration

Configuring this feature involves the following steps:

1. Local Cause Code Mapping at Global Configuration—This configuration supports the commands to configure local cause code mapping at Global configuration. For more information, see Configuring the Local Cause Code Mapping at Global Configuration, on page 187.
2. Local Cause Code Mapping under Call Control Policy Configuration. —This configuration supports the commands to configure local cause code mapping under Call Control Policy. For more information, see Configuring the Local Cause Code Mapping under Call Control Policy, on page 188.
3. Local Cause Code Mapping under AMF Service Configuration—This configuration supports the commands to configure local cause code mapping under AMF-service. For more information, see Configuring the Local Cause Code Mapping under AMF Service, on page 188.

Configuring the Local Cause Code Mapping at Global Configuration

To configure this feature, use the following configuration:

```
config
   local-cause-code-map name cause_code_map_name cause_code_type cause-code-5gmm
 cause_code_5gmm_type
   end
```

NOTES:

- **local-cause-code-map name** *cause_code_map_name cause_code_type*—Specify a name for Cause Code Map.

  The *cause_code_type* includes one of the following:

  - auth-failure—UE authentication failure
  - clear-subscriber—UE subscriber clear condition type
  - ctxt-xfer-fail—Context transfer failure between AMF and MME
  - ims-vops-failure—IMS voice-centric UE registration failure
  - peer-node-unknown—No response from peer node

- `rat-type-restriction`—Restriction with RAT type
- `registration-restriction`—Restriction with Registration
- `restricted-zone-code`—Restricted zone code
- `udm-unavailable`—UDM not available

cause-code-5gmm *cause_code_5gmm_type*—Specify the *cause_code_5gmm_type*. For the values of *cause_code_5gmm_type*, see *Local Cause Code Mapping condition and 5GMM Cause Codes* table.

Configuration Example

The following are the example configurations.

```
config
   local-cause-code-map name lc1 auth-failure cause-code-5gmm
no-suitable-cells-in-tracking-area
   end
```

```
config
   local-cause-code-map name lc2 ctxt-xfer-fail cause-code-5gmm restricted-service-area
   end
```

```
config
   local-cause-code-map name example ims-vops-failure { no-suitable-cells-in-tracking-area
 | redirection-to-epc-required }
   end
```

Configuring the Local Cause Code Mapping under Call Control Policy

```
config
   call-control-policy policy_name
      local-cause-code-map cause_code_map_name
      end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the Call Control Policy name.
- **local-cause-code-map** *cause_code_map_name*—Specify the *cause_code_map_name* which is configured at *Configuring the Local Cause Code Mapping at Global Configuration*.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy ccp1
         local-cause-code-map lc1
         end
```

Configuring the Local Cause Code Mapping under AMF Service

To configure this feature, use the following configuration:

```
config
   amf-services service_name
      local-cause-code-map cause_code_map_name
      end
```

NOTES:

- **local-cause-code-map** *cause_code_map_name*—Specify the *cause_code_map_name* which is configured at Configuring the Local Cause Code Mapping at Global Configuration, on page 187 .

Configuration Example

The following is an example configuration.

```
config
   amf-services amf
      local-cause-code-map lc2
      end
```

Failure Handling Template

Configuring the response timeout for failure handling involves the following steps:

- Response Timeout Configuration at Endpoint—This configuration provides the commands to configure response timeout at endpoint. For more information, see Configuring the Response Timeout at Endpoint, on page 189.
- Response Timeout Configuration at Failure Profile—This configuration provides the commands to configure response timeout at failure profile level. For more information, see Configuring the Response timeout at Failure Profile, on page 190.

The following is an example of the failure handling template configuration for the AUSF. This configuration is similar for all other interfaces.

Configuring the Response Timeout at Endpoint

To configure the response timeout at endpoint level, use the following configuration:

```
config
   profile nf-client nf-type name_of_nf_type
      ausf-profile profile_name
         locality locality_name
            service name type service_name
               responsetimeout timeout_value
               end
```

NOTES:

- **profile nf-client nf-type** *name_of_nf_type*—Specify the NF.
- **ausf-profile** *profile_name*—Specify a name for AUSF profile.
- **locality** *locality_name*—Specify a name for locality.
- **service name type** *service_name*—Specify a name for service type.
- **responsetimeout** *timeout_value*—Specify the timeout value in seconds. Must be an integer.

Configuration Example

The following is an example configuration.

```
config
   profile nf-client nf-type ausf
      ausf-profile AUP1
         locality LOC1
            service name type nausf-auth
               responsetimeout 2000
               end
```

Configuration Verification

To verify the configuration:

```
show running-config profile nf-client nf-type ausf | details
profile nf-client nf-type ausf
 ausf-profile AUP1
  locality LOC1
   priority 30
   service name type nausf-auth
    responsetimeout 2000
    endpoint-profile EP1
     capacity   30
     priority   1
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.229
      primary ip-address port 9047
      secondary ip-address ipv4 209.165.200.229
      secondary ip-address port 9047
      tertiary ip-address ipv4 209.165.200.229
      tertiary ip-address port 9047
     exit
    exit
   exit
  exit
 exit
exit
```

Configuring the Response timeout at Failure Profile

When the request is failed and the failure profile is selected, the response time is considered from the failure handling profile.

To configure the response timeout at failure profile level, use the following configuration:

```
config
   profile nf-client-failure nf-type name_of_nf_type
      profile failure-handling failure_handling_name
         service name type service_name
            responsetimeout timeout_value
            end
```

NOTES:

- **profile nf-client-failure nf-type** *name_of_nf_type*—Specify the NF.
- **profile failure-handling** *failure_handling_name*—Specify a name for failure handling.
- **service name type** *service_name*—Specify a name for service type.

- **responsetimeout** *timeout_value*—Specify the timeout value in seconds. Must be an integer.

Configuration Example

The following is an example configuration:

```
config
   profile nf-client-failure nf-type ausf
      profile failure-handling FH1
         service name type nausf-auth
            responsetimeout 1000
            end
```

Configuration Verification

To verify the configuration:

```
show running-config profile nf-client-failure nf-type ausf | details
profile nf-client-failure nf-type ausf
 profile failure-handling FH1
  service name type nausf-auth
   responsetimeout 1000
   message type AusfAuthenticationReq
    status-code httpv2 503
     retry               3
     retransmit          2
     retransmit-interval 25
     action              retry-and-terminate
    exit
   exit
   message type AusfAuthenticationCfm
    status-code httpv2 503
     retry               3
     retransmit          2
     retransmit-interval 25
     action              retry-and-terminate
    exit
   exit
  exit
 exit
exit
```

Behavior for Multiple Failure Cause Code Configuration

If multiple status codes return one after another matches the failure handling profile, the following known behavior is observed:

- Example—When retry count is configured and retransmit value is not configured.

```
config
  profile nf-client-failure nf-type smsf
   profile failure-handling FH5
    service name type nsmsf-sms
     responsetimeout 1000
     message type SmsfActivationReq
      status-code httpv2 500
       retry  3
       retransmit-interval 2000
       action retry-and-ignore
      exit
      status-code httpv2 504
       retry  2
       retransmit-interval 2000
```

```
      action retry-and-ignore
      end
```

For the example mentioned,

- If AMF receives 500 response for the first try, then it performs a second retry.
- In the second retry, if AMF gets 504 response, AMF tries twice.
- When this retry count (for 504 response) is exhausted, AMF doesn't resume the retry count for first one (500 response).
- The maximum retries depend on the maximum number of endpoints configured (primary, secondary, tertiary) or NRF discovered ones.

- Example—When retry count and retransmit value are configured.

```
config
  profile nf-client-failure nf-type smsf
   profile failure-handling FH5
    service name type nsmsf-sms
     responsetimeout 1000
     message type SmsfActivationReq
      status-code httpv2 504
       retransmit 3
       retry 2
       action retry-and-terminate
       end
```

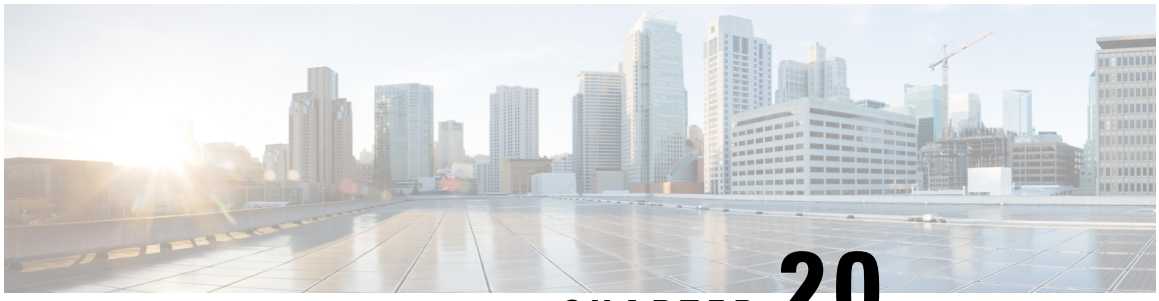
For the example mentioned,

- If both retransmit value and retry count are configured, retransmit happens first and then retry.

  Retransmmission is done thrice and if it fails, retry to done for secondary endpoint.

  If retry returns 504 response, retransmmission is done three times and if it fails, retry is done for tertiary endpoint.

Note Retries are always done to another endpoint, while retransmmission is done always to same endpoint.



CHAPTER 20

Failure/Exception Handling Framework Support

Feature Summary and Revision History

Summary Data

Table 68: 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 69: 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 70: 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 71: 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 72: 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 73: 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 74: 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 75: 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 76: Internal Errors

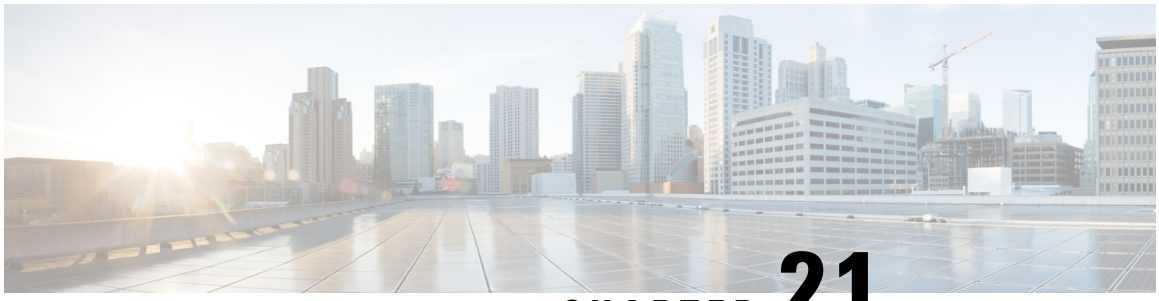
Error	Description	Reject Cause/Action
Timeout	The AMF does not get a response from UDM.	Registration Reject with cause #15, No suitable cells in tracking area
Timeout	5The AMF does not get a response from AUSF.	Drop the message

Error Handling for Protocol Data – NAS

Table 77: 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



CHAPTER 21

High Availability Services

Feature Summary and Revision History

Summary Data

Table 78: 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 79: Revision History

Revision Details	Release
Changes to spawning of protocol endpoint pods in a single-server deployment scenario	2023.03.0
Sub-feature introduced. SCTP High Availability Service	2022.01.0
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
- SCTP

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

Table 80: Feature History

Feature Name	Release Information	Description
Protocol Endpoint Pod Spawn in Single-server Deployment	2023.03	In a single-server deployment scenario, AMF allows spawning of two protocol endpoint pod replicas on the same node to support resiliency. AMF achieves this functionality by enabling the following command in the AMF Ops center. **k8s single-node true** For information on deploying AMF on a single server, contact your Cisco account representative.

Feature Description

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

Note It is recommended to support a maximum of two protocol pod replicas for high availability. If both protocol pod replicas go down back to back or together, the security context data gets lost.

Typically, the two replicas of protocol endpoint pods are spawned on active-standby mode on different servers to achieve redundancy and resiliency.

Note In a single server deployment of AMF, two replicas of protocol-ep pods can be spawned on the same node by enabling the **k8s single-node true** command in the AMF Ops-center. For more information on single server deployment of AMF, contact your Cisco account representative.

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 request 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.

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
```

SCTP High Availability Service

Feature Description

SCTP uses virtual IP (VIP) to support HA. This feature supports two SCTP endpoints.

The SCTP pod starts and listens on VIP. If one SCTP pod goes down, traffic moves to the other SCTP pod using VIP.

Feature Configuration

To configure this feature, use the following configuration procedure:

1. Configure the k8 node labels, on which the SCTP pod should run.

   k8 label sctp-layer key smi.cisco.com/node-type value sctp

   Note The label must have a minimum number of two K8 nodes for active or standby pods to work.

2. Configure the two replicas as active and standby pod for SCTP. The active pod receives the traffic.

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

NOTES:

- **replicas** *replica_count*—Specify the number of SCTP replicas per node.

3. Configure the VIP for IPv4 and IPv6 using the following commands:

```
config
   instance instance-id instance_id
      endpoint sctp
        vip-ip ipv4_addressoffline { vip-interface interface_name | vip-port
 port_number }
         vip-ipv6 ipv6_address { offline  | vip-ipv6-port ipv6_port_number
}
         end
```

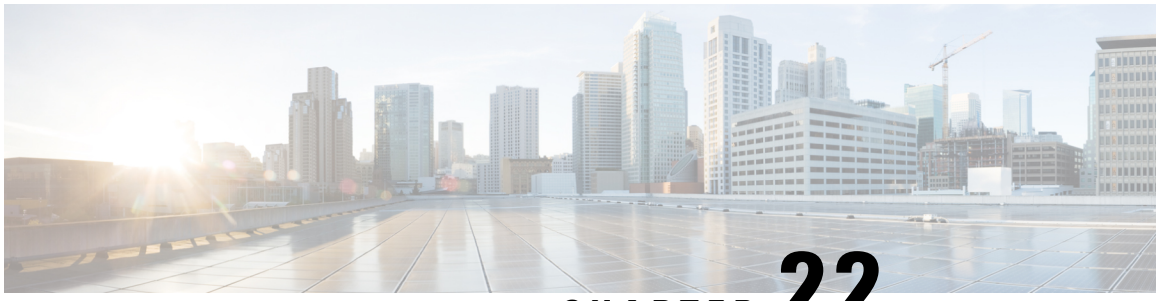
NOTES:

- **vip-ip** *ipv4_address* **[offline | vip-interface** *interface_name* **| vip-port** *port_number* **]**—Specify the IPv4 address of the pod on which VIP is enabled, interface, and the port number. This configuration marks VIP-IP as offline (standby).
- **vip-ipv6** *ipv6_address* **[offline | vip-ipv6-port** *ipv6_port_number* **]**—Specify the IPv6 address of the pod on which VIP is enabled. This configuration marks VIP-IP as offline (standby) if you specify as offline.

Configuration Example

The following is an example configuration.

```
config
   instance instance-id 1
      endpoint sctp
         replicas 2
         instancetype IPv6
         vip-ipv6 0001:000:00c1::4 vip-ipv6-port 1000
         end
```



CHAPTER 22

Idle Entry Procedure

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.	2020.01

Feature Description

The AMF supports transitioning the UE from ECM_CONNECTED to ECM_IDLE state.

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

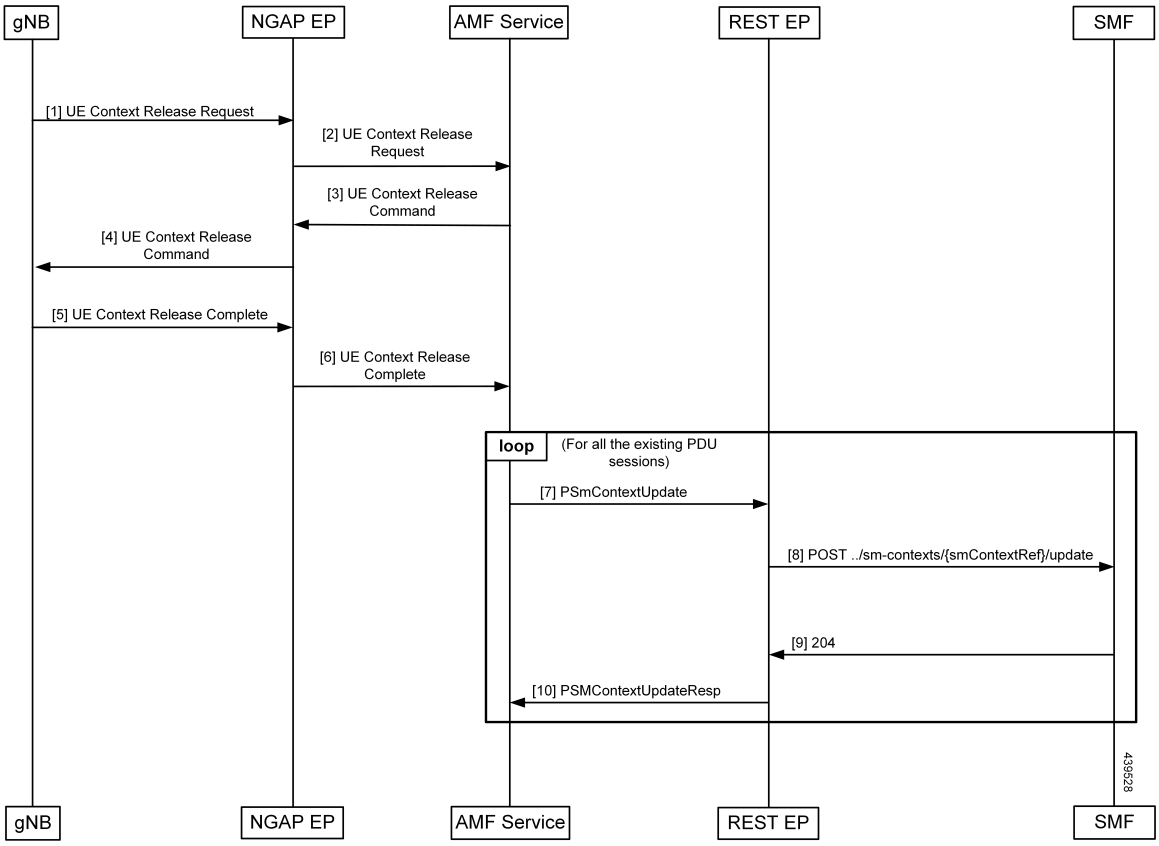


Table 83: gNB-Initiated UE Context Release Procedure Call Flow Description

Step	Description
1	The AMF receives the UE Context Release Request from the gNB.
2	The AMF sends the UE Context Release Command to the gNB.
3	The AMF receives the UE Context Release Complete from the gNB.

Step	Description
4	The SmContextUpdate procedure is started for all the existing PDU sessions of the subscriber.
5	Once the SmContextUpdate is complete, the UE is moved to the IDLE state.
6	The NGAP EP sends the Context Release Complete to the AMF Service. The T3512 timer is started when processing this message.
7	On expiry of the T3512 timer, the UE Detach Timer is started.
8	On expiry of the UE Detach Timer, the deregistration procedure is triggered.
9	The SMF sends the 204 message to the REST EP.
10	The REST EP sends the PSM Context Update Response message to the AMF Service.

UE or NW-Initiated Deregistration followed by UE Release Procedure Call Flow

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

Figure 36: UE or NW-Initiated Deregistration followed by UE Release Procedure Call Flow

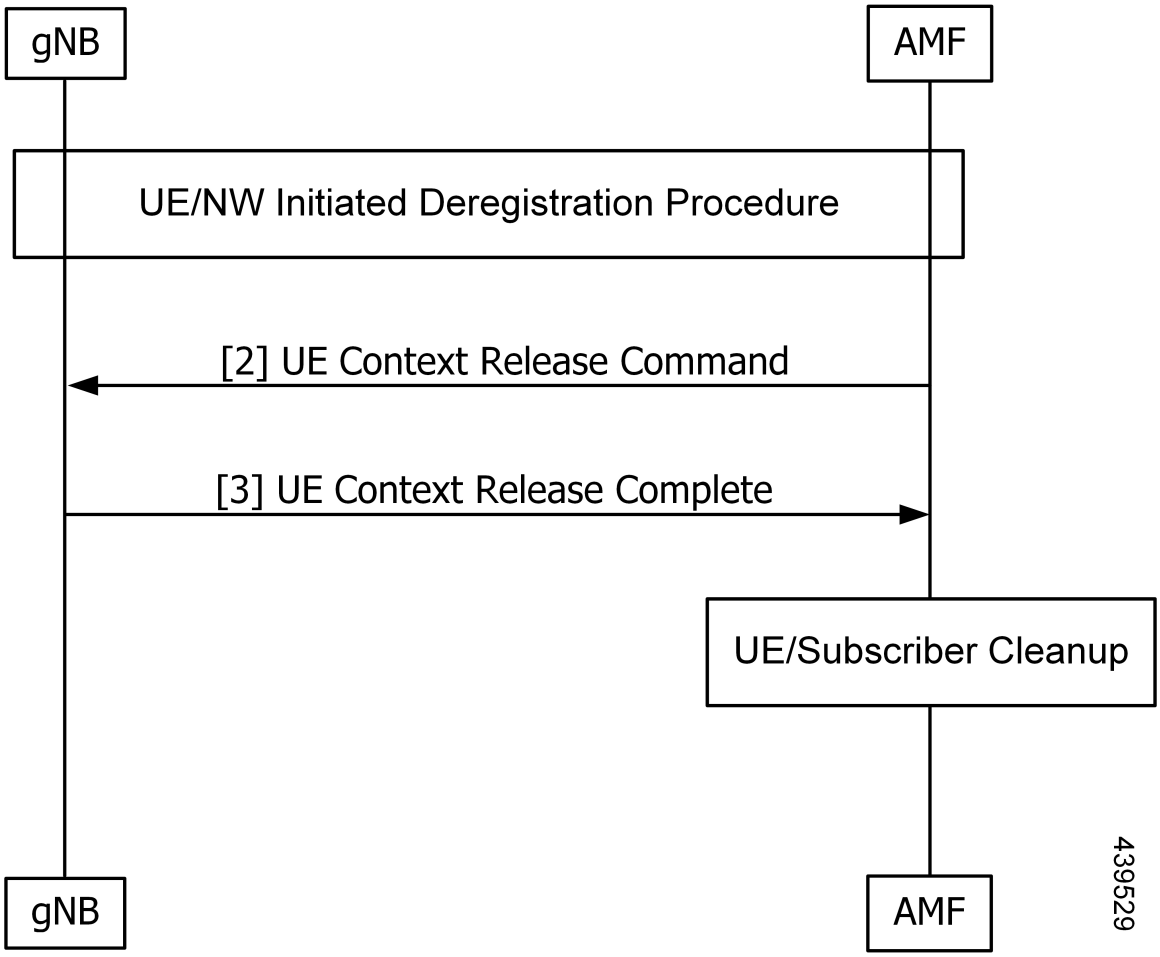
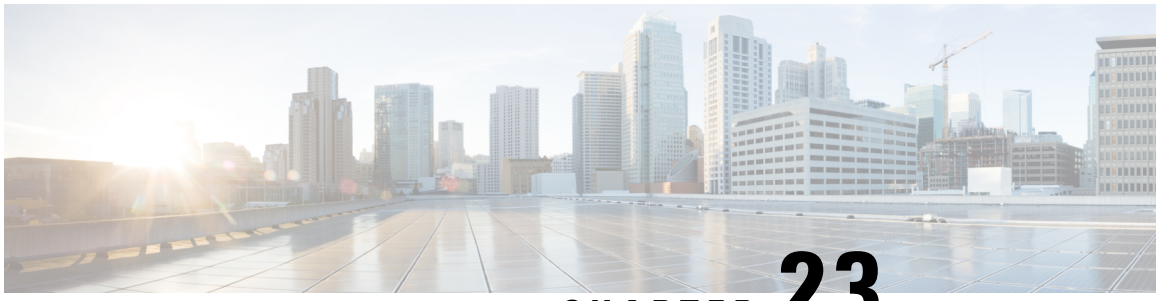


Table 84: UE or NW-Initiated Deregistration followed by UE Release Procedure Call Flow Description

Step	Description
1	The UE or NW-Initiated Deregistration procedure is completed. The Deregistration Request or Accept is completed and the UE is moved to the deregistered state.
2	The AMF sends the UE Context Release Command to the gNB.
3	The AMF receives the UE Context Release Complete from the gNB.
4	As the UE deregistration is already complete and the UE is moved to the deregistered state, the UE Context or subscriber Cleanup is triggered, and the subscriber and session is deleted from CDL.



CHAPTER 23

Internode Registration Support

Feature Summary and Revision History

Summary Data

Table 85: 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 86: Revision History

Revision Details	Release
Updates on context-transfer-guard timer details	2023.02.0
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 215 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

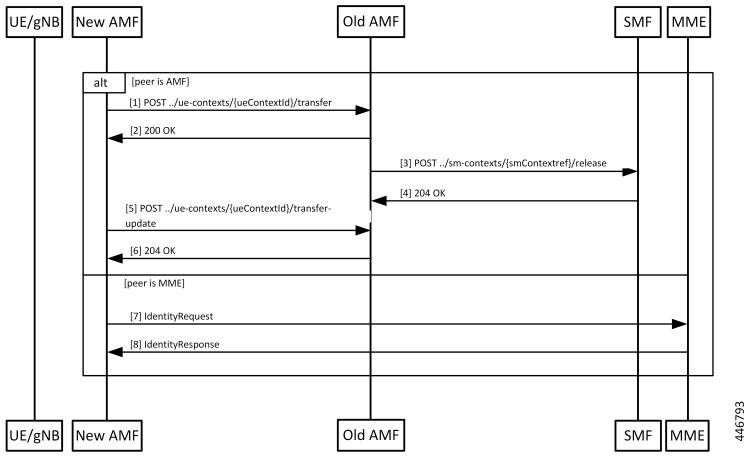


Table 87: Identification with Peer Node Call Flow Description

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.

Step	Description
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.
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

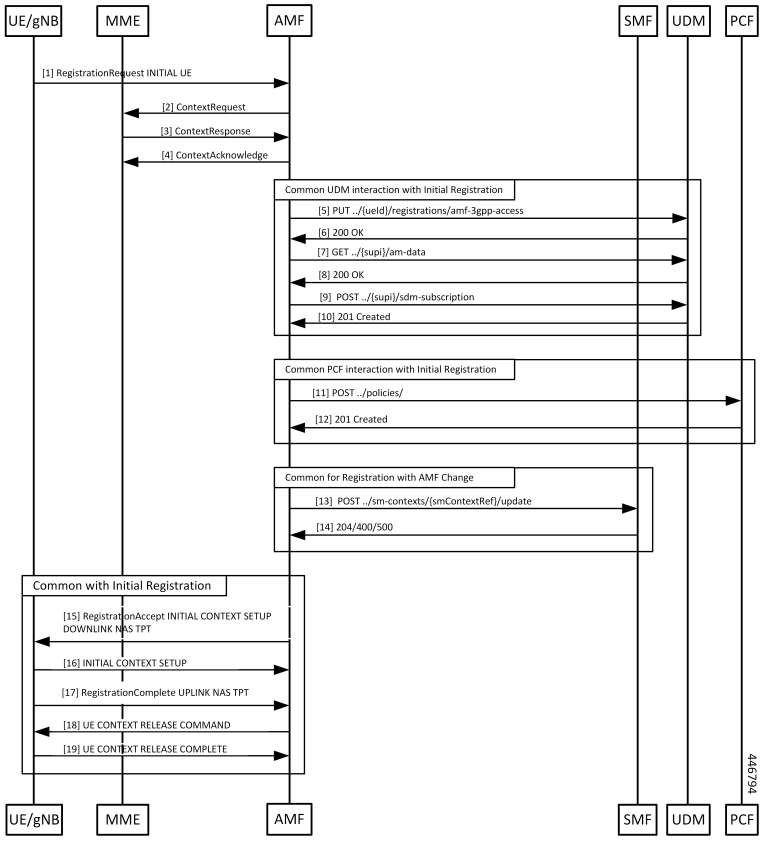


Table 88: Identification with Peer Node Call Flow Description

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 215.

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

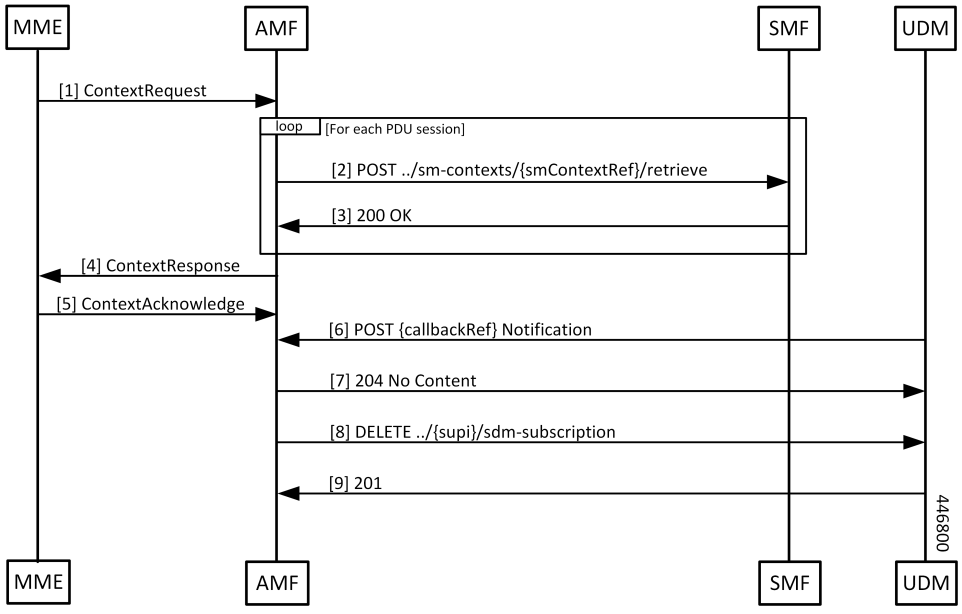


Table 89: AMF to MME Idle Mode Handoff Call Flow Description

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. It starts context-transfer-guard timer (configured with greater than zero (0)). On expiry of the context-transfer-guard timer, the source AMF performs the following: Triggers the UDM Deregistration internally to clear the local ueContext.
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. If the guard timer is not running, the AMF releases any local resources, and responds to the UDM. Otherwise amf responds to the UDM, and waits for the guard timer to expire before cleaning up the UEcontext.
8	The AMF clears the subscription to changes in subscription data at the UDM.
9	The UDM responds to the request from the AMF.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         timers
            context-transfer-guard
```

```
n26-interface value guard_time_value
end
```

NOTES:

- **call-control-policy** *policy_name*—Configure the Call Control Policy.
- **context-transfer-guard**—Specify the context transfer guard timer. The AMF starts this timer on receiving the TransferUpdate. On expiry, the AMF clears the PDUs locally.
- **n26-interface value** *guard_time_value*—Specify the interface n26-interface value in seconds. It must be an integer in the range of 0—35712000. The default value is zero (0).

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

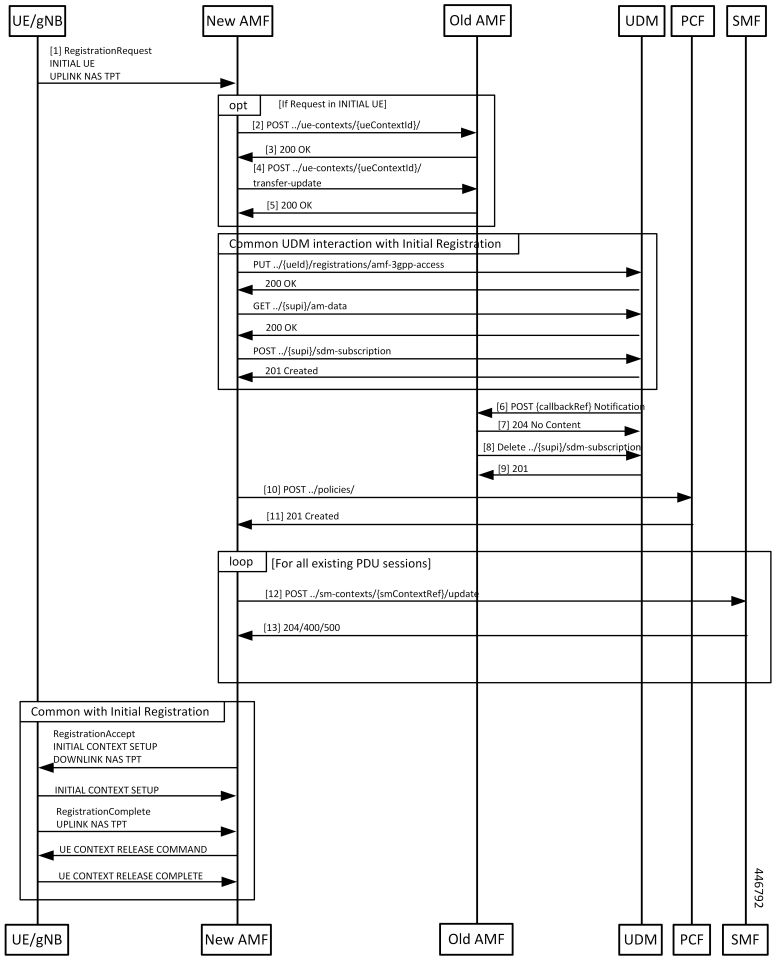


Table 90: Registration with AMF Change Call Flow Description

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.

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	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.
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

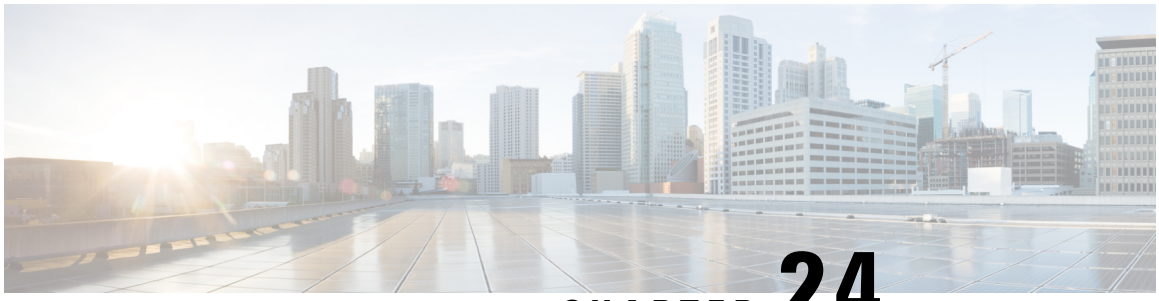
- Optional authentication of the UE
- Change of PCF during mobility
- Rejection/Clearing of PDU sessions

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 24

IPv6 Support on SBI Interface

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

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.

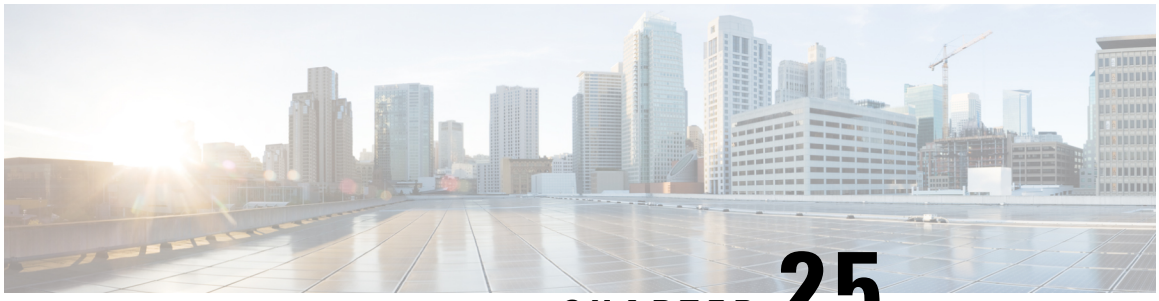
Configuration Example

The following is an example configuration for IPv4.

```
config
   instance instance-id 1
      endpoint sbi
         replicas 2
         loopbackPort 1000
         instancetype IPv4 vip-ip 209.165.200.224 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 209:165:200:225::4 vip-ipv6-port 1001
         end
```



CHAPTER 25

Low Mobility Handover (Xn/N2)

Feature Summary and Revision History

Summary Data

Table 93: 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 94: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

The low mobility handover feature supports the following functions:

- Handover cancel for N2 without AMF change
- Handover cancel for N2 with source and target AMF change

- Handover failure procedure with and without AMF change

AMF doesn't support the following:

- Collision
- Non-3GPP access
- Trace
- Event subscription
- PCF interactions

How It Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

N2 Handover Cancel Call Flow

This section describes the N2 Handover cancel call flow.

The source NG-RAN sends the Handover Cancel Request to the source AMF, before sending the Handover command to the UE.

It sends this request when it observes the following:

- Timer expiry
- Internal failure within the source NG-RAN
- UE return to source cell

The Handover Cancel Request releases the handover reserved resources in the target system.

Figure 41: N2 Handover Cancel Call Flow

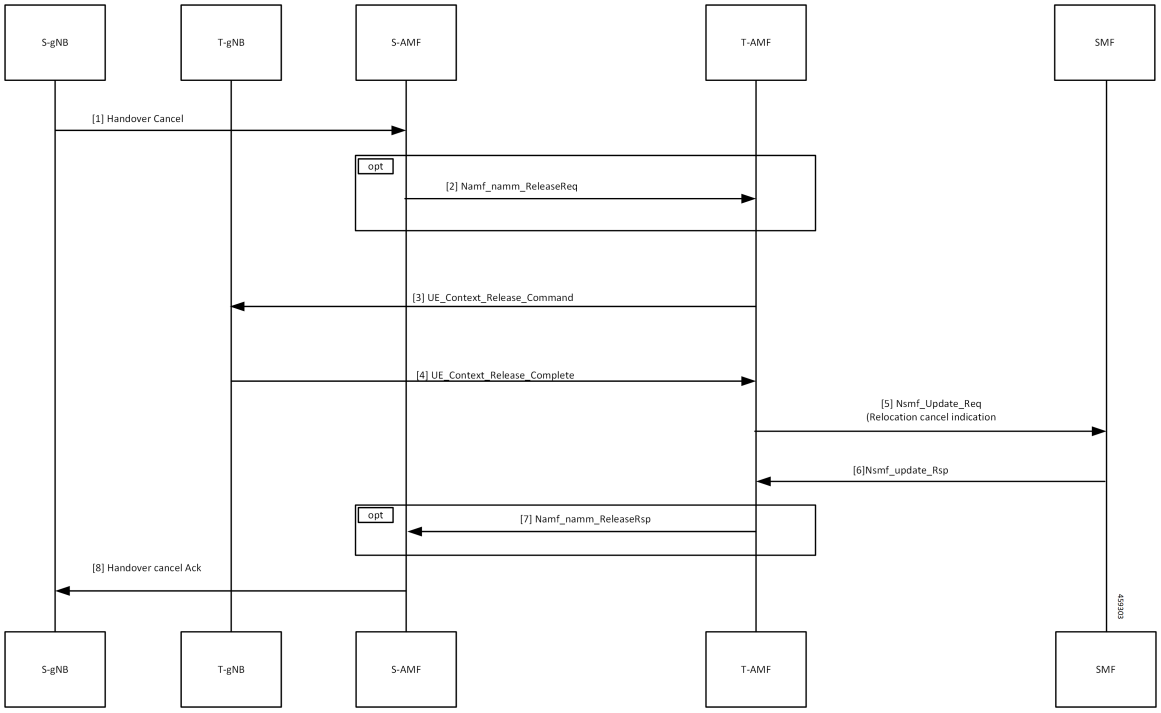
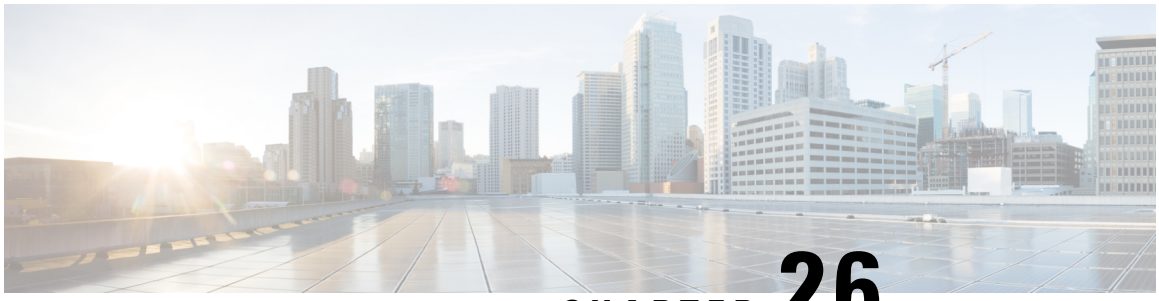


Table 95: N2 Handover Cancel Call Flow Description

Step	Description
1	The S-gNB (source gNB) sends the Handover Cancel to the S-AMF (source AMF).
2	The S-AMF sends the Namf_Comm_ReleaseReq to the T-AMF (target AMF).
3, 4	The T-AMF sends the UE Context Release Command to the T-gNB (target gNB) and receives the UE Context Release Complete.
5	The T-AMF sends the Relocation Cancel Indication (Nsmf_Update_Req) to the SMF.
6	The SMF sends Nsmf_update_Rsp to the T-AMF.
7	The S-AMF receives Namf_Comm_ReleaseRsp from the T-AMF.
8	The S-AMF sends Handover Cancel ACK to the S-gNB.



CHAPTER 26

Mobile Equipment Identity Check Procedures

Feature Summary and Revision History

Summary Data

Table 96: 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 97: 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 42: UE Identity Procedure for Authentication Failure Call Flow

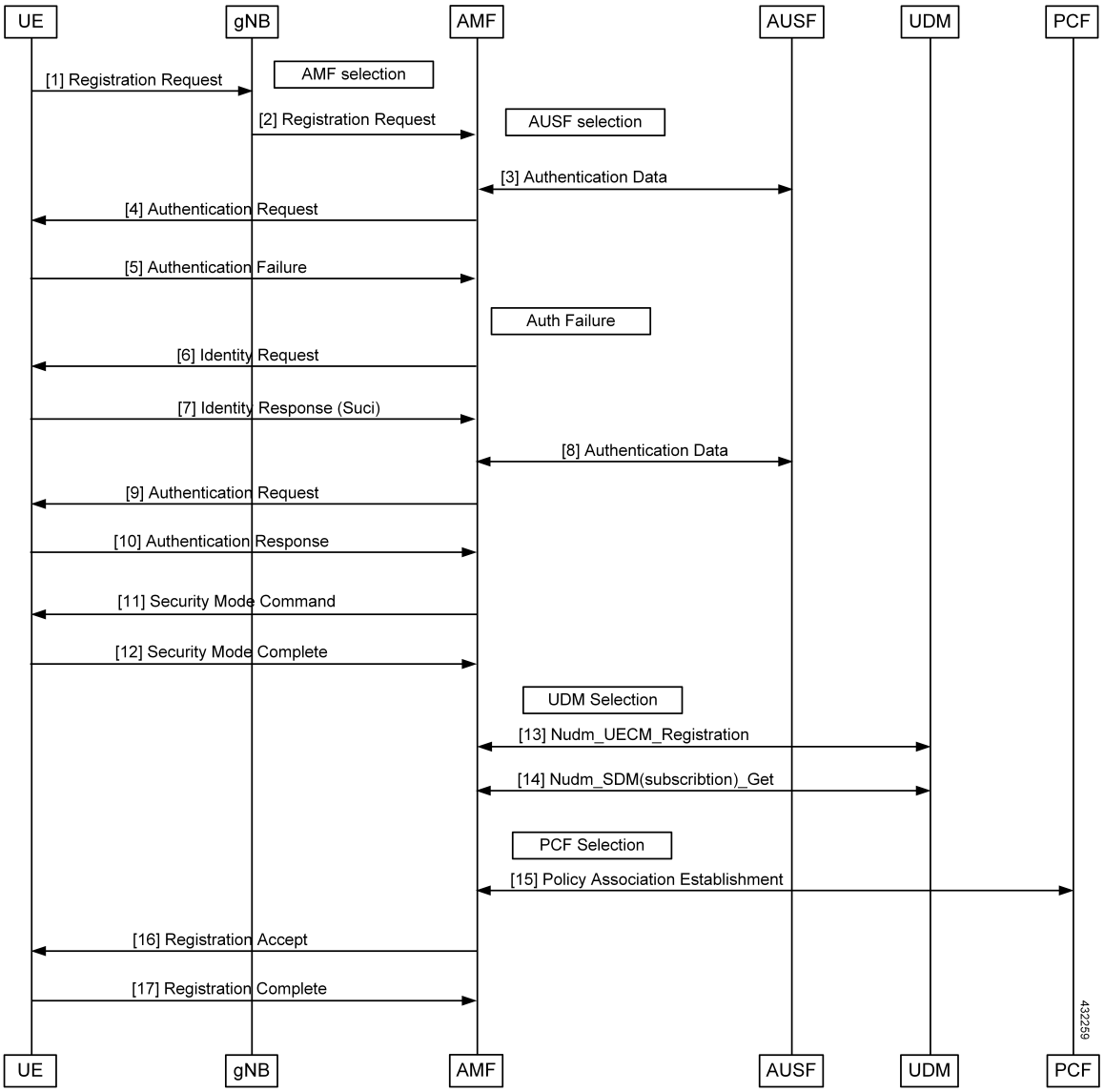


Table 98: UE Identity Procedure for Authentication Failure Call Flow Description

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 43: UE Identity Procedure for Unknown GUTI Registration Call Flow

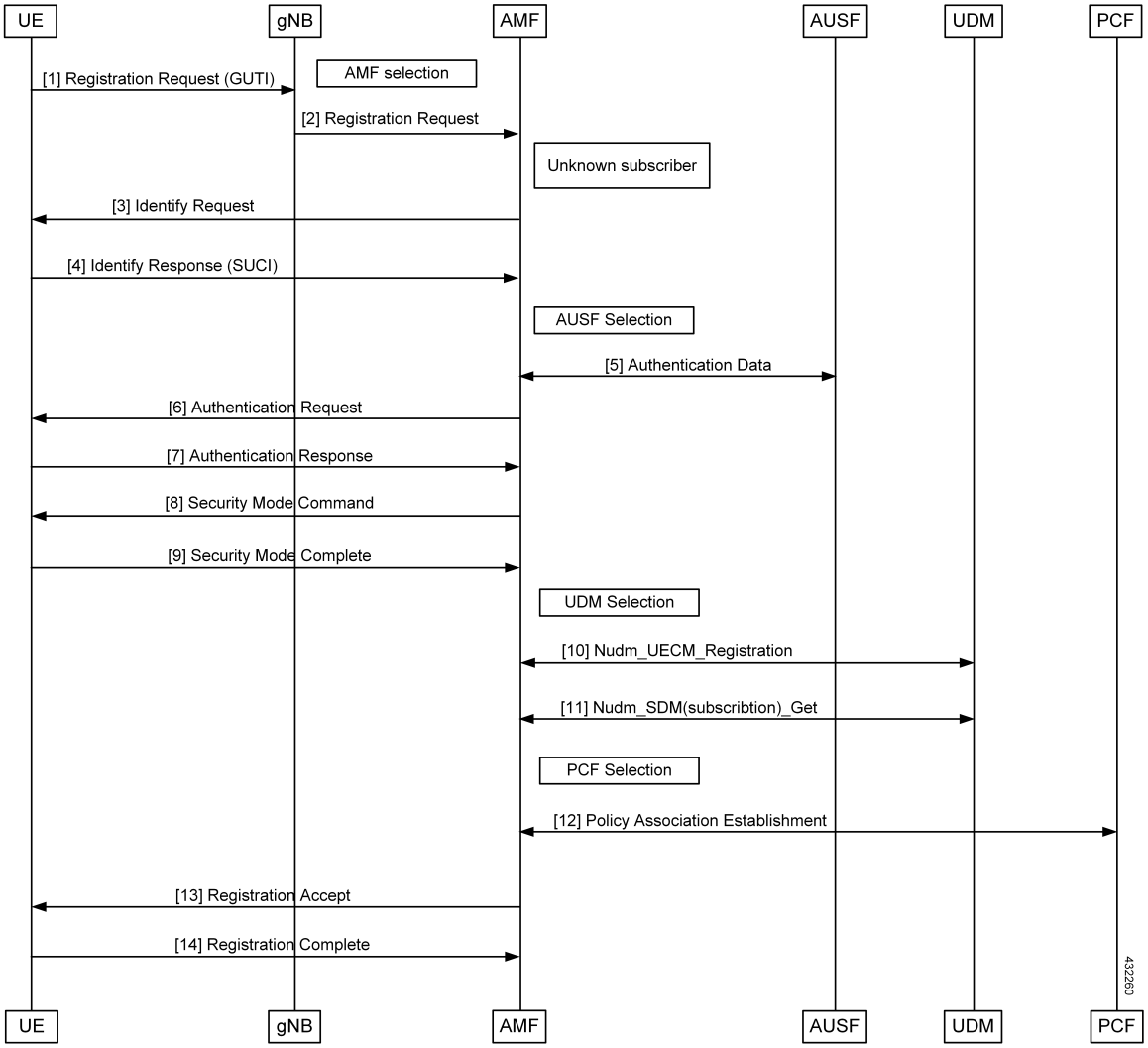
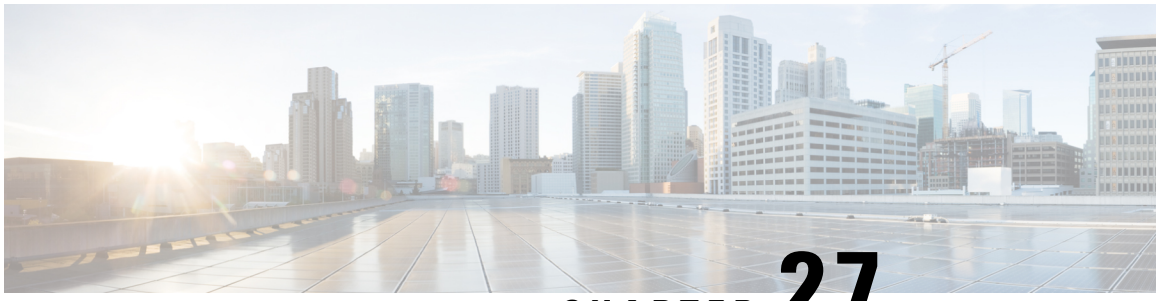


Table 99: UE Identity Procedure for Unknown GUTI Registration Call Flow Description

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 27

Mutual TLS (mTLS) Support and Validation

Feature Summary and Revision History

Summary Data

Table 100: Summary Data

Applicable Products or Functional Area	AMF
Applicable Platforms	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	For related information, see the *TLS Transport Support* chapter in this document.

Revision History

Table 101: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

The AMF supports the mutual TLS secure channel for SBI interfaces. With the mTLS Support for SBI interfaces, the AMF performs the following:

- Handles mutual TLS requests from the server and the client
- Supports HTTP2 over the TLS secure channel for all NF interfaces

This feature also supports in generating alarms when the certificates expire within a configured threshold period.

Relationships

The mTLS support for SBI interfaces feature has the relationship with TLS transport support feature. The following are the roles associated with the AMF:

- Server Configuration in AMF, on page 233
- Client Configuration in AMF, on page 234

For related information, see the *TLS Transport Support* chapter in this document.

Prerequisites

The mTLS Support for SBI interfaces feature has the following prerequisite:

- The user must procure and configure the following:
  - Certificate Authority (CA) certificates
  - Other certificates or keys necessary for the server and the client
- For more information on the following topics, see the *TLS Transport Support* chapter in this document.
  - For the client, and the server certificate configuration
  - For the ca-certificate configuration
  - For uri-scheme https, in the profile nf-client configuration

How it Works

This section describes how this feature works. It has the following synopsis:

- The TLS protocol is used for transport layer protection.
- The AMF supports TLS versions 1.2 and 1.3 for all inbound and outbound HTTPS, and outbound TCP transport.
- The AMF supports enabling mutual TLS for the SBI endpoint.

Limitations

This feature has the following limitations:

- The mTLS secure channel support feature for the AMF provides transport layer encryption between nodes for security compliance purposes only.
- The AMF doesn't support NF security requirements as per 3GPP specifications of 5G.
- The AMF supports L1-X1 over the UDP in Cisco format only. As a result, the AMF doesn't support the mTLS on the L1-X1 interface.
- The AMF doesn't support dynamic mTLS CLI change configuration.

Server Configuration in AMF

The AMF acts as the server for all peer NFs over the SBI interface.

The SBI interface servers characteristics are determined by **instance instance <id> endpoint sbi** configurations.

The server certificates get configured at the SBI endpoint.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   instance instance-id instance_id
      endpoint sbi
         uri-scheme {http | https}
         mtls-enable {false | true}
         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 as https. The default value is http.
- **mtls-enable {false | true}**—Specify the mTLS configuration as either true or false.
- **certificate-name** *certificate_name*—Specify the certificate name for the server which is used by AMF for HTTPS messages. The list of certificate names is obtained from the **nf-tls** command.

Configuration Example

The following is an example configuration.

```
config
 instance instance-id 1
  endpoint sbi
   uri-scheme https
```

```
  mtls-enable true
  certificate-name serv-cert
  exit
 exit
exit
```

Configuration Verification

To verify the configuration, use the following command:

```
amf# show running-config instance instance-id 1 endpoint sbi
```

Client Configuration in AMF

The AMF acts as client-to-peer NFs while sending notifications or updates. The characteristics of the client configurations are determined by using the **endpoint-profile** configuration. The server name gets configured, when the URI scheme is in a secured (HTTPS) environment for locally configured NF profiles and NRF-related configurations.

Feature Configuration

To configure this feature, use the following configuration. The following commands help in enabling the mTLS option along with the server name at the NF and NRF-related configurations:

```
config
   profile nf-client
      nf-type ausf
         ausf-profile AUP1
         locality LOC1
         service type nausf-auth
         endpoint-profile ep_profile_name
            type EP1
            locality LOC1
            uri-scheme https
            server-name server_name
   group nrf
      mgmt MGMT_name
         service type nrf nnrf-nfm
         endpoint-profile ep_profile_name
            name mgmt-prof
            uri-scheme https
            server-name server_name
   group nrf
      discovery udmdiscovery
         service type nrf nnrf-disc
         endpoint-profile ep_profile_name
            name EP1
            uri-scheme https
            server-name server_name
            end
```

NOTES:

- **profile nf-client nf-type ausf ausf-profile** *AUP1*—Specify the required NF client profiles and provide the local configuration.
- **service type nausf-auth** | **service type nrf nnrf-nfm** | **service type nrf nnrf-disc**—Specify the service names as per the 3GPP standards.
- **group nrf mgmt** *MGMT_name*—Specify the NRF self-management group configurations.
- **instance instance-id** *instance_id*—Specify the instance ID.
- **endpoint-profile** *ep_profile_name*—Specify the endpoint-profile name.
- **uri-scheme {http | https}**—Specify the uri-scheme as https. The default value is http.
- **server-name** *server_name*—Specify the **DNS name** (FQDN) of the peer NF and the **server-name** must match the DNS attribute of the **subjectAltName** field in the peer NF certificates.

Configuration Example

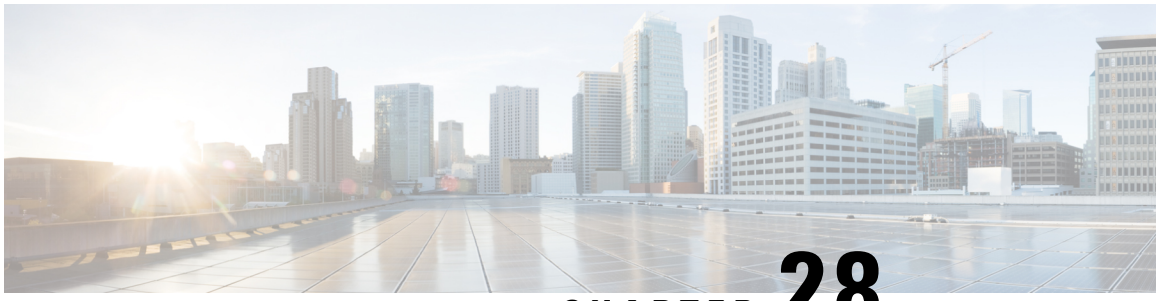
The following is an example configuration.

```
config
 group nrf mgmt MGMT
  service type nrf nnrf-nfm
   endpoint-profile
    name mgmt-prof
    uri-scheme https
    server-name server_name
    endpoint-name mgmt-1
     primary ip-address ipv4 209.165.201.1
     primary ip-address port 9051
    exit
   exit
  exit
 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 https
      server-name server_name
      endpoint-name EP1
       priority 56
       primary ip-address ipv4 209.165.201.1
       primary ip-address port 9047
      exit
     exit
    exit
   exit
  exit
 exit
```

Configuration Verification

To verify the configuration, use the following command:

```
amf(config)# show full-configuration profile
```



CHAPTER 28

N1N2 Message Transfer

Feature Summary and Revision History

Summary Data

Table 102: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on SMS over the Non-Access Stratum Procedures: Enabled - Configuration required to disable
Related Documentation	Not Applicable

Revision History

Table 103: Revision History

Revision Details	Release
Introduced ability to send SMS over the NAS procedure	2022.01.0
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

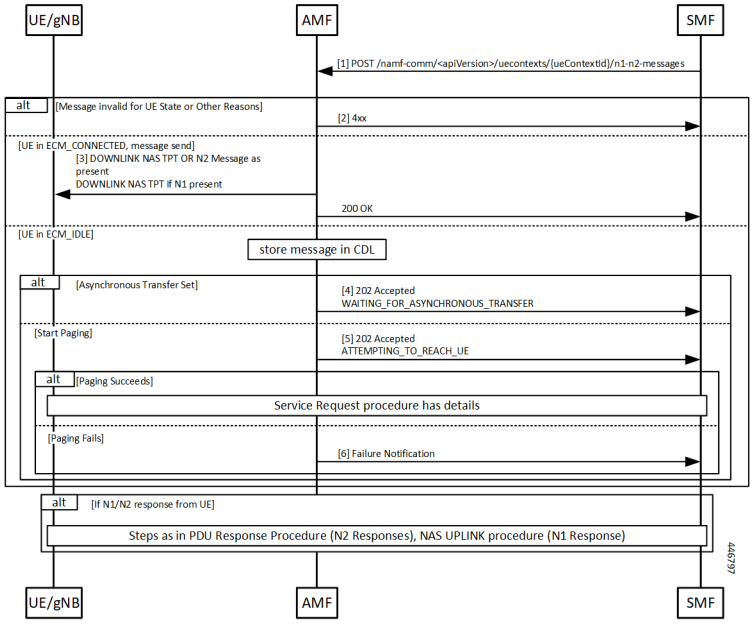
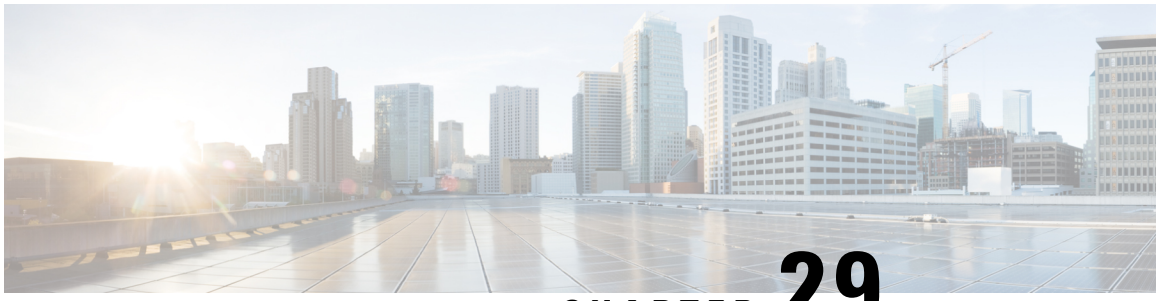


Table 104: N1N2 Message Transfer Call Flow Description

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 29

N2 Handover 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

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

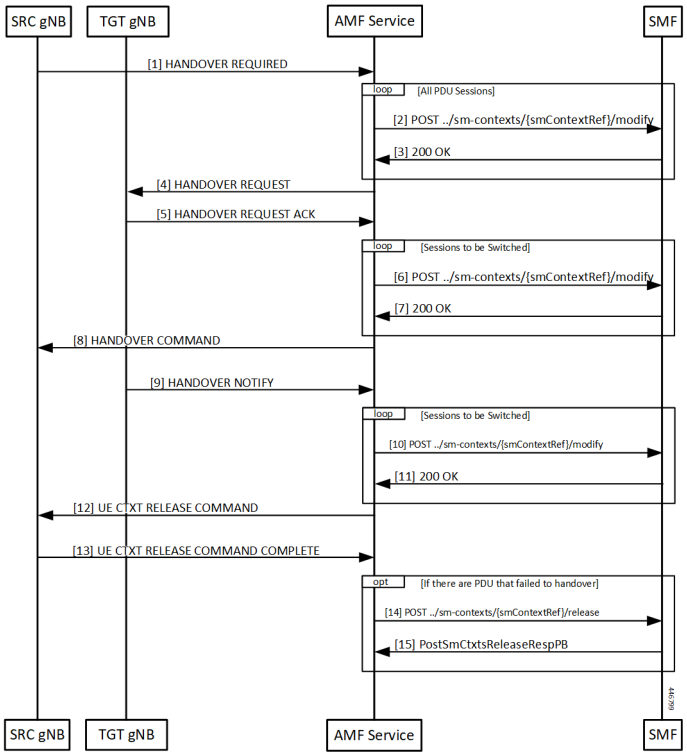


Table 107: N2 Handover without AMF Change Call Flow Description

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

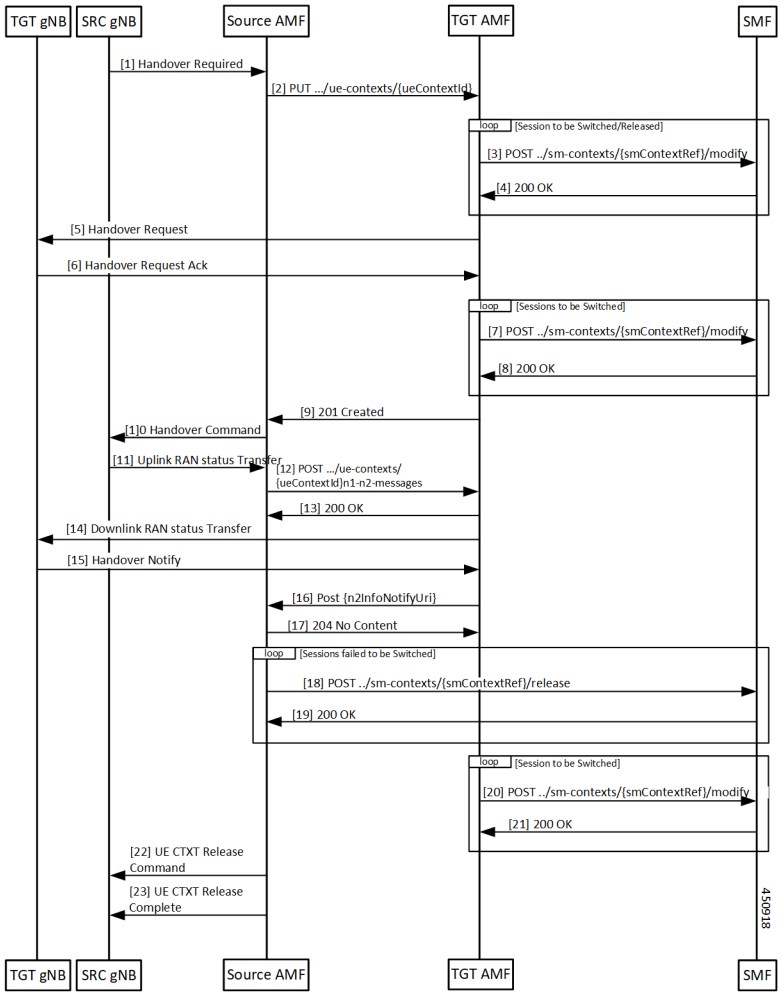
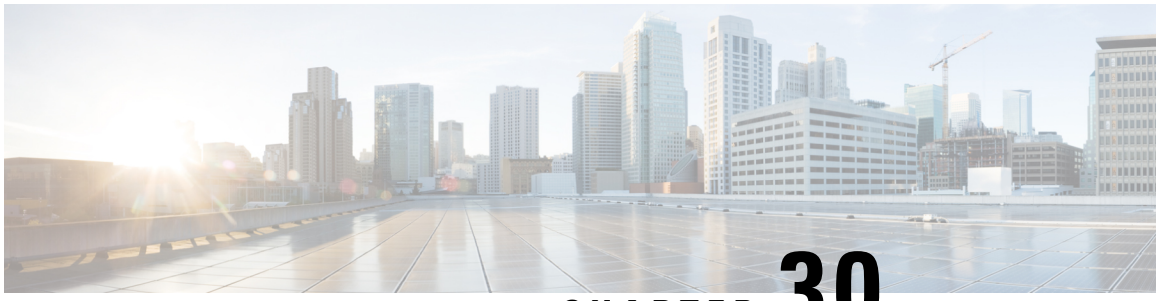


Table 108: N2 Handover with AMF Change Call Flow Description

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. **Note** In the CreateUE Context message, ncc remains absent, in the instance, when the value is 0.
3	The target AMF receives the message and verifies that it can serve the UE. For each PDU session that must be handed over, the AMF sends a Modify SM Context message to the SMF.

Step	Description
4	The SMF does all the necessary procedures that are 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.
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 in the gNB.
8	The SMF responds to the requests in 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 the release of resources in 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 in the source AMF.
16	The target AMF update the SMF on the completion of the handover.
17	The SMF acknowledges the message in 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 30

N26 Stack Integration Support

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.	2020.04

Feature Description

This feature supports the following:

- UDP Proxy and GTPC Endpoint

- EBI Allocation and Reallocation Support

UDP Proxy and GTPC Endpoint

Feature Description

AMF supports interworking procedures to work with EPS. The procedures use the GTP-C based N26 interface between AMF and MME. Interworking procedures with N26 provides IP address continuity on inter-system mobility to UEs that support 5GC NAS and EPS NAS and operate in single registration mode. Interworking procedures using the N26 interface enables the exchange of MM and SM states between the source and target network.

To support N26 interface, AMF needs to support UDP proxy and GTPC Endpoint.

- **UDP Proxy:** Single instance of UDP proxy running on the system. UPD proxy receives/sends the UDP packets to/from GTPC Endpoint.
- **GTPC Endpoint:** The GTPC Endpoint (GTPC EP) POD handles the GTPC messages between AMF and MME. In order to enable interworking between EPC and the NG core, N26 interface is used as an inter-CN interface between the MME and 5GS AMF.

EBI Allocation and Reallocation Support

Feature Description

AMF supports assigning EBI service for the requests received from NF consumer service. Also, partial fulfillment of requests is supported. When no resources are available on AMF, the request are rejected by AMF

Standard Compliance

- 3GPP TS 23.502 version 15.5.1 Release 15, Section 4.11.1.4
- 3GPP TS 29.518 version 15.4.0 Release 15, Sections 5.2.2.6, 6.1.3.2.4.3

Limitations

In this release, priority-based eviction of already assigned EBI is not supported.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flow of EBI Allocation and Reallocation Support feature.

The EBIAssignment service operation is used during the following procedures (see 3GPP TS 23.502 [3], clause 4.11.1.4):

- UE requested PDU Session Establishment including Request Types **Initial Request** and **Existing PDU Session** (Non-roaming and Roaming with Local Breakout (see 3GPP TS 23.502 [3], Section 4.3.2.2.1).
- UE requested PDU Session Establishment including Request Types **Initial Request** and **Existing PDU Session** (Home-routed Roaming (see 3GPP TS 23.502 [3], Section 4.3.2.2.2).
- UE or network requested PDU Session Modification (non-roaming and roaming with local breakout) (see 3GPP TS 23.502 [3], Section 4.3.3.2).
- UE or network requested PDU Session Modification (home-routed roaming) (see 3GPP TS 23.502 [3], Section 4.3.3.3).
- UE Triggered Service Request (see 3GPP TS 23.502 [3], Section 4.2.3.2) to move PDU Session(s) from untrusted non-3GPP access to 3GPP access.
- Network requested PDU Session Modification, when the SMF needs to release the assigned EBI from a QoS flow (see 3GPP TS 23.502 [3], Section 4.11.1.4.3).

The EBI Assignment service operation is sent by the SMF towards the AMF, to request the AMF to allocate EPS bearer ID(s) towards EPS bearer(s) mapped from QoS flow(s) for an existing PDU Session for a given UE. EBI allocation applies only to PDU Session(s) via 3GPP access supporting EPS interworking with N26. EBI allocation does not apply to PDU Session(s) via 3GPP access supporting EPS interworking without N26 or PDU Session(s) via non-3GPP access supporting EPS interworking.

SMF performs EBI Assignment service operation by invoking **assign-ebi** custom operation on the **individual ueContext** resource.

The following call flow shows the messaging that happens in the network. The components of the AMF are not specified here.

Figure 47: EBI Assignment Call Flow

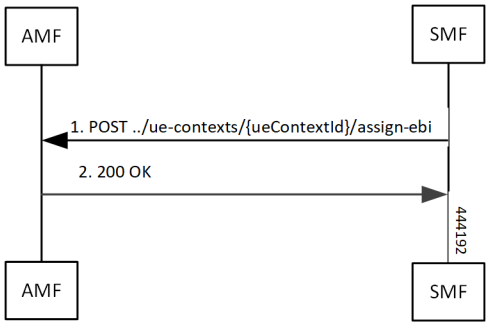
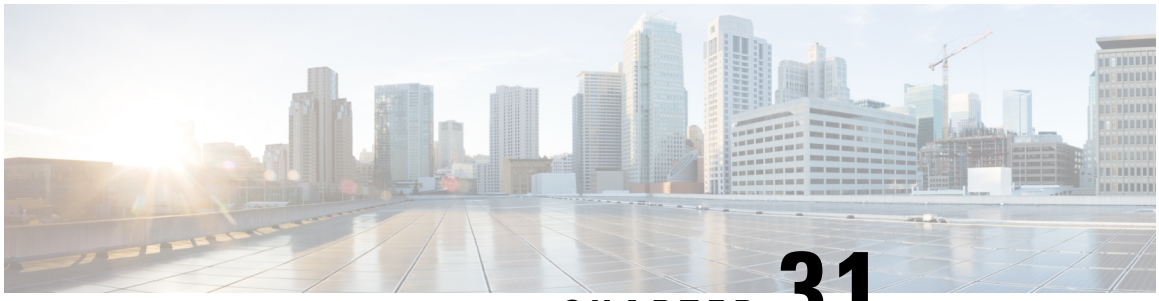


Table 111: EBI Assignment Call Flow Description

Step	Description
1	SMF sends Assign-ebi request to AMF.
2	AMF sends 200 *OK* message to AMF



CHAPTER 31

N26-based Handover Procedures - EPC Interworking

Feature Summary and Revision History

Summary Data

Table 112: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	

Revision History

Table 113: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

The N26 interface supports the following handover procedures:

- 5G to 4G (EPC) Handover
- 4G to 5G Handover

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

5G to 4G Handover Call Flow

This section describes the 5G to 4G handover call flow.

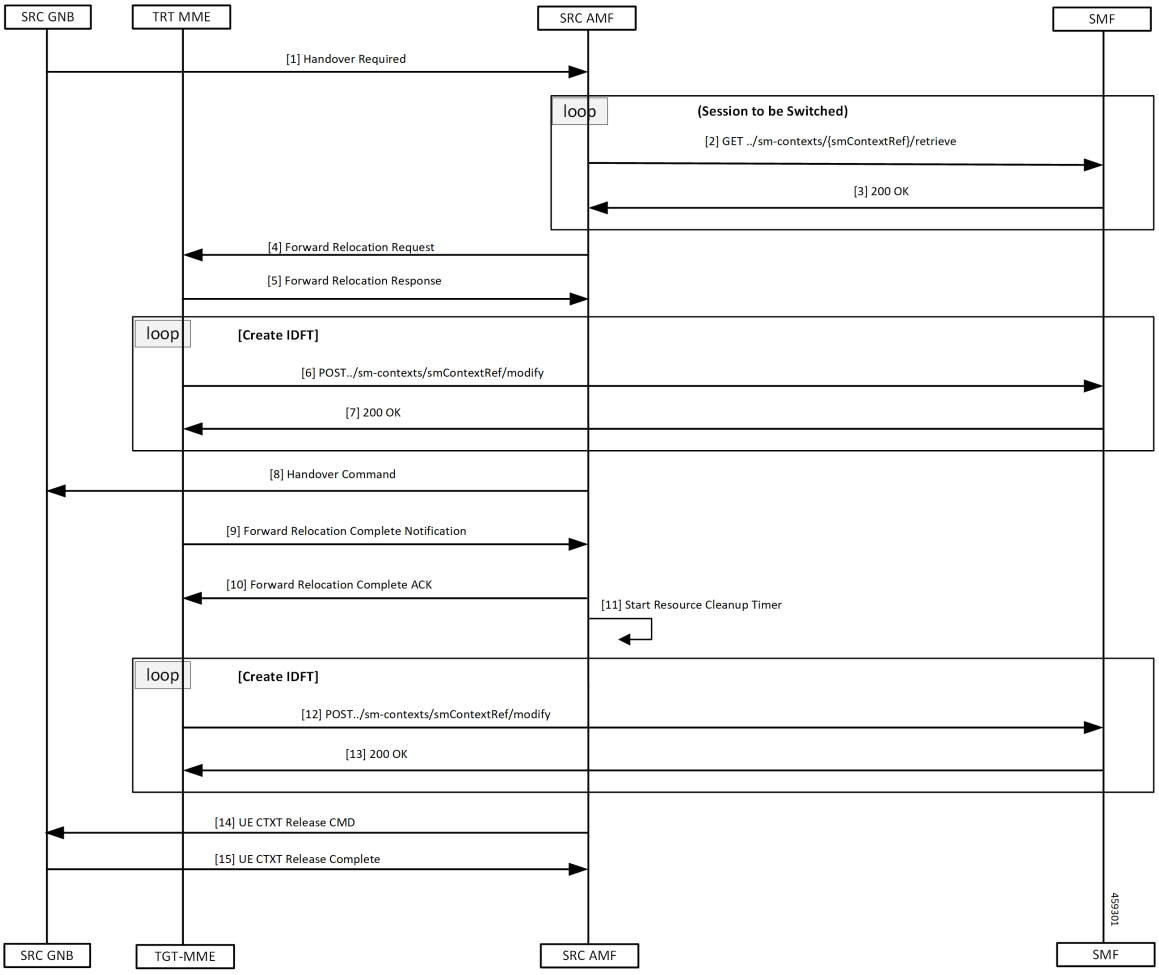


Table 114: 5G to 4G Handover Call Flow Description

1	The SRC GNB (source gNB) sends a Handover Required message to the SRC AMF (source AMF).
2, 3	The source AMF finds MME based on the received target ID. AMF finds the MME IP address through the AMF configuration or NRF discovery for the matching target ID.
4	When source AMF finds the IP address, it sends a Forward Relocation Request to the TGT-MME (target MME).
5	The target MME sets up resources at the enodeB, updates the S-GW, and responds to the source AMF with Forward Relocation Reponse.
6, 7	AMF requests SMF to setup Indirect Forwarding Tunnels. The SMF responds to the request from the AMF.
8	The source AMF sends a Handover Command to the source gNB.
9	As the handover completes on the MME, the target MME notifies the source AMF by sending a Forward Relocation Complete Notification.
10	The source AMF responds with a Forward Relocation Complete ACK to target MME.
11	The AMF starts a timer to clean up all the local resources and indirect tunnels.
12, 13	The AMF requests the SMF to clean up the IDFT tunnels created. The SMF responds to the AMF request.
14	The source AMF sends a UE Context Release Command to the source gNB to clean up all the resources at source gNB.
15	The source gNB responds with a UE Context Release Complete to the source AMF.

4G to 5G Handover Call Flow

This section describes the 4G to 5G handover call flow.

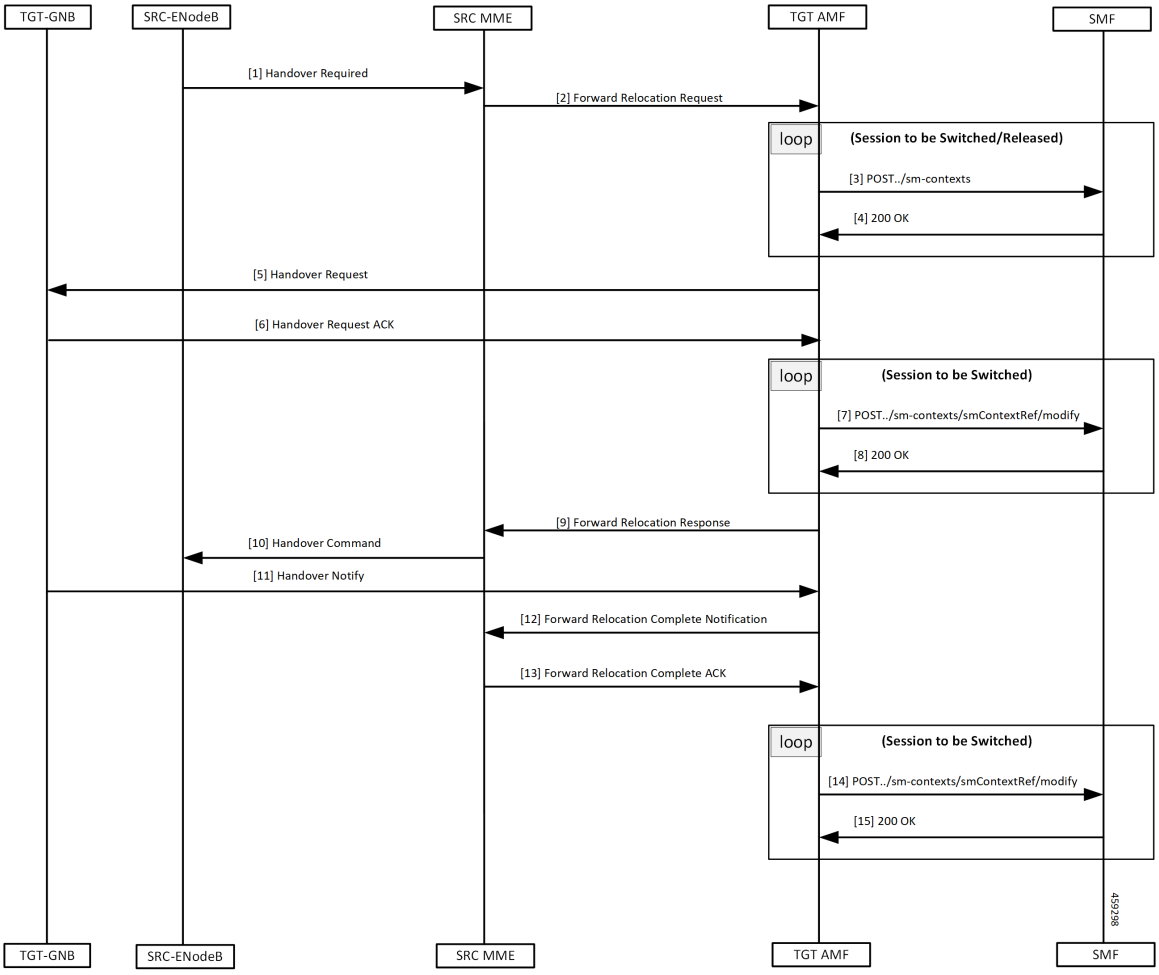


Table 115: 4G to 5G Handover Call Flow Description

Step	Description
1	As the UE transitions to 5GC, the SRC-ENodeB (source eNB) sends a Handover Required message to the SRC MME (source MME).
2	The MME does target-ID analysis, and chooses the TGT AMF (target AMF). The source MME sends a Forward Relocation Request to the TGT AMF (target AMF).
3	The target AMF creates associations with the SMF for the PDU sessions that are acceptable on the target AMF.
4	The SMF responds to the Create Request from the target AMF.
5	The target AMF selects the TGT GNB (taget gNB) that serves the UE, and sends a Handover Request to the target GNB.
6	After the GNB has allocated resources to the UE, it responds with a Handover Request ACK to the target AMF.

Step	Description
7, 8	The target AMF updates the SMF with information from the target GNB.
8	The SMF responds to the target AMF.
9	The target AMF responds to the request from the source MME using a Forward Relocation Response message.
10	The source MME sends a Handover Command to the SRC ENodeB (source eNB) to complete the handover.
11	Target gNB sends a Handover Notify to the target AMF when the UE handover gets completed.
12	The target AMF notifies the source MME using a Forward Relocation Complete notification.
13	The source MME acknowledges the message with a Forward Relocation Complete acknowledge.
14, 15	The target AMF notifies the SMF on the completion of the handover. The SMF acknowledges the notification.

Note When AMF receives the Registration Request message, it performs the following:

- When the message is received in Uplink NAS Transport, it assumes that the HO is successful and doesn't send the Context Request to the MME.
- When the message is received in Initial UE message, it sends the Context Request to the MME.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"*
- *3GPP TS 23.502 "Procedures for the 5G System (5GS)"*
- *3GPP TS 29.274 "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"*

Limitations

N26-based handover doesn't support the following:

- Handling of PGW-C-initiated and SMF-initiated N2 request by AMF, when other handover is in progress
- Non-IP PDN type
- Home routed roaming
- Direct tunneling

- Emergency fallback
- N3 Interworking Function

In this release, AMF doesn't capture GTPC messages as part of `monitor subscriber` output.

Feature Configuration

Configuring this feature involves the following steps:

- Configure 4G to 5G handover—This configuration provides the commands for the handover between EPC to 5GC. For more information, refer to Configuring the Handover from 4G to 5G, on page 256.
- Configure 5G to 4G handover—This configuration provides the commands for the handover between 5GC to EPC. For more information, refer toConfiguring the Handover from 5G to 4G, on page 256.

Configuring the Handover from 4G to 5G

To configure this feature, use the following configuration:

```
config
    amf-global
        call-control-policy policy_name
            default-slice name n26 sst sst_value sdt sdt_value
            end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the policy name.
- **default-slice name n26 sst** *sst_value* **sdt** *sdt_value*—Specify the Slice/Service type (SST) value and Slice Differentiator Type (SDT) value respectively. SST value must be an integer in the range of 0-255. SDT value must be a string.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy ccp1
         default-slice name n26 sst 12 sdt 123456
            end
```

Configuring the Handover from 5G to 4G

To configure this feature, use the following configuration:

```
config
    amf-services service_name
       peer-mme tai-match priority priority_value mcc mcc_value mnc mnc_value tac
 tac_value [ to end_tac_value ] address mme_address
        exit
```

```
instance instance-id instance_id
   endpoint protocol
      vip-ip ip_address
      exit
   endpoint gtp
      nodes node_replicas
      retransmission { max-retry maximum_number_of_retries | timeout
retransmission_timeout_value }
      end
```

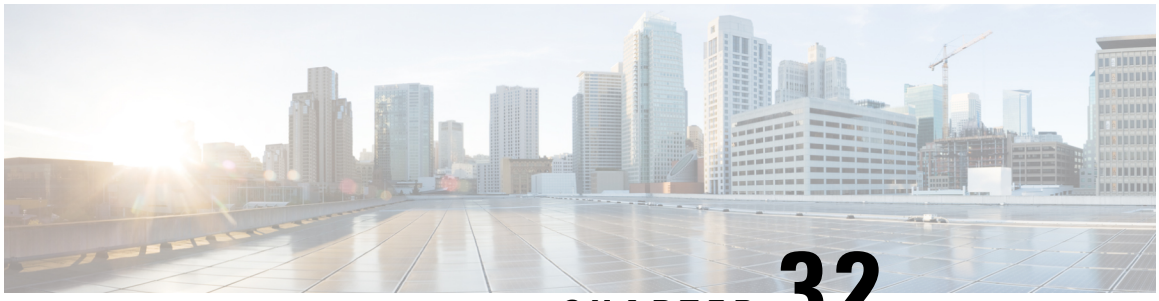
NOTES:

- **peer-mme tai-match priority** *priority_value* **mcc** *mcc_value* **mnc** *mnc_value* **tac** tac_value **[to** *end_tac_value* **] address** *mme_address*
  - **peer-mme tai-match priority** *priority_value*—Specify the priority value.
  - **mcc** *mcc_value*—Specify the three-digit Mobile Country Code. Must be an integer with three digits.
  - **mnc** *mnc_value*—Specify the two or three-digit Mobile Country Network. Must be an integer with three digits.
  - **tac** *tac_value*—Specify the Tracking Area Code value. Must be an integer in the range of 1-65535.
  - **to** *end_tac_value*—Specify the Tracking Area Code range for peer MME.
  - **address** *mme_address*—Specify the peer MME address.
- **nodes** *node_replicas*—Specify the replica nodes for resiliency.
- **max-retry** *maximum_number_of_retries*—Specify the number of request retry attempts. Must be an integer in the range 0–5 (default value: 3). To disable retransmission, set this value to zero (0).
- **timeout** *retransmission_timeout_value*—Specify the retransmission interval in seconds. Must be an integer in the range 0–10 (default value: 2). To disable retransmission, set this value to zero (0).

Configuration Example

The following is an example configuration.

```
config
   amf-services amf1
      peer-mme tai-match priority 1 mcc 311 mnc 480 tac 30 address 209.165.200.224
      exit
   instance instance-id
      endpoint protocol
         vip-ip 209.165.200.225
         exit
      endpoint gtp
         nodes 1
         retransmission timeout 2 max-retry 5
         end
```



CHAPTER 32

Network-Initiated Deregistration Request

Feature Summary and Revision History

Summary Data

Table 116: 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 117: 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 48: Purge of Subscriber Data in AMF Call Flow

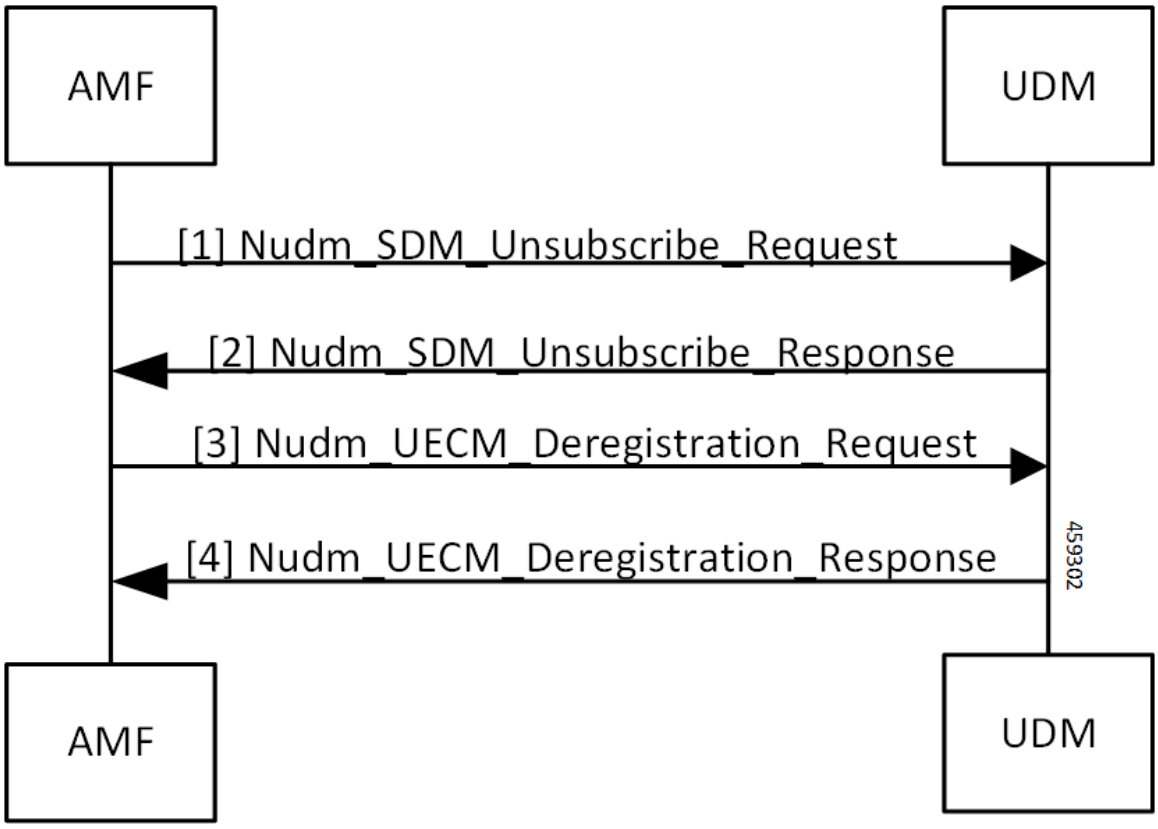


Table 118: Purge of Subscriber Data in AMF Call Flow Description

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.

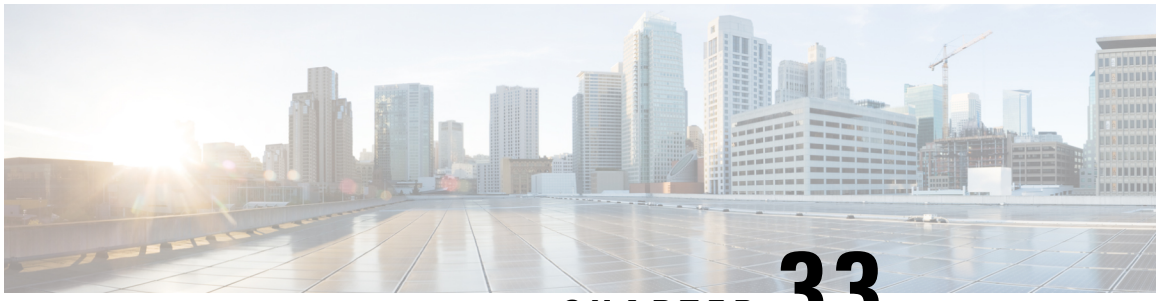
  Default purge timer value is 86400 seconds.

  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 33

Network Slicing Support

Table 119: Feature History

Feature Name	Release Information	Description
Network Slicing Support	2024.01	Cisco AMF allows the slice selection and reallocation during the UE registration. Default Setting: Disabled – Configuration Required

Feature Summary and Revision History

Summary Data

Table 120: 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 121: Revision History

Revision Details	Release
First introduced.	2023.04.0

Feature Description

Slice selection is the process of choosing a specific network slice supported by the network. The AMF supports the network slice selection during the registration. The AMF selects the slice based on the requested NSSAI, subscription data from UDM, locally configured slices, and slicing information received from NSSF. Upon successful UE registration, the AMF conveys the allowed NSSAIs to both the AN (gNB) and the UE, so that UE uses the appropriate slice to access the required services.

If AMF is unable to serve any of the slices requested by the UE, the AMF initiates the re-allocation functionality. AMF supports redirection of registration request message through the direct signaling to selected target AMF (received in NSSF response) or by rerouting the NAS message to target AMF through RAN.

When the AMF receives an indication from the UDM about change in slice subscription, the AMF informs the UE with new allowed/rejected and configured slices using UE configuration update procedure.

How it Works

This section describes how this feature works.

Call Flows

This section describes about the various call flows pertaining to this feature:

Figure 49: Slice Selection

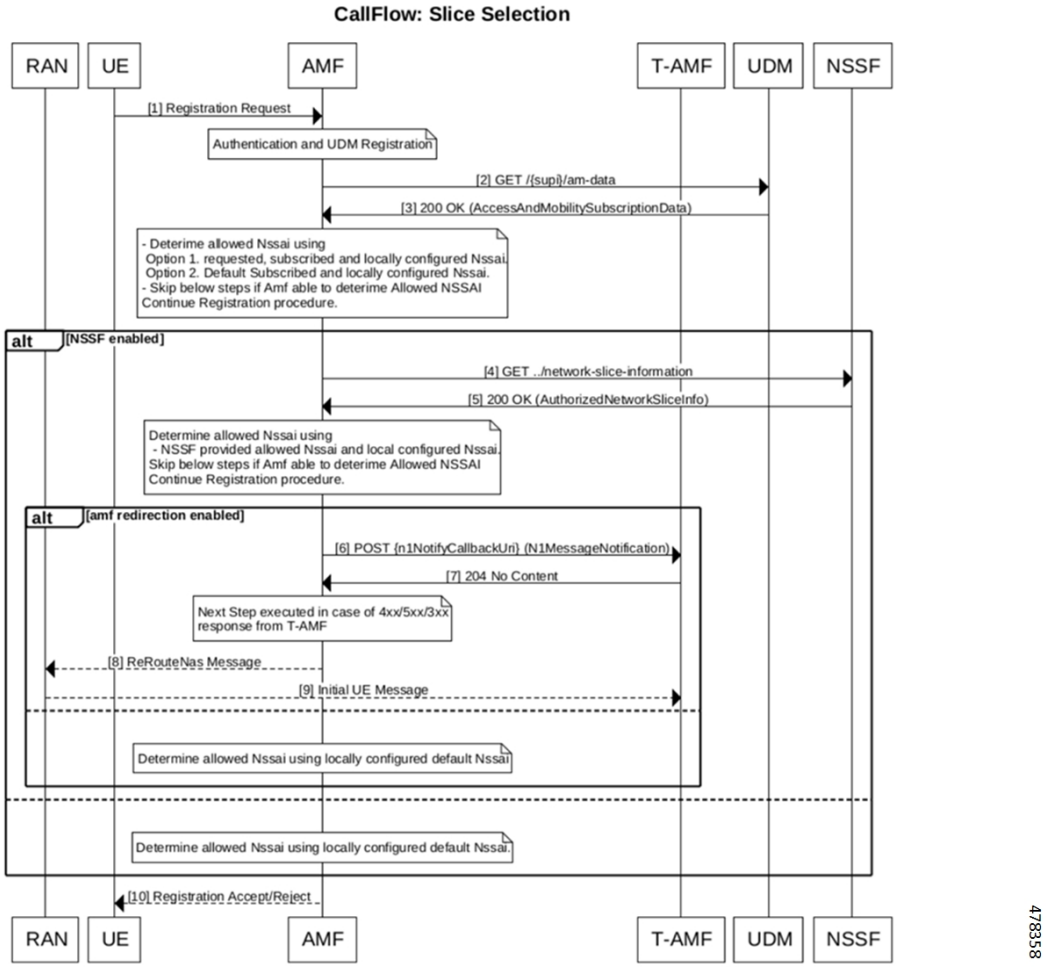


Table 122: AMF Slice Selection

Step	Description
1	UE Requested NSSAI are matched with local configuration and with the subscribed SNSSAI received from UDM. For local configuration, AMF service level NSSAI needs to be configured.
2	If there is no match, then next step is to match the default SNSSAI from UDM with local slice configuration.
3	If there is no match, and if the NSSF interaction is enabled then query NSSF and make slice selection request: • Get allowed NSSAI list and configured NSSAI from slice selection response and match with local configured slice. • If NSSF interaction is not enabled, accept the subscriber with locally configured default-NSSAI. **Note** NSSF is locally configured in the AMF.

Step	Description
4	If there is no match, and if AMF redirection is enabled, use targetAmfSet or candidateAMF from slice selection response and proceed with AMF relocation else accept subscriber with locally configured default-NSSAI.
5	If slice matches, continue with registration procedure. **Note** The Global/PLMN level slices information are considered as local configuration. **1.** If UDM doesn't provide subscribed S-NSSAIs, it considers the default S-NSSAIs for comparison. • Allowed NSSAIs in registration accept: The matching S-NSSAIs are considered as allowed NSSAIs and are filled in registration accept message. • Rejected NSSAIs in registration accept: The AMF may include this IE to inform the UE of one or more S-NSSAIs that were included in the requested NSSAI in the REGISTRATION REQUEST message but were rejected by the network. • Configured NSSAIs in registration accept: The AMF may include a new configured NSSAI for the current PLMN in the REGISTRATION ACCEPT message if: • The REGISTRATION REQUEST message doesn't include the requested NSSAI. • The REGISTRATION REQUEST message includes the requested NSSAI containing a S-NSSAI that is not valid in the serving PLMN. • The REGISTRATION REQUEST message includes the network slicing indication IE with the default configured NSSAI indication bit set to "Requested NSSAI created from default configured NSSAI".
6	The AMF obtains the configured S-NSSAI by utilizing locally configured PLMN-level slice and subscription details. **Note** In case of registration reject due to the cause set to 62 - “No network slices available”. The AMF provides rejected NSSAI in registration accept/reject with the cause "S-NSSAI not available in the current PLMN or SNPN" unless calculated by NSSF.
7	If UDM includes “provisioningTime” (in NSSAI IE) in subscription response. The AMF provides acknowledgment (/am-data/subscribed-snssais-ack) to UDM after receiving registration complete.

AMF Reallocation

Following are the call flows for the reallocation procedure.

Figure 50: Source AMF

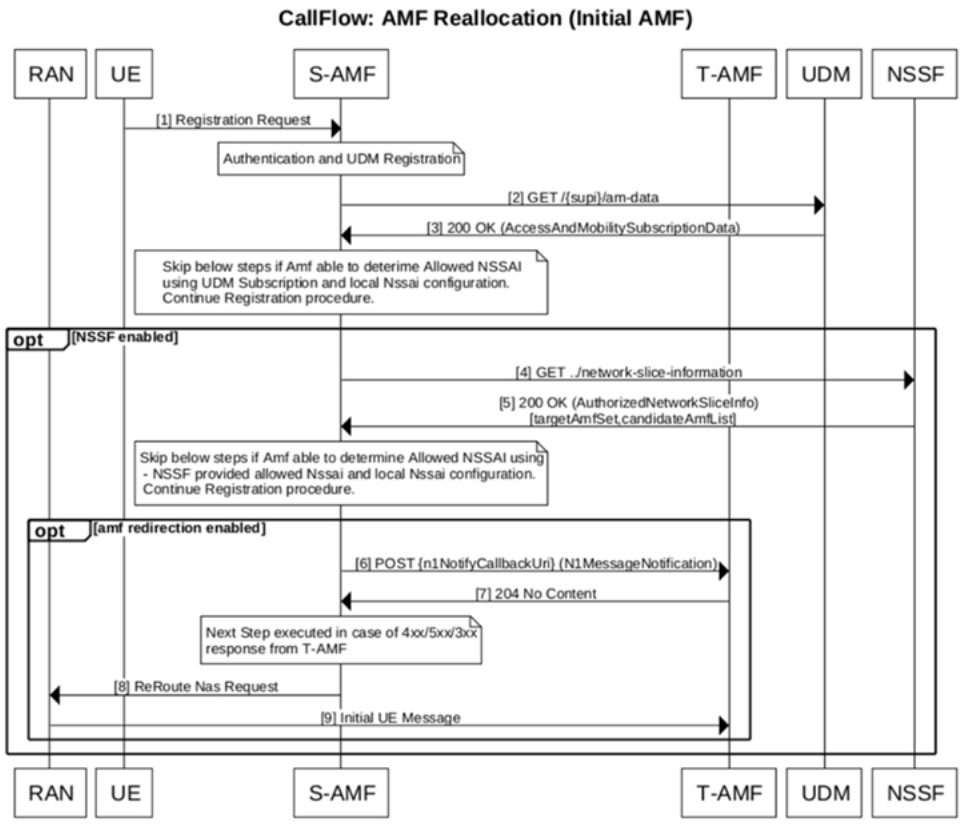


Table 123: Source AMF

Step	Description
1	The AMF redirection uses the "N1MessageNotify" message which is callback API (that means, it uses notification-subscription framework).
2	All AMFs needs to be pre-registered with NRF with “defaultNotificationSubscription”. It includes callback URL for N1MessageNotify.
3	The AMF uses the locally configured NRF (not received from NSSF) in slice selection response.
4	From the discovered AMFs, the source AMF sends N1MessageNotify message to callback URL.

Step	Description
5	If multiple instance Id's are received as part of candidate AMF List, then the S-AMF initiates a N1 message notify to T-AMF selected based on first instance id and if receives status other than 204 in N1 Message Notify Response, then it initiates the request again to target selected based on next instance id in candidate AMF List.
6	In case NRF is not available, local configuration is supported for destination AMF IOT only: • TargetAmfSet" needs to be configured as endpoint-profile name and • "CandidateAMF" needs to be configured as endpoint-name under NF-client profile.
7	The AMF reroutes the message through the RAN (REROUTE NAS REQUEST)if direct signaling to target AMF fails.

Figure 51: Destination AMF

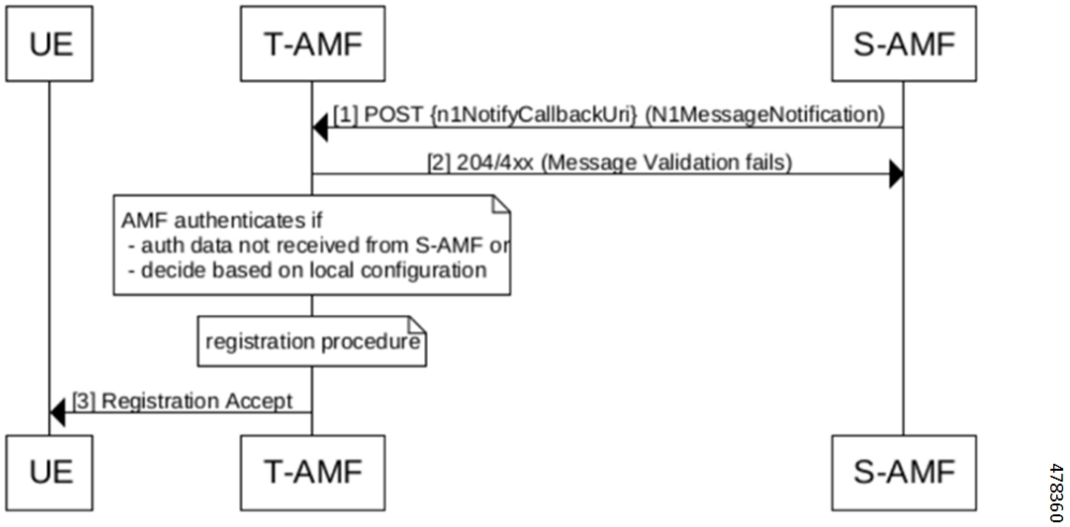


Table 124: Destination AMF

Step	Description
1	The target AMF upon receiving N1Message notify decodes the message and extracts the UEContext, location information, and gNB information
2	The AMF authenticates the subscriber based on local configuration and in case authentication data is not received from source AMF then it continues with the registration procedure with details received. **Note** If gNB is not connected to the AMF, then the registration fails.

Slice Update Notification

Following are the call flows for the slice update notification.

Figure 52: UE Configuration Update for UDM Subscription Change

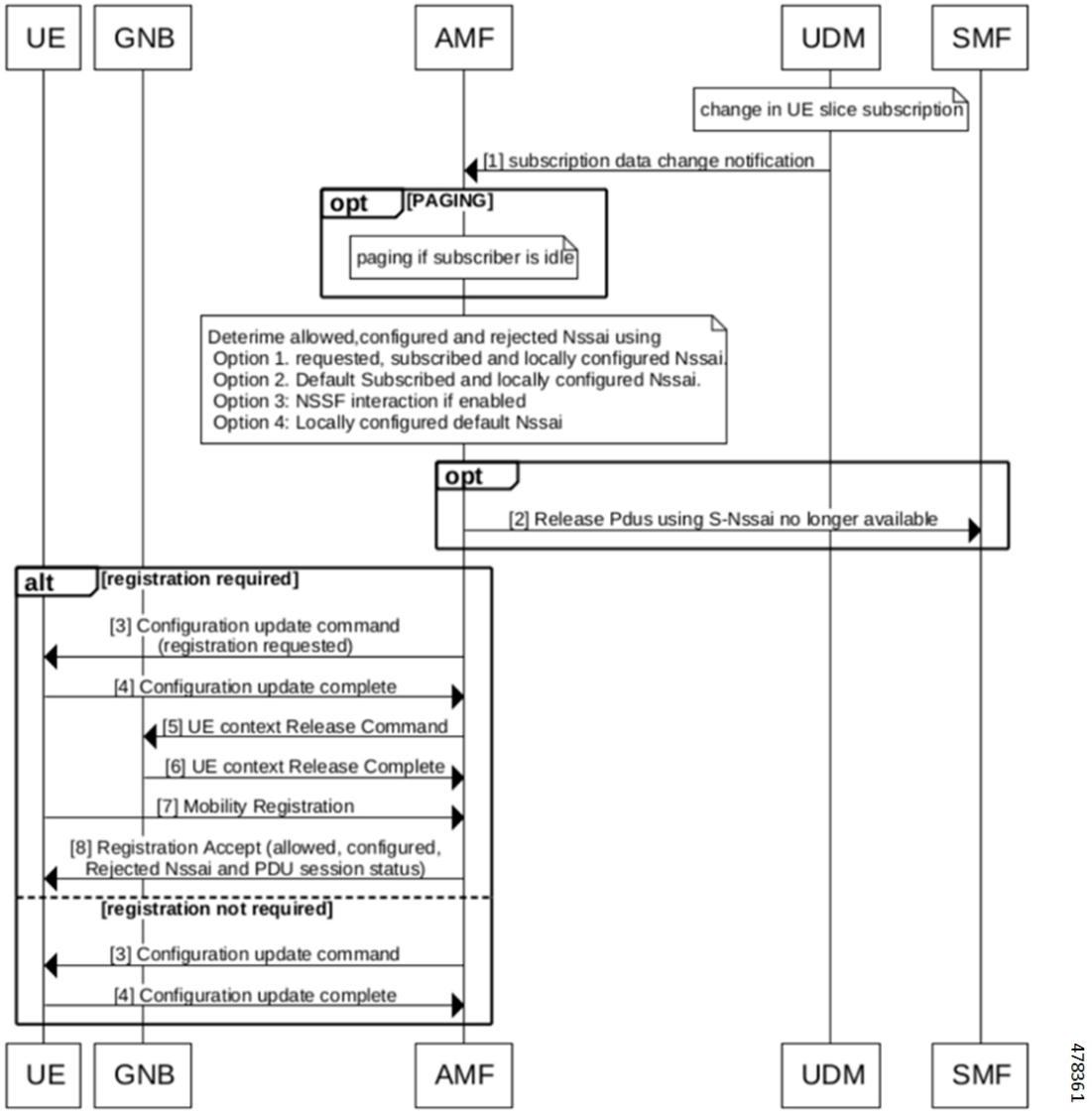


Table 125: UE Configuration Update for UDM Subscription Change

Step	Description
1	The UDM sends the notification to AMF when “subscription data for network slicing changes”.

Step	Description
2	The AMF re-calculates the slice information based on local configuration or using NSSF. If there is any change in slice (allowed-NSSAI, rejected-NSSAI, and configured NSSAI), then the amf-service sends the UE configuration update. The AMF provides UE with: • an indication that the acknowledgment from UE is required. • Allowed S-NSSAIs, configured S-NSSAIs for the Serving PLMN (if required), rejected S-NSSAI(s) (if required). • If the changes to the allowed NSSAI require the UE to perform immediate registration procedure because they affect the existing connectivity to network slices. The serving AMF indicates to the UE the need for the UE to perform a registration procedure.
3	When a network slice used for a one or multiple PDU Sessions is no longer available for a UE, the following applies: • The AMF releases a non-emergency PDU session for which network slice is no longer available and indicates SMF to release such PDUs. • The AMF modifies the PDU session status correspondingly. The PDU session(s) context is locally released in the UE after receiving the PDU session status in the registration accept message.
4	If UE is in the connected mode then UE configuration Update is sent else AMF triggers paging.
5	After receiving the acknowledgment, the AMF releases the NAS signaling connection for the UE in case of registration requested by AMF.
6	If there are established PDU session (s) associated with emergency services, then the serving AMF indicates to the UE the need for the UE to perform a registration procedure but doesn't release the NAS signaling connection to the UE. The UE performs the registration procedure only after the release of the PDU session (s) used for the emergency services.
7	The AMF rejects any NAS Message from the UE carrying PDU session establishment request for a non emergency PDU session before the required registration procedure has been successfully completed by the UE.
8	In case configuration update fails (example, subscriber not reachable): • The AMF releases a non-emergency PDU session for which network slice is no longer available and indicates SMF to release such PDUs. • The new calculated slice is provided when subscriber perform initial/mobility registration. • In case N1N2 or service request comes, the AMF sends the configuration update after handling the incoming message.

Note The configuration update doesn't happen for emergency subscriber.

Figure 53: Idle Time Expiry

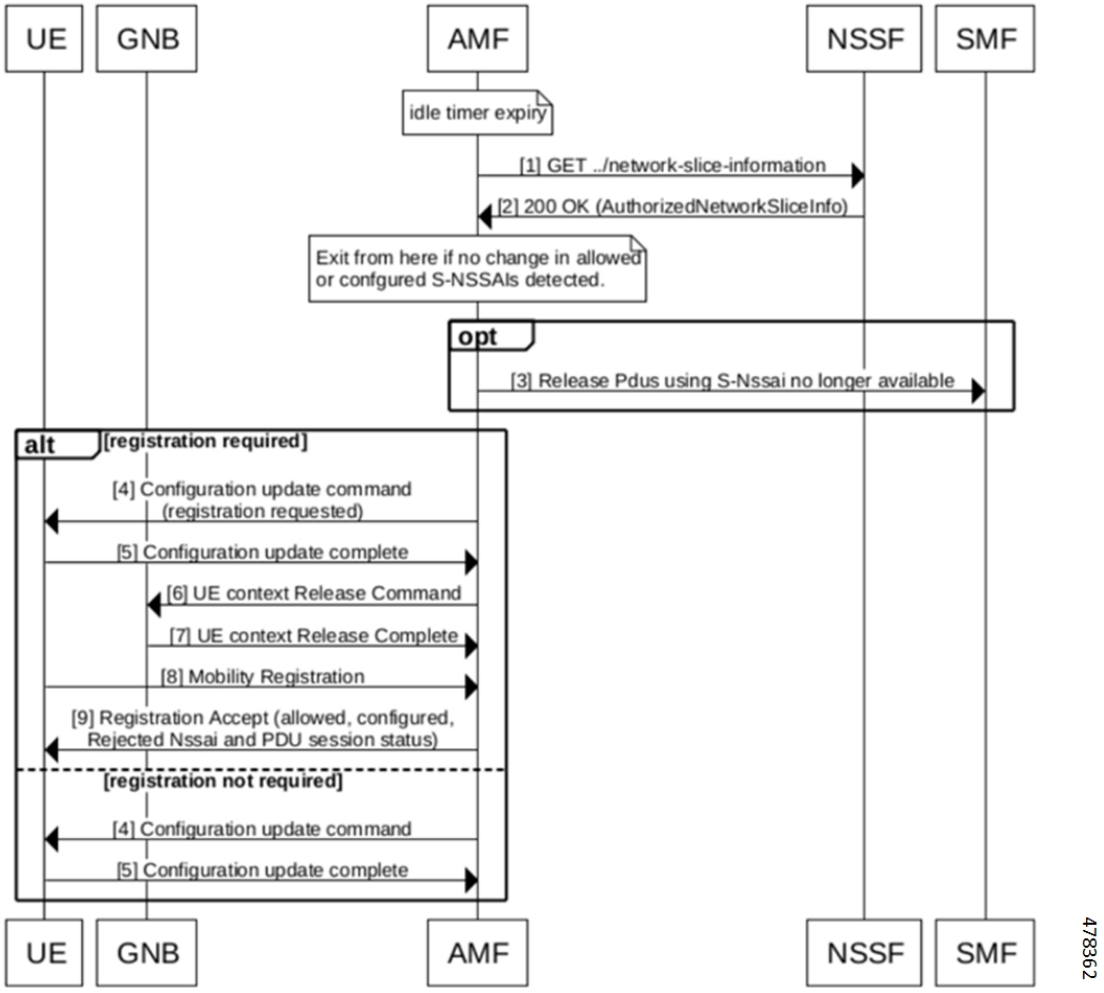
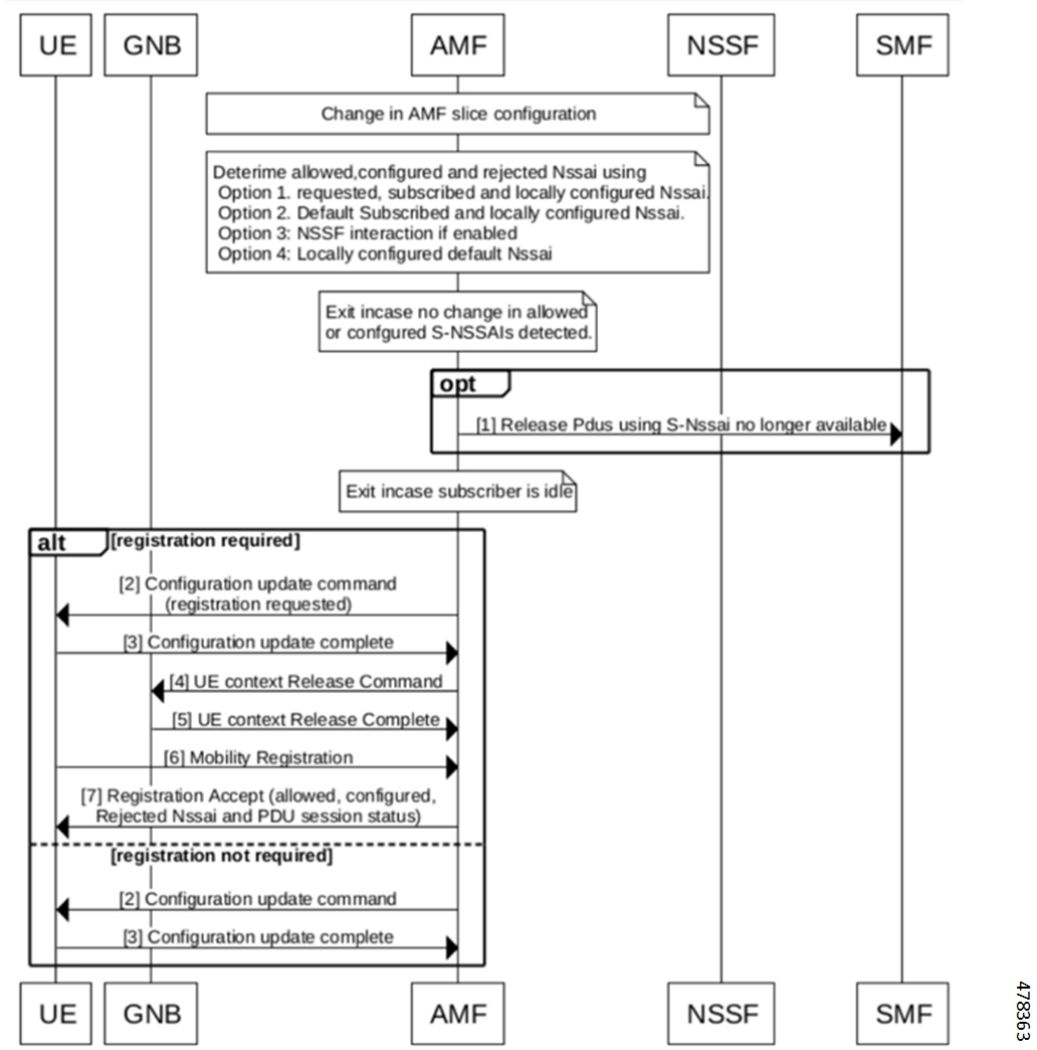


Table 126: Idle Time Expiry

Step	Description
1	On idle timer expiry, The AMF re-calculates the slice information using NSSF. **Note** prerequisite is to enable the configuration for "Enabling the UE Configuration Update".
2	The UE configuration update is sent only for those subscriber for which the NSSF was used previously for slice selection.

Figure 54: Slice Configuration Change

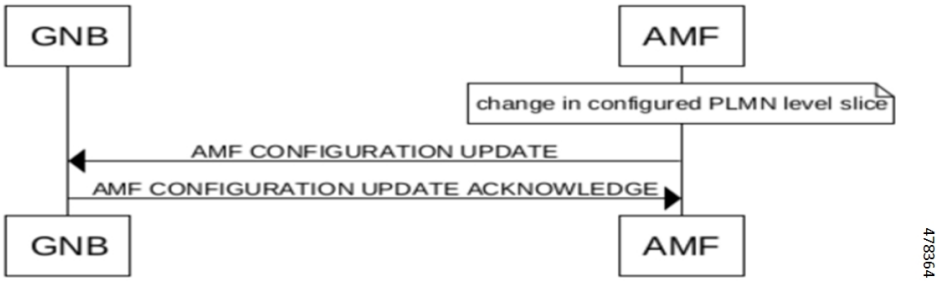


Note The AMF sends indication about the network slicing subscription change in UE configuration update, only in case of UDM subscription data changes notification.

Table 127: Slice Configuration Change

Step	Description
1	The AMF updates all non-emergency subscriber for which old slice information is no longer valid.
2	The behavior is same as the "UDM Change notification for subscriber in connected mode".
3	For idle subscriber (no paging), The AMF releases the non-emergency PDU session for which network slice is no longer available and indicates SMF to release such PDUs.

AMF Configuration Update



Changes in the slice configuration per PLMN is notified to GNBs using AMF configuration update message.

NRF Registration or Modification

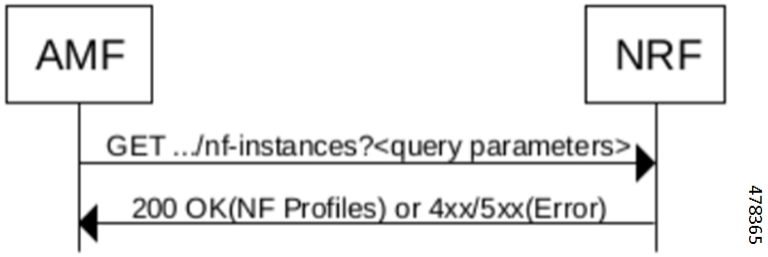
During the NRF registration/modification, the AMF sends the slice information in nfProfile which is configured at AMF.

Attribute Name	Data Type	Description
sNssais	array (Snssai)	S-NSSAIs of the network function. If not provided, the NF can serve any S-NSSAI. When present this IE represents the list of S-NSSAIs supported in all the PLMNs listed in the plmnList IE.

Note The TAI level information and NSI-list is not sent to NRF during registration or modification.

Peer NF Discovery through NRF

The AMF supports the discovery of peer NFs based on the slice data. The “SNSSAIS” is configured in the query-params CLI. The AMF, while sending the discovery request to NRF, must include the SNSSAIS for the filter criteria in the query parameters.



Attribute Name	Data type	Description
SNSSAIS	array (SNSSAIS)	If included, this IE contains the list of S-NSSAIs that are served by the NF (service) instances being discovered. The NRF returns those NF profiles/NF services of NF (service) instances that have at least one of the S-NSSAIs in this list.

Limitations

Following are the limitations for this feature:

- The AMF doesn't support the slice selection for roaming subscriber (Mapped NSSAI).
- The AMF doesn't support the network slice specific authentication and authorization (NSSAA).
- The AMF doesn't support the slice selection for handover scenario (Xn and N2).
- The AMF doesn't support the reallocation for the roaming subscribers and registration with the foreign-5g-GUTI.
- The AMF doesn't support the PDU establishment using NSSF.
- The AMF doesn't support discovery of peer AMF using SNSSAI as query parameter.
- The AMF supports reallocation only for the initial registration.

Feature Configuration

Configuring this feature involves the following steps:

- Slice Selection Enable and Slice Migration—This configuration enables the slice selection. For more information, refer to Configuring the AMF Reallocation, on page 275.
- Inclusion Mode—This configuration provides the commands for Inclusion mode configuration. For more information, refer to Configuring the Inclusion Mode, on page 276.
- Enabling UE Update—This configuration enables the UE update. For more information, refer to Enabling the UE Configuration Update, on page 277.
- Query Parameters for AMF Discovery—This configuration provides the Query parameters commands for AMF discovery. For more information, refer to Configuring the Query Parameters for AMF Discovery, on page 277.
- NSSF—This configuration provides the commands for NSSF configuration. For more information, refer to Configuring the NSSF, on page 278.
- Local AMF—This configuration provides the Local AMF configuration. For more information, refer to Configuring the Local AMF, on page 281.

Configuring the AMF Reallocation

To configure the reallocation, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         policy amf-redirection use-source-key { false | true }
         policy amf-redirection horizontal-key-derivation { false | true
 }
         policy nssf-interaction { disabled | enabled }
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- If the NSSF interaction is disabled, and slice selection fails, in that case AMF falls back to the default slice configuration on AMF and registration accept is sent with the default slice in the allowed NSSAI. If the default slice configuration is absent (which is less likely since it is mandatory for the N26 HandIn to succeed), only then AMF sends the registration reject.
- In case amf-redirection is disabled, then S-AMF doesn't reroute to T-AMF and initiates registration reject with cause code set to 62 - "No network slices available".
- Use-source-key: If true, then T-AMF uses the key received from S-AMF.
- horizontal-key-derivation: If true, then S-AMF generates a new key and sends newly generated keys in N1MsgNotify.
- The AMF-redirection is enabled by configuring use-source-key/horizontal-key-derivation or both with true/false and if none of the options are configured then AMF-redirection is considered to be in disabled state.

Configuring the AMF Slice

The following is the global level slice configuration representing system level slice configuration supported by AMF.

```
config
   amf-services amf_service_name
      nssai name slice_name
         sst sst_value
         sdt sdt_value
         end
```

NOTES:

- **nssai name** *slice_name* - Specify the slice name.
- **sst** *sst_value* - Specify the SST value.
- **sdt** *sdt_value* - Specify the SDT name.

Note The AMF supports a maximum of eight slices.

Configuring the Emergency Slice

When you configure the emergency slice, then the AMF sends this slice in the registration accept message for emergency subscriber.

```
config
   emergency-profile profile_name
      nssai
         sst sst_value
         sdt sdt_value
         end
```

NOTES:

- **emergency-profile***profile_name* - Specify the emergency profile name.
- **sst** *sst_value* - Specify the SST value.
- **sdt** *sdt_value* - Specify the SDT name.

Note You must associate an emergency profile to amf-service or operator policy to enable this configuration.

Configuring the Inclusion Mode

When you configure this CLI, the inclusion mode is sent in registration accept.

To configure the Inclusion mode, use the following CLI:

```
config
   amf-global
      call-control-policy policy_name
         policy slicing inclusion-mode policy_inclusion_mode
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- **policy slicing inclusion-mode** *policy_inclusion_mode*—Specify the policy inclusion mode for slicing. The possible values for the inclusion mode is - A, B, C, and D.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy local
```

```
policy slicing inclusion-mode B
end
```

Configuring Default Slice

Use the following CLI to configure the default slice in AMF:

```
config
   amf-global
      call-control-policy policy_name
        default-nssai
           sst sst_value
           sdt sdt_value
           end
```

NOTES:

- **sst** *sst_value* - Specify the SST value.
- **sdt** *sdt_value* - Specify the SDT value.

Enabling the UE Configuration Update

When you configure this CLI, the AMF sends the configuration update command to UE upon idle timer expiry if there are any changes in the slices (configured or allowed S-NSSAIs) for any subscriber.

```
config
   amf-global
      call-control-policy policy_name
         policy ue-cfg-update on-nssf-slice-change { true | false }
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- **policy ue-cfg-update on-nssf-slice-change { true | false }**—Enable or disable the UE configuration update.

Configuration Example

The following is an example configuration.

```
config
  amf-global
     call-control-policy local
        policy ue-cfg-update on-nssf-slice-change true
        end
```

Configuring the Query Parameters for AMF Discovery

To configure the query parameters for AMF discovery, use the following configuration:

```
config
   profile network-element amf amf_name
```

```
nf-client-profile nf_client_name
failure-handling-profile profile_name
query-params { target-plmn | amf-set-id | target-nf-instance-id }
end
```

NOTES:

- **profile network-element amf** *amf_name*—Specify the name of AMF network element.
- **nf-client-profile** *nf_client_name*—Specify the name of NF client.
- **failure-handling-profile** *profile_name*—Specify the name of failure handling profile name.
- **query-params { target-plmn | amf-set-id | target-nf-instance-id }**—Specify the query parameters for AMF discovery.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      profile network-element amf amf1
         nf-client-profile nf1
         failure-handling-profile FH5
         query-params [ target-plmn amf-set-id target-nf-instance-id ]
         end
```

Configuring the Query Parameter for Slice Data in NF Discovery

To configure the query parameters in NF discovery, use the following configuration:

```
config
   profile network-element { pcf | smf }
      failure-handling-profile profile_name
      query-params { snssais }
      end
```

NOTES:

- **profile network-element** *profile_name*—Specify the network profile name.
- **failure-handling-profile** *profile_name*—Specify the name of failure handling profile name.
- **query-params { snssais }**—select SNSSAIS as query parameter in network function discovery.

Configuring the NSSF

Configuring the NSSF involves the following configurations:

1. Network Element Profile List—This configuration provides the commands to configure the Network element profile list. For more information, refer to Configuring the Network Element Profile List, on page 279.
2. Profile Network Element—This configuration provides the commands to configure the profile networkeElement. For more information, refer to Configuring the Profile Network Element, on page 279.

3. Profile NF-client—This configuration provides the commands to configure the profile NF-client. For more information, refer to Configuring the Profile NF-client, on page 279.
4. Profile NF-client-failure—This configuration provides the commands to configure the Profile NF-client-failure. For more information, refer to Configuring the Profile NF-client-failure, on page 280.
5. Profile NF-pair NF-type—This configuration provides the commands to configure the Profile NF-pair NF-type. For more information, refer to Configuring the Profile NF-pair NF-type, on page 281.

Configuring the Network Element Profile List

To configure the network element profile list, use the following configuration:

```
config
   amf-global
      operator-policy policy_name
         ccp-name ccp_name
         network-element-profile-list nssf nssf_name
         end
```

NOTES:

- **operator-policy** *policy_name*—Specify the operator profile name.
- **ccp-name** *ccp_name*—Specify the Configuration Control Point (CCP) name. The CCP is used for managing and controlling configuration settings.
- **network-element-profile-list nssf** *nssf_name*—Specify the NSSF with the network element profile.

Configuring the Profile Network Element

To configure the profile network element, use the following configuration:

```
config
 profile network-element nssf nssf_name
  nf-client-profile nf_client_name
  failure-handling-profile failure_handling_profile_name
  end
```

NOTES:

- **profile network-element nssf** *nssf_name*—Specify the profile name for the network element.
- **nf-client-profile** *nf_client_name*—Specify the network function client profile name.
- **failure-handling-profile** *failure_handling_profile_name*—Specify the failure handling profile name.

Configuring the Profile NF-client

To configure the profile NF-client, use the following configuration:

```
config
   profile nf-client nf-type nf_client_name
      nssf-profile profile_name
         locality locality_name
            priority priority_value
```

```
service name type nnssf-nsselection
   endpoint-profile profile_name
      capacity capacity_value
      uri-scheme uri_scheme_name
      version
      uri-version uri_version
      exit
  exit
  endpoint-name end_point_name
     priority priority_value
        primary ip-address ipv4 ipv4_address
        primary ip-address port ipv4_port_number
        secondary ip-address ipv4 secondary_ipv4_address
        secondary ip-address port secondary_ipv4_port_number
        tertiary ip-address ipv4 tertiary_pv4_address
        tertiary ip-address port tertiary_ipv4_port_number
        end
```

NOTES:

- **profile nf-client nf-type** *nf_client_name*—Specify the profile name of the NF client.
- **nssf-profile** *profile_name*—Specify the profile name for the NSSF.
- **locality** *locality_name*—Specify the locality name within the NSSF profile.
- **priority** *priority_value*—Specify the priority value of the locality name within the NSSF profile.
- **endpoint-profile** *profile_name*—Specify the associated end point profile name.
- **capacity** *capacity_value*—Specify the capacity of the endpoint.
- **uri-scheme** *uri_scheme_name*—Specify the uri scheme associated with the endpoint.
- **uri-version** *uri_version*—Specify the uri version associated with the endpoint.

Configuring the Profile NF-client-failure

To configure the profile NF-client-failure, use the following configuration:

```
config
   profile nf-client-failure nf-type nssf nssf_name
      profile failure-handling failure_handling_profile_name
         service name type nnssf-nsselection
            responsetimeout timeout_value
               message type NssfNSSelectionReq
                  status-code httpv2 503
                  retry retry_count
                  action retry-and-ignore
                  end
```

NOTES:

- **profile nf-client-failure nf-type nssf** *nssf_name*—Specify NF (Network Function) client failure profile.
- **profile failure-handling** *failure_handling_profile_name*—Specify failure-handling profile name.

- **responsetimeout** *timeout_value*—Specify the response timeout for the specified services.
- **retry** *retry_count*—Specify the retry count for the status code.

Configuring the Profile NF-pair NF-type

To configure the profile NF-pair NF-type, use the following configuration:

```
config
   profile nf-pair nf-type nf_type_name
       locality client client_name
       locality preferred-server server_name
       locality geo-server server_name
       end
```

NOTES:

- **profile nf-pair nf-type** *nf_type_name*—Specify NF (Network Function) type name.
- **locality client** *client_name*—Specify the locality name for the client.
- **locality preferred-server** *server_name*—Specify the server name as the preferred server locality.
- **locality geo-server** *server_name*—Specify the geographical location for the geo-server.

Note The failure handling configuration leading to the session delete is not valid for NSSF.

Configuring the Local AMF

It’s optional configuration when real NRF isn’t available.

The following is an example configuration.

```
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 10.81.70.232
      primary ip-address port 9052
      default-notification-subscriptions s1
       notification-type N1_MESSAGES
       callback-uri http://xx.xx.xx.xx:xxxx/namf-comm/v1/callbacks/n1-message-notify
       n1-message-class 5GMM
       end
```

Configuring Label Slice Data Filters in Metrics

you can enable or disable the slice data filters for the slices only in metrics by using the following CLIs:

Use the following CLI for disabling the slice data filter:

```
config
        amf-global
           metric-label-filter
           slice-data disabled
        end
```

Use the following CLI for enabling the slice data filter:

```
config
        amf-global
           metric-label-filter
           slice-data slices [ sst-sdt sst-sdt sst ]
        end
```

Note A maximum of eight slices can be configured and there is no validation to check the sst/sd format.

NOTES:

- **metric-label-filter**—To define and configure the metric label filters.
- **slice-data** *slices [sst-sdt sst-sdt sst]*—Specify the slices to configure the metric label filter.

Configuring Clear Subscriber with Slice Filter

By using the **clear subscriber** command, you can configure the new slice filter to clear all subscribers with specified slice in accepted slice list. This is not applicable to emergency subscribers or non-emergency subscribers with emergency PDUs.

Note

- You can specify only one slice at a time.
- There is no validation to check the sst/sd format.

Following is the example of the clear subscriber configuration:

```
clear subscriber nssai
Description: Specify slice value. Format sst-sd or sst (e.g. 4-abc12e or 123)
Possible completions: <string>

[amf] amf# clear subscriber nssai 4-123546
result
ClearSubscriber Request submitted
```

Bulk Statistics

amf_ngap_message_total

The `amf_ngap_message_total` metric tracks the total number of NGAP Next Generation Application Protocol (NGAP) messages sent by the AMF. These messages are categorized based on different attributes:

- `app_name`: Specifies the name of the application (AMF).
- `message_direction`: Indicates the direction of the message (example, "outbound").
- `message_type`: Specifies the type of NGAP message (example, "N2ReRouteNasRequest").
- `service_name`: Identifies the service name (example, "amf-protocol-ep").

Example usage:

```
amf_ngap_message_total{app_name="AMF", message_direction="outbound",
message_type="N2ReRouteNasRequest", service_name="amf-protocol-ep"}
```

n2_service_stats

The `n2_service_stats` metric provides statistics related to N2 service operations in the AMF. These statistics include:

- `app_name`: Specifies the name of the application (AMF).
- `message_type`: Indicates the type of N2 service operation (example, "N2ReRouteNasRequest").
- `service_name`: Identifies the service name (example, "amf-service").
- `status`: Indicates the status of the service operation (example, "success").

Example usage:

```
n2_service_stats{app_name="AMF", message_type="N2ReRouteNasRequest",
service_name="amf-service", status="success"}
```

n22_service_stats

The `n22_service_stats` metric provides statistics related to N22 service operations in the AMF. These statistics include:

- `app_name`: Specifies the name of the application (AMF).
- `message_type`: Indicates the type of N22 service operation (example, "NssfGetNetworkSliceInformationReq").
- `service_name`: Identifies the service name (example, "amf-service").
- `status`: Indicates the status of the service operation (example, "success/failure").

Example usage:

```
n22_service_stats{app_name="AMF", message_type="NssfGetNetworkSliceInformationReq",
service_name="amf-service", status="success"}
```

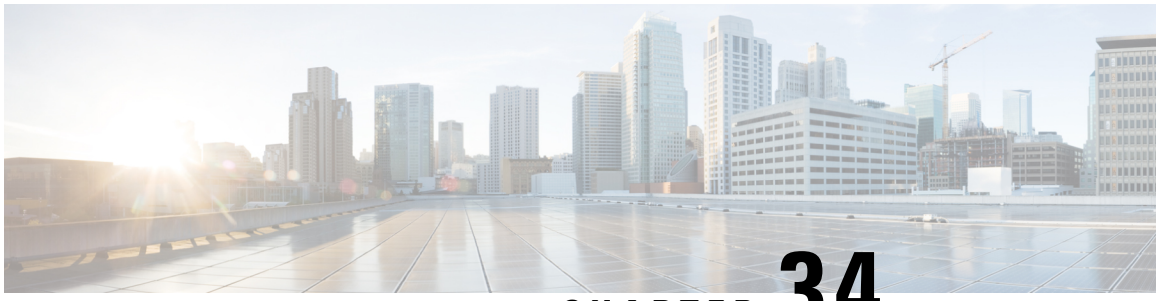
n14_service_stats

The `n14_service_stats` metric provides statistics related to N14 service operations in the AMF. These statistics include:

- `app_name`: Specifies the name of the application (AMF).
- `message_type`: Indicates the type of N14 service operation (example, "N14N1MessageNotifyClientRequest").
- `service_name`: Identifies the service name (example, "amf-service").
- `status`: Indicates the status of the service operation (example, "success/failure").
- `reason`: Provides additional information about the operation's status.

Example usage:

```
n14_service_stats{app_name="AMF", message_type="N14N1MessageNotifyClientRequest",
service_name="amf-service"}
```



CHAPTER 34

Node Manager Endpoint Onboarding Support

Feature Summary and Revision History

Summary Data

Table 128: 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 129: 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.

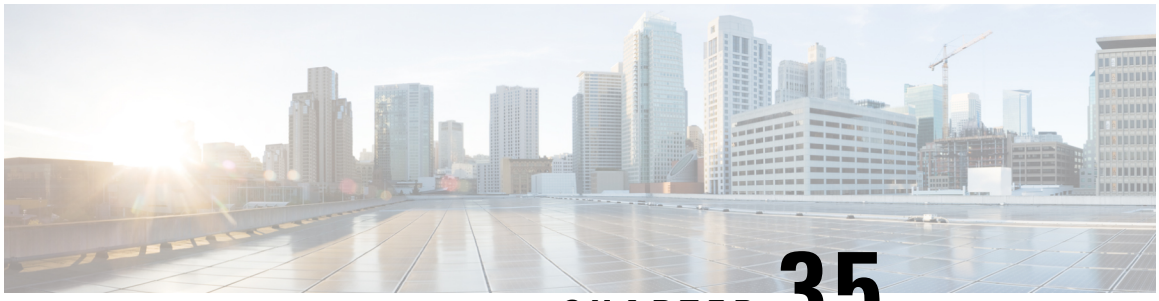
Feature Configuration

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 35

NRF (Network Function Repository) Services

Feature Summary and Revision History

Summary Data

Table 130: Summary Data

Applicable Products or Functional Area	AMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	

Revision History

Table 131: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

Network Repository Function (NRF) functions as a centralized repository for all the 5G network functions (NFs). It performs the following:

- Provides NF service registration and discovery, in the operator network
- Enables NFs to identify appropriate services in each or one another
- Supports the service discovery function
- Receives NF Discovery Request from an NF instance
- Provides information about discovered NF instances

The AMF functions and benefits the user in multiple activities such as the following:

- Supports and sends the following:
  - **registration**
  - **heartbeat**
  - **update**
  - **deregistration**
  - **NF Discovery-Request**
- Includes the following:
  - **nf-type**
  - **plmn-info**
  - **slice-data**
  - **ddn**
- Sends the **NFDiscovery** request towards the NRF during the discovery of network elements
- Enables or disables the parameters through the **NFDiscovery** request

The AMF checks and queries NF discovery APIs of the NRF. It helps when they aren't configured locally. It further discovers or locates the following network functions:

- **AUSF**
- **UDM**
- **PCF**
- **SMF**
- **SMSF**
- **NSSF**
- **Peer AMF**

The AMF supports the following NRF functionalities for GR-based instances:

- Creating, updating, and deleting a subscription
- Receiving a notification when the NF instance profile is either modified or deregistered from the NRF.

- Subscribing to notifications and receiving notifications, which were previously subscribed for registration or deregistration or profile changes of NF instances.

How it Works

This section describes how this feature works.

With the current GR-based AMF, the existing AMF NRF functionality *NewNrfLibApi* gets invoked. During this process, when *NewNrfLibApi* is associated with GR, the AMF needs to pass a valid *grInstanceID* to initiate the transaction.

The following list of procedures is supported for multiple transactions with required instance and validity details:

- **nrf init**
- **update**
- **registration**
- **heartbeat**
- **deregistration**
- **subscription**
- **notification**

NRF Interfaces

The AMF supports the following NRF interfaces and instances with their enhanced functionalities:

- NRF interface supports **TS 29.510 V15.6** specifications and adapts to the changes in 3GPP specifications for the already implemented interfaces. The supported list includes:
  - **discovery**
  - **register towards NRF**
  - **deregistration**
  - **update**
  - **notify**
  - **subscribe**
  - **heartbeat**
- NRF interface supports the enhanced version of the Subscribe for Notifications.
- NRF interface handles and receives the registration and deregistration notifications that were previously subscribed.

NRF Solutions

The AMF configures and supports the following NRF interfaces and instances with their enhanced solutions:

- In Yang model, this feature supports the following CLI configuration:
  - Repositories of endpoints or base URLs of the NRF
  - Profile discovery
  - NRF endpoints for the registration of ownership service profile
  - The local set of endpoints of **NFType** for the given **ServiceName**.
- Registers own **NFProfle** to the configured NRF.
- Checks for the cached **NFProfle** for the required service and accessibility.
- Discovers the **NFProfle** using the configured discovery repository for the **ServiceName** when the service can't be found or accessed.
- Uses the local configuration for the service, when **NFProfile** isn't discovered or found.
- Subscribes to NF instances, using the NRF Management interface, at the **init** and the AMF configuration change. It includes the following:
  - In **SubscriptionData**, the following can be filled:
    - **nfStatusNotificationUri**
    - **SubscrCond**
    - **nfInstanceId**
    - **validityTime**
  - Responses have the following subscription values:
    - **subscriptionId**
    - **validityTime**
  - Subscription has the following values:
    - The discovery of the **NFProfile**
    - On the same **NRF EP** used for discovery as well
- Resubscribes or avails the **PATCH** option to the **NFProfile**. It also changes the notification, using the NRF management interface on the expiry of **validityTime**. It includes the following:
  - Sends the proposed **validityTime** as **PatchItem**.
  - When NRF accepts the proposed **validityTime**, it responds with **returnCode 204**.
  - When NRF has an alternate **validityTime**, it responds with **returnCode 200**, and **validityTime** in **SubscriptionData**.
- Unsubscribes or removes the **DELETE** option for the subscription, before the shutdown.

Note This activity isn't supported, before the shutdown. Only the VIP offline scenario is supported.

- Deregisters the **NFProfile** at NRF before the shutdown.

Note This activity isn't supported, before the shutdown. Only the VIP offline scenario is supported.

- Handles the notification and cache, for the received **NFProfile**. It also includes the following:
  - When the added event is **NF_REGISTERED**, it also adds the received **NFProfile** to the cache.
  - When the removed event is **NF_DEREGISTERED**, it also removes the received **NFProfile** from the cache.

OAM Support

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

The following show commands are used to view and trace NRF options in the AMF Ops Center.

show nrf [*discovery-info* | *registration-info* | *subscription-info*]

NOTES:

- *discovery-info*—Shows discovery filter Information.
- *registration-info*—Shows Registration Information.
- *subscription-info*—Shows NF Subscription Information.

Statistics Support

The following counters-related or metrics-related statistics are supported for the Enhancing NRF Functionalities feature. It includes the following:

- **nf_discover_messages_total**
- **nf_management_stats_total**
- **nrf_subscription_send_messages_total**

nf_discover_messages_total

Description: Discover Messages statistics

Sample Query: `nf_discover_messages_total{nf_type=\"udm\", host=\"209.165.201.9:8082\", svc_name=\"nudm-sdm\", version=\"v1\", result=\"timeouOrRPCError\"}`

Labels:

- Label: `nf_type`

  Label Description: Network Function type

  Example: nrf, udm, amf, pcf, chf, ciscocontrol

- Label: `host`

  Label Description: End-Point address

  Example: 209.165.201.9:8082

- Label: `svc_name`

  Label Description: Network function service name

  Example: nudm-sdm, namf-comm

- Label: `version`

  Label Description: Api version info

  Example: v1, v2,

- Label: `result`

  Label Description: result of discover message.

  Example: 200, 201, 204, success, timeout_rpc_error, response_parse_failure

nf_management_stats_total

Description: NF management messages statistics

Sample Query: `nf_management_stats_total{host=\"209.165.201.9:8082\", svc_name=\"nudm-sdm\", version=\"v1\",direction=\"outbound\", message_type=\"registration\",result=\"timeouOrRPCError\" }`

Labels:

- Label: `host`

  Label Description: End-Point address

  Example: 209.165.201.9:8082

- Label: `svc_name`

  Label Description: Network function service name

  Example: nudm-sdm, namf-comm

- Label: `version`

  Label Description: Api version info

  Example: v1, v2,

- Label: `direction`

  Label Description: Direction indicates about the message going out or coming in.

  Example: inbound, outbound

- Label: `message_type`

  Label Description: Type of Message

  Example: registration, heartbeat, subscription, notification

- Label: `result`

  Label Description: result of discover message.

  Example: 200, 201, 204, success, timeout_rpc_error, response_parse_failure

nrf_subscription_send_messages_total

Description: NRF Subscription send messages total.

Sample Query: `nrf_subscription_send_messages_total{host=\"209.165.201.9:8082\", message_type=\"subscription\", req=\"initial\"}`

Labels:

- Label: `host`

  Label Description: End-Point address

  Example: 209.165.201.9:8082

- Label: `message_type`

  Label Description: subscription message type

  Example: unsubscription, subscription, updateSubscription

- Label: `req`

  Label Description: req type

  Example: resourceUri, initial, retry_2

Troubleshooting Information

This section describes troubleshooting information for this feature.

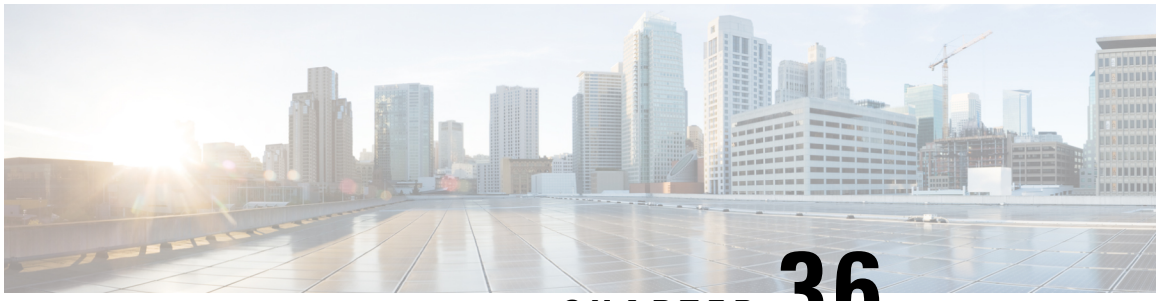
Trouble Ticket Content Data Collection

The following data are relevant when debugging issues with this feature.

Check the output of the following commands while debugging. The following is the list:

- **kubectl get pods -n** *namespace*
- **helm list**
- **helm get service -n** *namespace*
- **kubectl describe services** *nrf-service* **-n** *namespace*
- **show** full-configuration/running-configuration output from Ops Center

- **kubectl get pods -o yaml -n** *namespace restep pod_name*



CHAPTER 36

OAuth2 Client Authorization Support to NRF

Feature Summary and Revision History

Summary Data

Table 132: 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 133: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

This feature describes the authorization controls that are required for implementing all the network functions. The OAuth2 client authorization to NRF supports requesting AccessToken to NRF and validating AccessToken in the incoming requests.

All the network functions in the 5G core interact with each other using REST APIs. All these APIs are accessed without any authorization. These interactions between multiple network functions are processed without any access control mechanism. As per 3GPP standards, OAuth2 standards must be implemented for all the network functions to secure the access of REST APIs between these network functions.

As a mandatory security measure and as an upgraded requirement to protect the network function accessibility, the REST APIs are now accessed with an enhanced authorization mechanism. using OAuth2 standards.

Relationships

The network function of AMF can take two different roles, as the following:

- **NF Producer:** When a peer NF tries to access some of the service at AMF, it acts as NF producer.

  For more information, see AMF as NF Producer, on page 296.

- **NF Consumer:** When AMF as a client invokes a service at a peer NF, it acts as NF consumer.

  For more information, see AMF as NF Consumer, on page 298.

AMF as NF Producer

The AMF as an NF producer provides multiple services to the peer NFs. The following scenarios are processed for a successful communication to be established:

- The AMF must get registered with the NRF for a successful communication.
- Based on the configuration, the AMF Rest-EP must send the `oauth2Required` field set in the NF Service profile in the NF registration toward the NRF.
- The signing algorithm used to encrypt the token at the NRF must be configured using `access-token-jws-algo`. Currently, the following three algorithms are supported:
  - HS256—Where the shared secret key is provided at AMF.
  - RS256—Where private or public key is provided depending on the configuration at NRF.
  - ES256—Where private or public key is provided depending on the configuration at NRF.
- The AMF token validation is done by using a shared secret key or public key. It can be configured using `access-token-jws-key`.

How it Works

This section describes how this role works.

The AMF supports AccessToken validation in the incoming request. It is processed as in the following procedures:

- If an OAuth2 token is present in an incoming request from an NF consumer (such as SMF, UDM, peer AMF, and others), the AMF as an NF producer validates the token that is received in the incoming request.
- The signing algorithm used to encrypt the token at NRF can be accessed from `access-token-jws-algo`, and the respective shared secret key or public key can be accessed using `access-token-jws-key`.
- The AMF rejects an API request without the AccessToken or an API request with an invalid AccessToken. It returns the `status code 401` together with the www-authenticate header, with an error note as `invalid_token`.
- The AMF rejects an API request with an AccessToken validation token, for not having the required scopes to invoke the service operation. It returns the `status code 403` together with the www-authenticate header, with an error note as `insufficient_scope`.

Limitations

This feature has the following limitations:

- The AMF does not support the CLI changes for the NF-producer over the fly. They must be configured before the pod start-up.
- The AMF does not support the NSSF selection through NRF discovery and the access token will not be sent for NSSF.

Feature Configuration

To configure this feature, use the following configuration:

Note This configuration must be enabled in `amf-services` to register the AMF with NRF for the enablement of OAuth2 client authorization.

```
amf-services service_name
    amf-name amf_name
    locality locality_name
    oauth2-enabled
    access-token-jws-algo { HS256 | ES256 | RS256 }
    access-token-jws-key { shared_secret_key | public_key }
    exit
```

NOTES:

- **amf-services** *service_name*—Specify the name of the AMF service.
- **amf-name** *amf_name*—Specify the name of AMF.
- **locality** *locality_name*—Specify a name for the locality.
- **oauth2-enabled**—Enable the OAuth2 client authorization to register the AMF with NRF. The default value is false.

- **access-token-jws-algo { HS256 | ES256 | RS256 }**—Specify the type of the access token for the JWS Algorithm authorization.
- **access-token-jws-key { shared_secret_key | public_key }**—Specify the type of the access token for the JWS Key authorization.

Note When the `OAuth2-enabled` feature is configured, the options **access-token-jws-algo** and **access-token-jws-key** are mandatory.

Configuration Example

The following is an example configuration.

```
amf-services am1
 amf-name    amf1
 validate-Tais    false
 locality    LOC1
 oauth2-enabled
 access-token-jws-algo    { HS256 }
 access-token-jws-key    { public key }
 operator-policy-name    pem-file
 guamis mcc 123 mnc 456 region-id 1 set-id 14 pointer 3
 tai-groups test1
 exit
```

Configuration Verification

To verify the configuration:

```
show running-config amf-service am1
```

AMF as NF Consumer

The AMF as an NF consumer uses multiple services offered by the peer NFs.

The following scenarios are processed for a successful communication to be established:

- The AMF as a consumer looking for OAuth2-enabled profiles from NRF, must enable the AccessToken that is required in each `profile nf-client nf-type` configuration.
- The AMF as a consumer communicates with any of the applicable `nf-types`, such as AMF, PCF, UDM, AUSF, SMF, and SMSF.
- The AMF as a consumer sends the `Nnrf_AccessToken` request to the NRF server based on the `nf-client` configuration.
- The AMF as a consumer sends a request with an AccessToken to `nf-producer`. If it gets rejected due to the AccessToken validation failure, then the AMF failure handling template (FHT) handles those responses appropriately.

How it Works

This section describes how this role works. The AMF supports OAuth2 client authorization to NRF. This process gets executed with the following procedures:

- Only when the `nf-client` profile gets configured with `OAuth2-Enabled`, where the value gets set as true for a `nf-type`, the AMF considers those profiles with `OAuth2-Enabled` as true value.
- The AMF internally sends the AccessToken request to the NRF server, stores the received token in the cache. The same token gets reused until it expires.
- When the profile gets selected and the token also received, the application includes the AccessToken in the Authorization header in the request toward NF producer.
- If the `nf-client` profile doesn't get configured, that's when OAuth2 gets disabled on the consumer side. The AMF ignores those profiles with the `oauth2Required` and selects the producer among the rest of the profiles received in the discovery response.
- For AMF to send an AccessToken request to NRF, endpoints must get configured in the CLI for service type OAuth2 and the same must be set in the profile `nf-pair` for each type, wherever OAuth2 already enabled.
- When the `OAuth2-Enabled` gets set as true in the CLI and none of the discovered profiles from NRF has `oauth2Required`, then no profiles from the discovery get selected. It then reverts to the locally configured profiles. The AccessToken requests not sent as a locally configured profile, as it gets assumed as a base for the local trust policy. The NRF has no information about this development.
- When the `OAuth2-Enabled` gets set to false status in the CLI and all the discovered profiles get `oauth2Required` enabled, then none of these profiles in the discovery get selected. It then reverts to the locally configured profiles. If none of these profiles get configured locally, then the call fails.
- During the traffic running with the OAuth feature enabled, minimal numbers of 401-Unauthorized errors could be seen on the AMF side. To mitigate this risk, you can configure the failure handling template for all the possible causes (such as 401 error codes) to avoid any failed scenario of an end-to-end call.

Feature Configuration

To configure this feature, use the following configuration:

The following configuration is enabled only when the AMF sends the `Nnrf_AccessToken` request to the NRF server, when the `nf-client` is configured.

```
profile nf-client nf-type nf_type_name
    oauthenabled { true | false }
    nf-type-profile nf_type_profile_name
    locality locality_name
    priority priority_number
    service name type service_name type_npcf_am_policy_control
    endpoint-profile endpoint_profile_details
    capacity capacity_number
    uri-scheme http
    endpoint-name endpoint_name
    priority priority_number
    primary ip-address ipv4 ipv4_address
```

```
    primary ip-address port port_address
    exit
```

The following configuration must be done for an NRF endpoint, to which the AMF will send the AccessToken request.

```
group nrf auth nrf_group_name
    service type nrf oauth2
        endpoint-profile endpoint_profile_details
        capacity capacity_number
        uri-scheme http
        endpoint-name endpoint_name
        priority priority_number
        primary ip-address ipv4 ipv4_address
        primary ip-address port port_address
        exit
```

The following configuration must be used to specify auth-groups containing the NRF endpoint details for each NF type.

```
profile nf-pair nf-type nf_type_name
    nrf-auth-group nrf_auth_group_name
    nrf-discovery-group nrf_discovery_group_name
    locality client client_name
    locality preferred-server server_name
    locality geo-server geo_server_name
    cache invalidation { true | false } timeout timeout_number
    exit
```

NOTES:

- **profile nf-client nf-type** *nf_type_name*—Specify the NF and the profile name.
- **oauthenabled { true | false }**—Enable the oauthenabled profile configuration. The default value is false.
- **nf-type-profile** *nf_type_profile_name*—Specify the NF profile name.
- **locality** *locality_name*—Specify the locality.
- **priority** *priority_number*—Specify the priority request. Must be in numbers.
- **service name type** *service_name type_npcf_am_policy_control*—Specify the service name and the type.
- **endpoint-profile** *endpoint_profile_details*—Specify the endpoint profile details.
- **capacity** *capacity_number*—Specify the capacity requirement in number.
- **uri-scheme http**—Specify the URI scheme.
- **endpoint-name** *endpoint_name*—Specify the endpoint name.
- **primary ip-address ipv4** *ipv4_address*—Specify the primary IPv4 address.
- **primary ip-address port** *port_address*—Specify the primary port address.
- **group nrf auth** *nrf_group_name*—Specify the NRF group name to authenticate. Must be a string.
- **service type nrf oauth2**—Specify the service and the type of NRF, which must be authenticated to enable the OAuth2 profile configuration.

- **profile nf-pair nf-type** *nf_type_name*—Specify the nf-type in the profile name to authenticate. Must be a string.
- **nrf-auth-group** *nrf_auth_group_name*—Specify the nrf-auth-group name.
- **nrf-discovery-group** *nrf_discovery_group_name*—Specify the nrf-discovery-group name.
- **locality client** *client_name*—Specify the client name in the locality details.
- **locality preferred-server** *server_name*—Specify the preferred-server or client name in the locality details.
- **locality geo-server** *geo_server_name*—Specify the geo-server name in the locality details.
- **cache invalidation { true | false }**—Enable the cache invalidation configuration. The default value is false.
- **timeout** *timeout_number*—Specify the timeout duration in seconds.

Configuration Example

The following is an example configuration.

```
profile nf-client nf-type pcf
 oauthenabled { true }
 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 209.165.201.30
      primary ip-address port 9049
     exit
    exit
   exit
  exit
 exit
exit
group nrf auth oauthep
  service type nrf oauth2
    endpoint-profile EP1
      capacity 30
      uri-scheme http
      endpoint-name EP1
        priority 56
        primary ip-address ipv4 209.165.201.30
        primary ip-address port 9049
      exit
    exit
  exit
exit
profile nf-pair nf-type PCF
 nrf-auth-group      oauthep
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
```

```
 cache invalidation true timeout 1000
exit
```

Configuration Verification

To verify the configuration:

```
show profile nf-client nf-type pcf
```

OAM Support

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

Bulk Statistics Support

The following statistics are supported for the OAuth2 Client Authorization Support to NRF, on page 295 feature.

NF AccessToken Statistics

Total AccessToken Message count:

- Labels:

  nf_oauth_messages_total

- Host:

  Refers to the host information (IP: Port) of the URL to which the access token request is being sent.

- Service Name: NF AccessToken service

  Example: **nnrf-oauth**

- Version: API version

  Example: **v1**

- NfType:

  peer nf type

- GrInstanceID:

  gr-instance-id

- Result:

  [Success | error response status code | RPC/Timeout error | Request parse failure | Response parse failure | Invalid notification event | Invalid Nf instance URI | Internal Error]

Token Validation Statistics for AMF as Producer

App infra statistics for outgoing responses:

- Labels: **outgoing_response_total**

- Invalid token format or signature mismatch:

  {app_name="AMF", protocol="http", service_name="amf-rest-ep", status="error", status_code="invalid_token"}

- Token payload verification fail:
  - Invalid scope:

    {app_name="AMF", protocol="http", service_name="amf-rest-ep", status="error", status_code="app_invalid_scope"}

  - Other IE failures:

    {app_name="AMF", protocol="http", service_name="amf-rest-ep", status="error", status_code="app_invalid_token"}

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

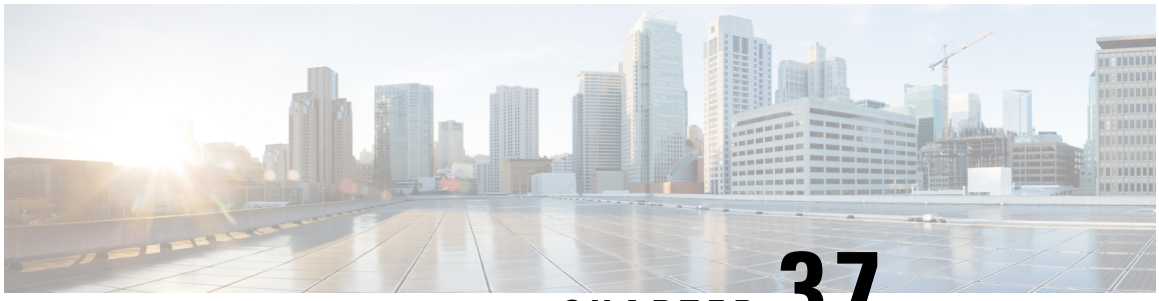
Data Type Support

The following statistics are supported for the OAuth2 Client Authorization Support to NRF, on page 295 feature.

AccessTokenReq

- `grant_type`
- `nfInstanceId`
- `nfType`
- `targetNfType`
- `scope`

For information on data type support for AMF, see the *UCC 5G AMF Metrics Reference* document.



CHAPTER 37

Overload Control for N2 and NAS

Feature Summary and Revision History

Summary Data

Table 134: 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 135: Revision History

Revision Details	Release
First introduced.	2022.03.0

Feature Description

The congestion control feature lets you define the system conditions which when matched impacts the system's performance. To prevent an impact of the congestion on the subscriber sessions, you can configure the system policies that are to be invoked when facing congestion.

Congestion control monitors the system to detect situations that match the conditions which may potentially degrade the system's performance when it is under heavy load. Typically, these conditions are transient (for example, high CPU or memory utilization) and gets resolved faster. However, if these conditions persist longer or they occur frequently during the specific time interval, a severe congestion occurs.

The congestion control feature monitors the system resources, such as CPU usage, memory, the number of active sessions, and the number of Go routines.

Note AMF does not provide a configuration to set the congestion control threshold for system CPU usage, memory usage, and maximum number of goroutine processes.

How it Works

This section describes how this feature works.

N2 Overload Control

When the congestion control feature is enabled, and a congestion threshold is exceeded, the AMF invokes congestion control policies. The AMF informs the control policies to the gNB, which throttles the traffic using the NGAP Overload Start or Stop messages. The AMF sends an NGAP Overload Start message to the gNBs to which it is connected. In the Overload Response IE that the AMF sends to gNBs, the AMF requests the gNBs to reject or allow certain sessions.

After the congestion is cleared, the AMF sends the NGAP Overload Stop message to the NG-RAN node indicating that AMF is resuming regular operations.

NAS Congestion Control

In the overload condition, the AMF rejects the NAS messages from a UE using a 5G-RAN. When AMF rejects a NAS request due to congestion, AMF sends the T3346 IE using the specified T3346 value. With the Mobility Management back-off timer running, the UE can initiate only the Deregistration procedures and procedures that are not affected by the congestion control, such as emergency services and mobile-terminated services.

During a congestion situation, AMF rejects the following requests with the 5GMM cause as Congestion and the T3346 timer value in the Registration Request (including Mobility and Periodic Registration Request) and service requests. The AMF includes the timer value in the Deregistration Request, which UE invokes during the admin clear subscriber process.

Suppose the AMF rejects a Registration Request or service request with the T3346 timer value higher than the sum of the UE's Periodic Registration Update timer T3512 and the Implicit Deregistration timer. In that case, the AMF adjusts the mobile reachable timer and the implicit deregistration timer, or both. With this adjustment, the AMF does not implicitly deregister the UE while the Mobility Management back-off timer is in-progress.

The AMF does not preserve the back-off-timer value which is sent to UE.

For information on the T3346 timer, see the Session Timers, on page 381 chapter.

With the Overload Control feature configured:

- The protocol-ep pod has X minute timer running locally. On expiry of the timer, the protocol-ep pod identifies the system overload state and accordingly sends the overload start or stop message.
- On configuration change, AMF sends overload Stop if overload start was sent earlier. Further, AMF continues to monitor the overload state and send stop/start messages accordingly.
- When the standby Protocol-ep pod becomes active, it collects the system load, determines the overload state, and sends the corresponding message. If AMF identifies an overload situation, the Protocol-ep pod sends an Overload Start message, else, sends the overload stop message if AMF is no longer overloaded.

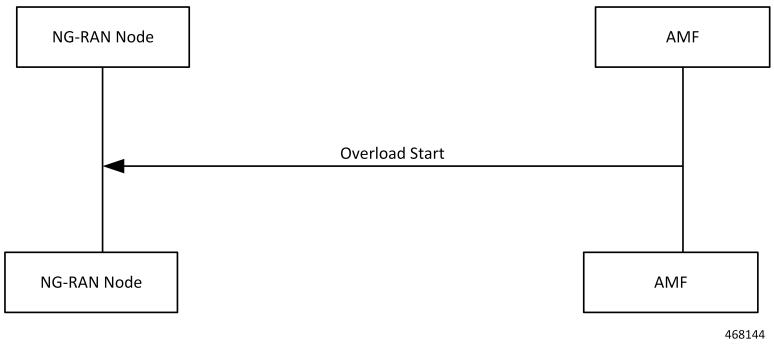
Call Flows

This section describes the key call flows for this feature.

Overload Start Message Call Flow

This section describes the Overload Start Message call flow.

Figure 55: Overload Start Message Call Flow

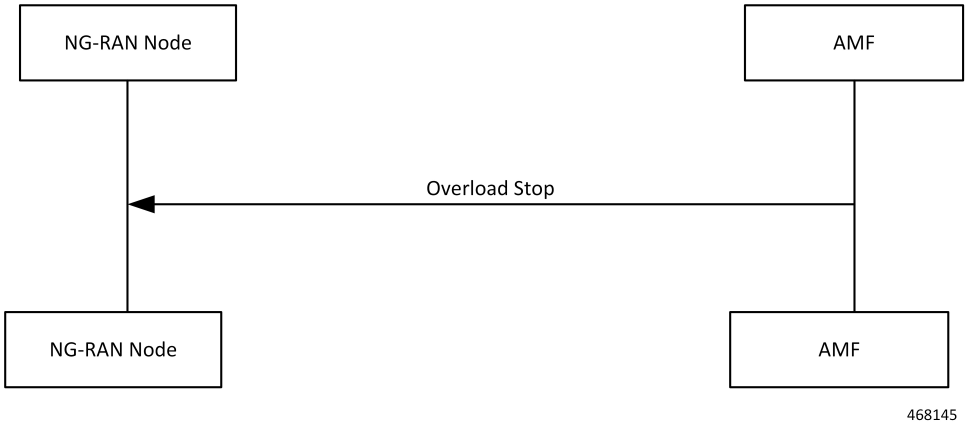


When the overload control is configured and the congestion threshold is reached, the AMF sends an Overload Start Message to the NG-RAN Node.

Overload Stop Message Call Flow

This section describes the Overload Stop Message call flow.

Figure 56: Overload Stop Message Call Flow



After the overload situation is resolved, the AMF sends an Overload Stop Message to the NG-RAN node indicating that the AMF is ready to resume the process the sessions.

NAS Congestion Control Call Flow

This section describes the NAS Congestion Control call flow.

Figure 57: NAS Congestion Control Call Flow

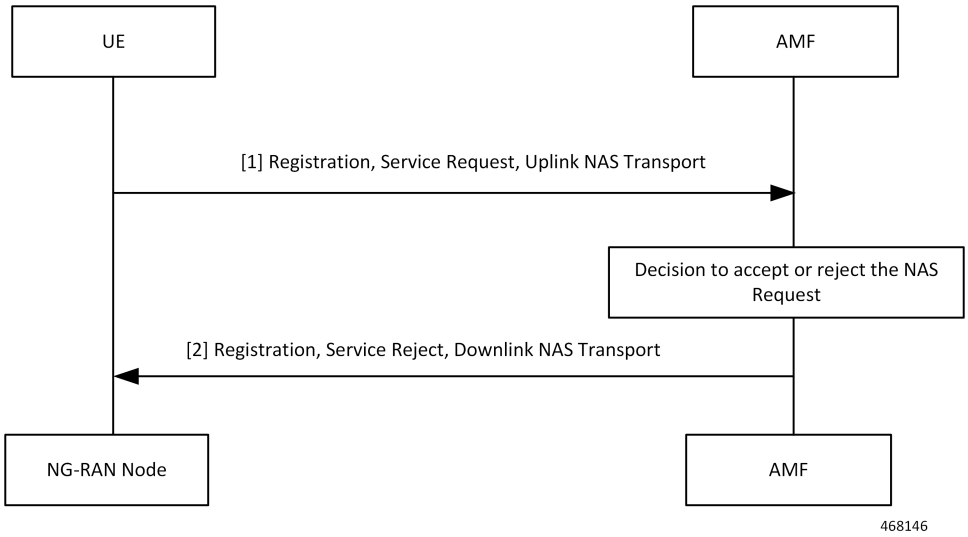


Table 136: NAS Congestion Control Call Flow Description

Step	Description
1	UE sends the Registration Request, Service Request, and Uplink NAS Transaction Request to AMF. When the NAS congestion configuration is enabled, the AMF accepts the following: • Requests received for emergency services. • De-Registration Request that originated in the UE. • Mobility Registration Update requests received when UE is in the CM-CONNECTED state. • Service request received when UE is in the CM-CONNECTED state. • Service request that is received in response to a paging request. • UL NAS Transport (Payload container type: N1 SM information) PDU Release.
2	Depending on AMF's overload capacity, it may reject the following requests: • Service request received when UE is in CM-IDLE state. • Periodic Registration Requests. • Mobility Registration Update requests received when UE is in the CM-IDLE state. • Nonemergency Initial Registration Requests. • Uplink NAS Transport requests with payload container type as N1 SM information. • Uplink NAS Transport requests with payload container type as SMS) dropped on AMF.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.501 "System architecture for the 5G System (5GS)"*
- *3GPP TS 38.413 "NG-RAN; NG Application Protocol (NGAP)"*
- *3GPP TS 24.501 "Non-Access-Stratum (NAS) protocol for 5G System (5GS)"*
- *3GPP TS 24.008 "Mobile radio interface Layer 3 specification; Core network protocols"*

Limitations

This feature has the following limitations in this release:

- The N2 Overload Control is applied at the system-level and not supported at individual S-NSSAI.
- The NAS Congestion Control is not supported per DNN, S-NSSAI, DNN—S-NSSAI, and at certain UE groups.
- Overload Control does not support congestion clearance of the REST interface.

Feature Configuration

Configuring this feature involves the following steps:

1. Configure the action profile, system load threshold and define the load stages as critical, major, and minor.

   The Protocol-ep pod periodically fetches the current system load and identifies the system overload state (minor, major, critical) and associated action profile. The Protocol-ep pod compares the new system load with last recorded system load, updates the locally stored overload information, and sends the determines whether to send the overload start or stop message.

   For more information, see Configuring Congestion Control Threshold, on page 310.

2. Configure the actions that must take an effect when the overload situation arises in N2 and NAS. For more information, see Configuring Congestion Action Profile, on page 311.

Configuring Congestion Control Threshold

To configure this feature, use the following configuration:

```
config
   amf-global congestion-control-threshold { critical | major | minor }
      action-profile action_profile value integer_value
      end
```

NOTES:

- **amf-global**—Enter the AMF global configuration mode.
- **congestion-control-threshold { critical | major | minor }** —Specify the system load stage for which the threshold is set.
- **action-profile** *action_profile* —Specify the action profile name.
- **value** *integer_value*—Specify the threshold value in the range 1–100. The **value** is associated with the system load stage that you have configured using **congestion-control-threshold**.

Configuration Example

The following is an example configuration:

```
config
   amf-global congestion-control-threshold critical
      action-profile sample_profile value 15
      end
```

Configuration Verification

To verify the configuration:

```
show running-config amf-global congestion-control-threshold
```

Sample Output

```
amf-global
 congestion-control-threshold critical value 95 action-profile critcal_profile
```

```
 congestion-control-threshold major value  90 action-profile major_profile
 congestion-control-threshold minor value 85 action-profile minor_profile
exit
```

Configuring Congestion Action Profile

To configure this feature, use the following configuration:

```
config
   congestion-action-profile action-profile action_profile_name
      n2-overload
         report-overload {
permit-emergency-sessions-and-mobile-terminated-services-only |
permit-high-priority-sessions-and-mobile-terminated-services-only |
reject-new-sessions | reject-non-emergency-sessions }
         traffic-load-reduction load_reduction_percentage
      nas-congestion-enabled
      end
```

NOTES:

- **congestion-action-profile**—Enter the congestion action configuration mode.
- **action-profile** *action_profile_name*—Specify the action profile name that is mapped to the system load stage.
- **n2-overload**—Configure parameters that must be applied when N2 is overloaded.
- **report-overload** —Configure the overload response message that AMF sends to gNB.

  The **report-overload** includes the following options:

  - **permit-emergency-sessions-and-mobile-terminated-services-only**—Configure to permit only emergency sessions and mobile-terminated services to access AMF during the overload situation.
  - **permit-high-priority-sessions-and-mobile-terminated-services-only**—Configure to permit only high priority or emergency sessions and mobile-terminated services that AMF sends to the gNBs.
  - **reject-new-sessions**—Configure to reject all new connection requests except emergency requests sent to the AMF during the overload situation.
  - **reject-non-emergency-sessions**—Configure to reject all nonemergency or nonhigh priority Sessions Creation Requests during the overload situation.

- **traffic-load-reduction** *load_reduction_percentage*—Specify the percentage of traffic load to be reduced at gNB. *load_reduction_percentage* must be an integer in the range 1–99.
- **nas-congestion-enabled**—Enable the congestion control feature for NAS. **nas-congestion-enabled** is disabled by default.

Configuration Example

The following is an example configuration:

```
config
   congestion-action-profile action-profile sample_profile
      n2-overload
```

```
        report-overload { permit-emergency-sessions-and-mobile-terminated-services-only |
 permit-high-priority-sessions-and-mobile-terminated-services-only | reject-new-sessions |
 reject-non-emergency-sessions }
        traffic-load-reduction 20
     nas-congestion-enabled
     end
```

Configuration Verification

To verify the configuration:

show running-config congestion-action-profile

Sample Output

```
congestion-action-profile critcal_profile
 n2-overload traffic-load-reduction 98
 n2-overload report-overload reject-new-sessions
 nas-congestion-enabled
exit
```

OAM Support

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

Bulk Statistics Support

The following statistics are supported for the Overload Control for N2 and NAS feature:

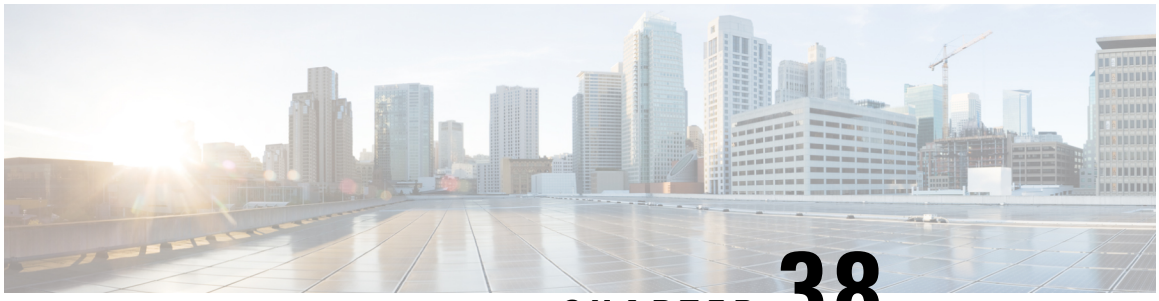
amf_overload_status

Description: The counter indicates the overload status as:

- Minor
- Major
- Critical

Example:

```
amf_overload_status{app_name="AMF",cluster="clu1",data_center="dc1",instance_id="2",service_name="amf-protocol-ep"}
 2
```



CHAPTER 38

Paging Overload Protection

Feature Summary and Revision History

Summary Data

Table 137: 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 138: Revision History

Revision Details	Release
First introduced.	2022.03.0

Feature Description

Congestion control is a proactive mechanism where AMF lets you configure the number of paging requests that are sent for each gNB. When a congestion is detected, AMF drops the new paging requests.

How it Works

This section describes how this feature works.

The AMF provides a configuration that regulates the number of paging requests that the AMF sends for each gNB. If the paging requests count exceeds the configured value, the AMF ignores the new requests regardless of their type and priority.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   amf-global
      network-protection-overload rate-limit paging { rate  paging_rate |
burst  number_messages_allowed }
      end
```

NOTES:

- **network-protection-overload rate-limit paging**—Configure the overload protection parameters.
- **rate** *paging_rate*—Specify the number of paging request messages that AMF sends to the gNB per second. *paging_rate* accepts values in the range 1–65535.
- **burst** *messages_allowed* —Specify the number of paging messages that AMF must process before applying the threshold. The gNB drops the messages that are received after the threshold value matches the configured value. *messages_allowed* accepts values in the range 1–65535.

Configuration Example

The following is an example configuration:

```
config
   amf-global
      network-protection-overload rate-limit paging { rate 50000 | burst 45000 }
      end
```

Configuration Verification

To verify the configuration:

```
show running-config amf-global network-protection-overload
amf-global
 network-protection-overload rate-limit paging
  rate  1000
  burst 250
 exit
exit
```

OAM Support

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

Bulk Statistics Support

The following statistics are supported for the Paging Overload Protection feature.

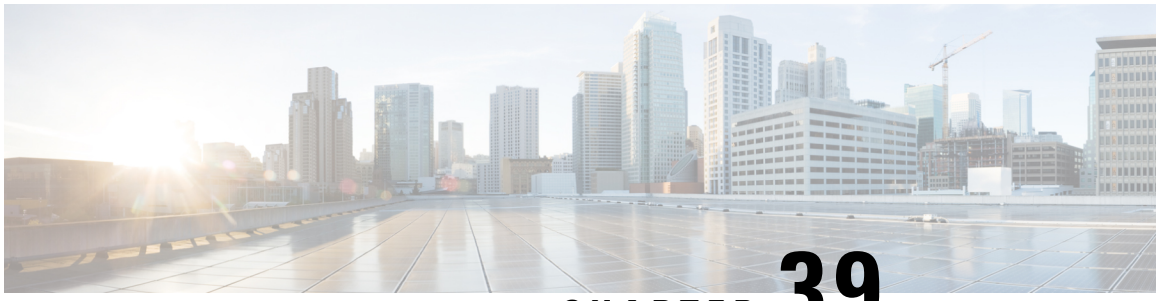
RateLimitPaging_Dropped

Description: The total count of NGAP messages that are dropped after applying the paging limit range.

Sample Query:

```
amf_ngap_message_total{message_direction=\"outbound\",
message_type=\"RateLimitPaging_Dropped\"}
```

For information on bulk statistics support for AMF, refer *UCC 5G AMF Metrics Reference*.



CHAPTER 39

Paging Support

Feature Summary and Revision History

Summary Data

Table 139: 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 140: 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.
- AMF supports handling of new N1N2 messages when UE is in IDLE mode and paging is already triggered due to a previous N1N2 message. AMF doesn't support handling of simultaneously received multiple N1N2 messages when UE is in IDLE mode and paging is not yet triggered.

- 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 322.
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 323.
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 324.
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 325.
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 326.

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
            end
```

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
```

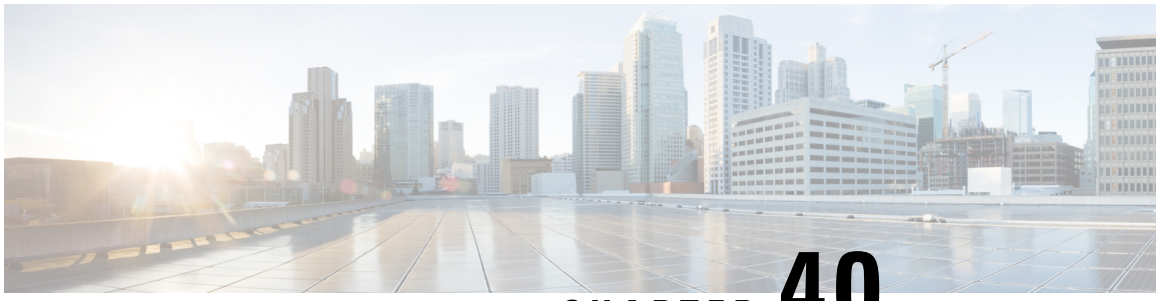
AMF Paging Configuration Example

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 40

gNB-Initiated Reset Procedure

Feature Summary and Revision History

Summary Data

Table 141: 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 142: 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:

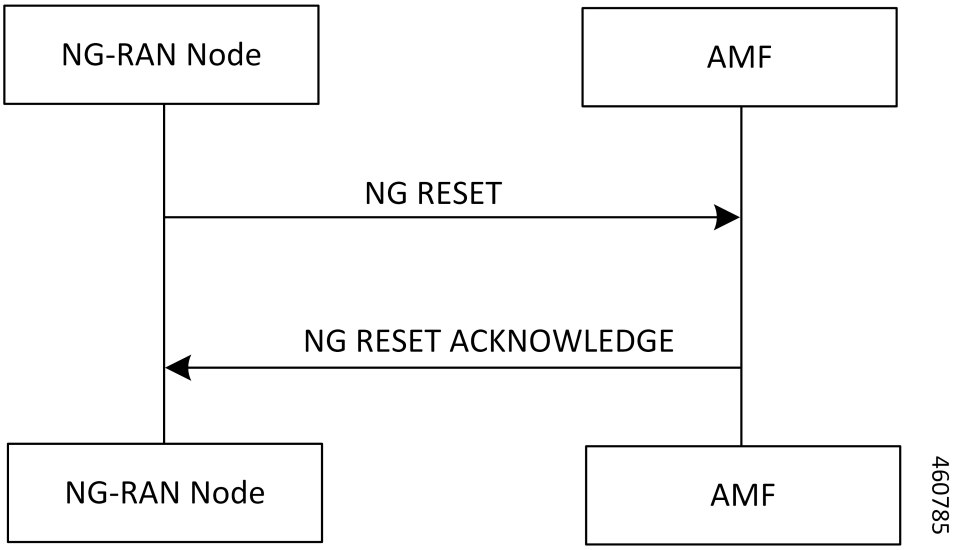
```
IE Type: id-ResetType(88)
{'ResetType': {'choice-Extensions': None,
'nG-Interface': None,
'partOfNG-Interface': {0: {'UE-associatedLogicalNG-connectionItem': {'aMF-UE-NGAP-ID':
4194359,
'iE-Extensions': None,
'rAN-UE-NGAP-ID': 12346}}}}}
```

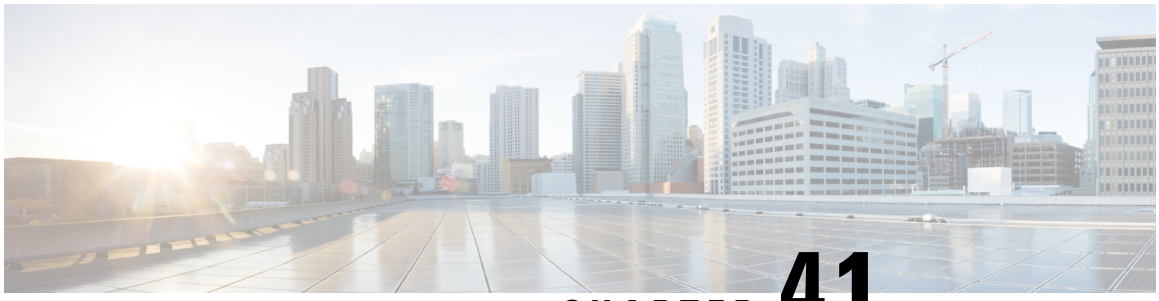
How it Works

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 58: Reset Procedure Initiated from gNB to AMF





CHAPTER 41

Periodic Registration Support

Feature Summary and Revision History

Summary Data

Table 143: 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 144: 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 (MR) timer. It is configurable but is different from T3512. T3512 is the configured in the UE, and the 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 state, 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.

The AMF sends the T3512 timer value in the Registration Accept or Registration Reject message to the UE and the UE uses this value to send the 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 59: Periodic Registration without Authentication Call Flow

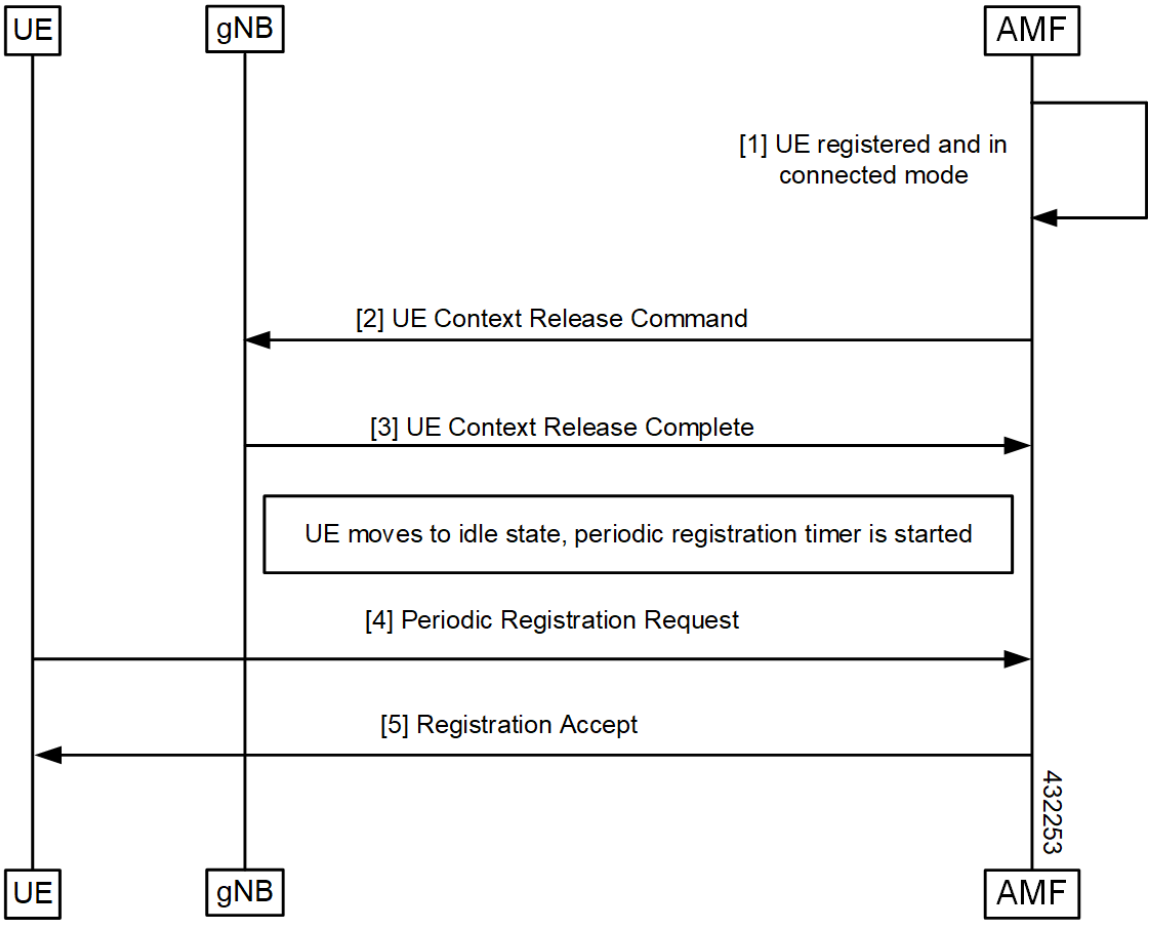


Table 145: Periodic Registration without Authentication Call Flow Description

Step	Description
1	The UE registered with the network and it's in CONNECTED mode.
2	The AMF sends the Context Release Command to the gNB.
3	The AMF receives the Context Release Complete from the gNB.
4	When UE moves to IDLE state, a periodic timer started and UE sends periodic registration request to the AMF.
5	The UE receives Registration Accept from the AMF.

Periodic Registration with Authentication Call Flow

This section describes the Periodic Registration with Authentication call flow.

Figure 60: Periodic Registration with Authentication Call Flow

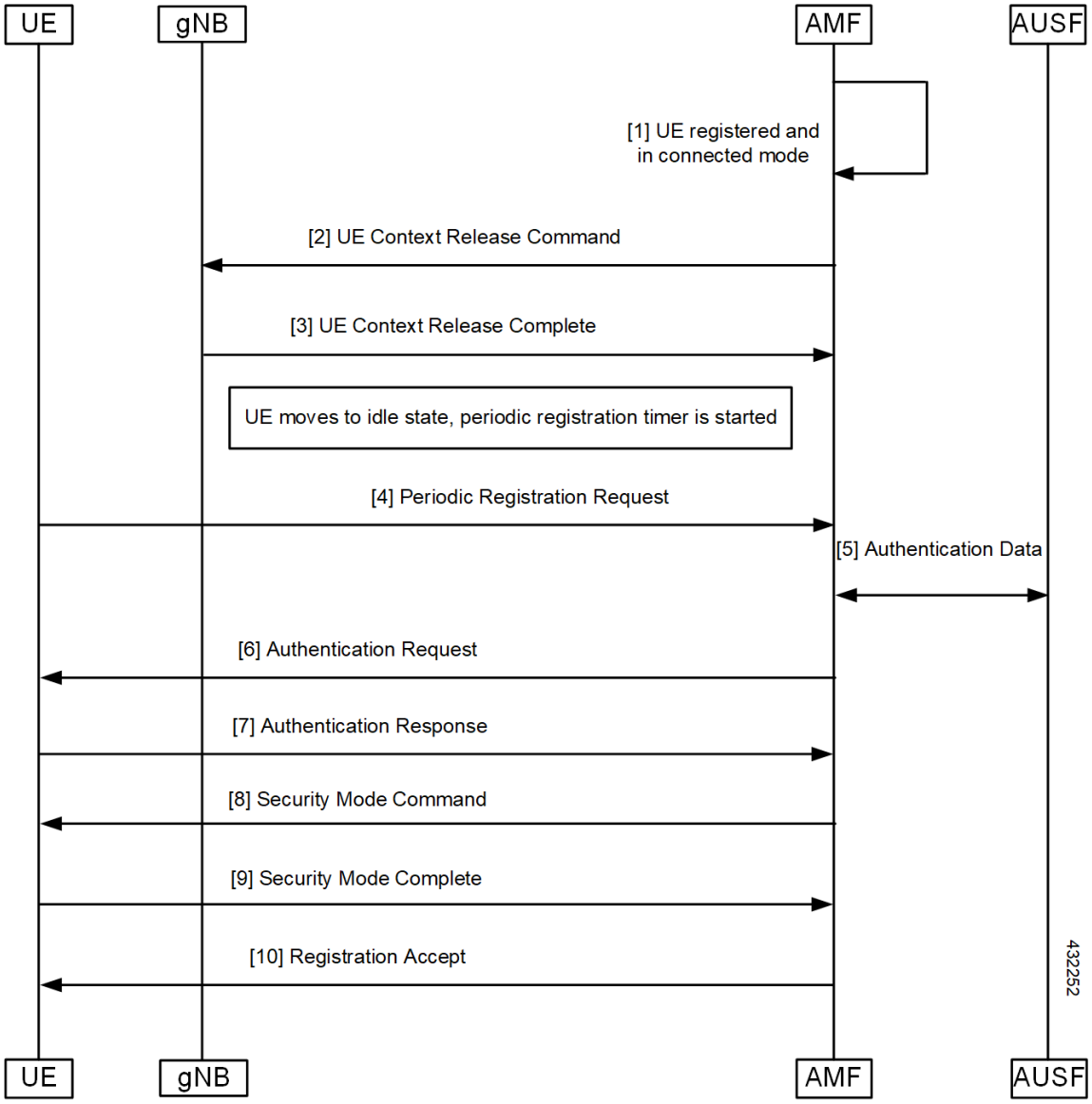


Table 146: Periodic Registration with Authentication Call Flow Description

Step	Description
1	Periodic Registration with Authentication UE registered with the network and it's in CONNECTED mode.
2	The AMF sends the Context Release Command to the gNB.
3	The AMF receives the Context Release Complete from the gNB.

Step	Description
4	When the UE moves to IDLE state, a periodic timer started and the UE sends the Periodic Registration Request to the AMF.
5	Authentication data exchanged between the AMF and the AUSF.
6	The AMF sends the Authentication Request to the UE.
7	The AMF receives the Authentication Response from the UE.
8	The AMF sends the Security Mode Command to the UE.
9	The AMF receives the Security Mode Complete Command from the UE.
10	The AMF sends the Registration Accept to the AMF.

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 337.
- Periodic registration is enabled in the call-control profile. For more information, refer to Configuring Authentication Enable, on page 337.

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.

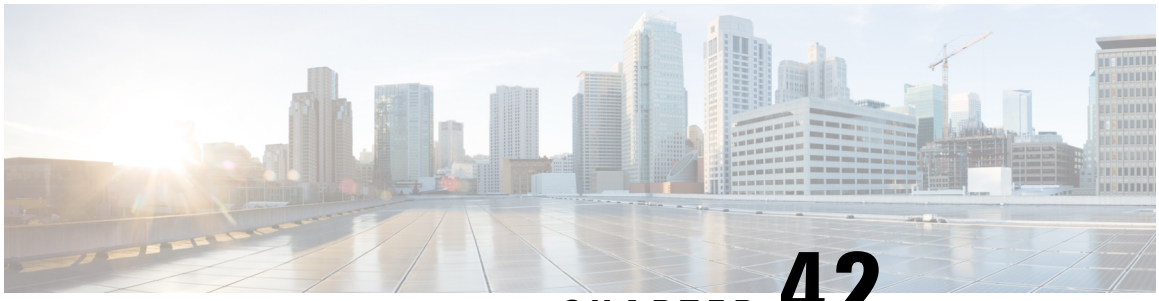
OAM Support

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 42

Relative Capacity Configuration Update

Feature Summary and Revision History

Summary Data

Table 147: Summary Data

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

Revision History

Table 148: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

The AMF supports modification of relative AMF capacity and notifies to the connected gNodeBs. The AMF also provides an option to control the rate at which existing sessions can be cleared in the AMF.

How it Works

This section describes how this feature works.

When the AMF detects changes in the Relative AMF Capacity configurations, it performs the following actions:

- The AMF triggers the configuration updates toward all the gNBs and each request has a timeout value of 30 seconds, which is a hardcoded value.
- The AMF waits for all the responses and timeout to occur for all the requests toward gNBs.
- The AMF consolidates the completed list of gNBs from which failure is received with TimeToWait IE from gNB. The IE indicates the minimum time, for which the AMF must wait before retransmitting.
- The AMF calculates the maximum value of TimeToWait, received across all the failure responses as the waiting time, before it retransmits to all the failed gNBs.
- The AMF retransmits only to those gNBs which have sent TimeToWait IE and retransmission will be done only once. No further action will be taken on further failure responses.
- If there are new configuration changes and if there is already an AMF configuration update procedure in progress, then the ongoing configuration is prioritized. The AMF handles the new configuration changes, only after the completion of the ongoing AMF configuration update procedure.

Clear Sub

Operators can clear the existing sessions at specific rate by issuing **clear sub all** command along with the rate option.

Call Flows

This section describes the key call flows for this feature.

AMF Configuration Updates Call Flow

This section describes the AMF Configuration Updates call flow.

Figure 61: AMF Configuration Updates Call Flow

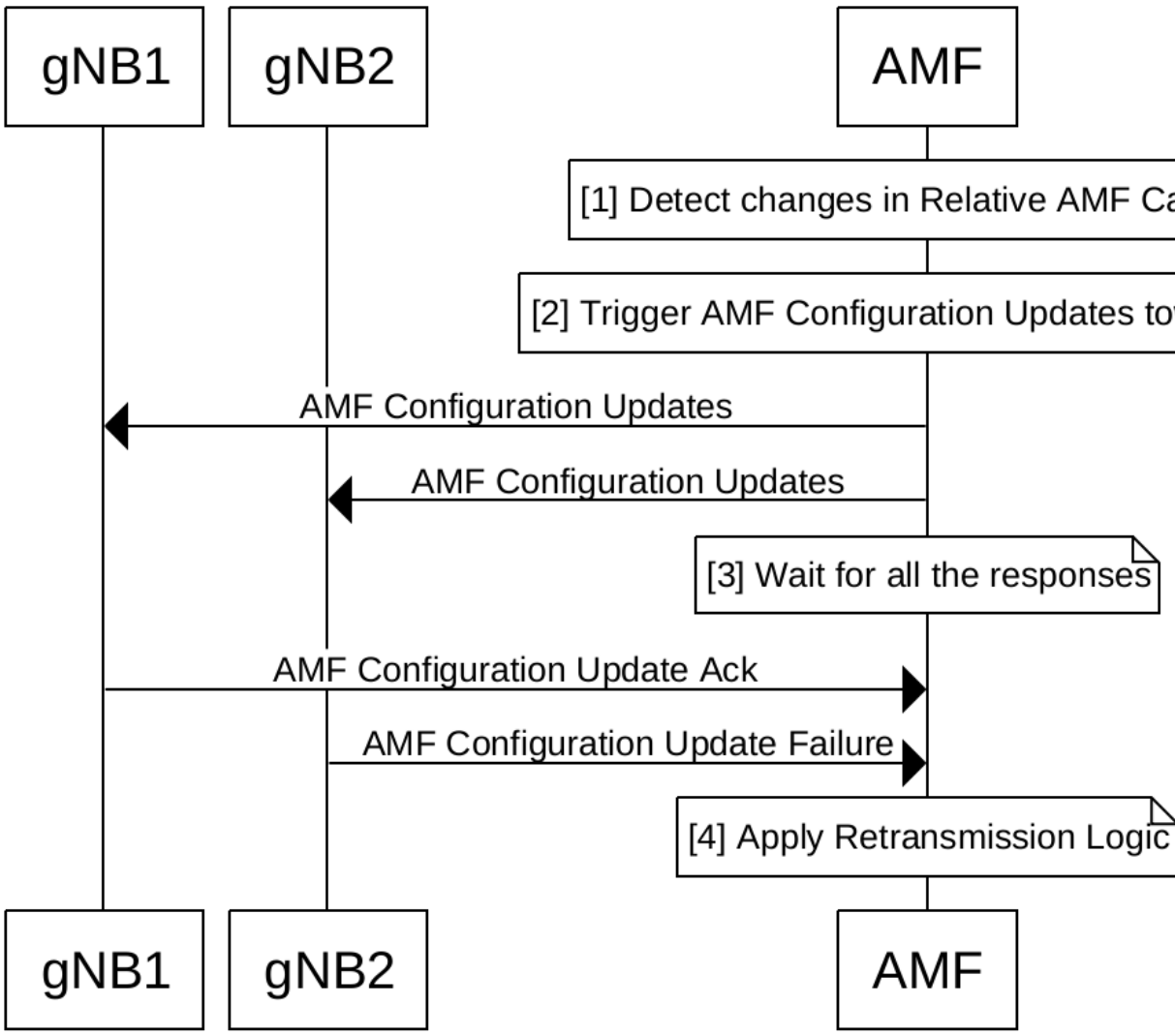


Table 149: AMF Configuration Updates Call Flow Description

Step	Description
1	The configuration for the relative AMF capacity is detected and modified.
2	The modified AMF configuration updates are triggered toward all the available gNBs, such as gNB1, gNB2, and so on.
3	The AMF waits and consolidates responses from gNBs.

Step	Description
4	Calculates overall wait time as the Maximum of all incoming TimeToWait and starts retransmissions. Retransmission is done toward those gNBs, which have responded with the TimeToWait IE. **Note** Retransmission is done only once.

Note The following are important feature-related references:

- The AMF does not update any capacity changes toward the NRF, as part of this feature.
- If there is a protocol pod restart, the ongoing AMF configuration updates procedure will be aborted, and not resumed.

Feature Configuration

Configuring this feature involves the following steps:

- Clearing Subscribers with Rate
- Configuring Relative AMF Capacity

Clearing Subscribers with Rate

To clear Subscribers with Rate, use the following command:

```
clear subscriber all rate rate
```

Configuring Relative AMF Capacity

To configure Relative AMF Capacity, use the following configuration:

```
config
   amf-services service_name
      relative-amf-capacity capacity_number
```

NOTES:

- **subscriber**—Specifies the UE subscriber clear condition type.
- **all**—Clears all the subscriber sessions.
- **rate** *rate*—Specifies the rate at which the AMF attempts to clear the existing sessions, within the range of 100-500. The default value is 100.
- **relative-amf-capacity** *capacity_number*—Specifies the AMF capacity, within the range of 0–255. The default value is 127.

Configuration Example

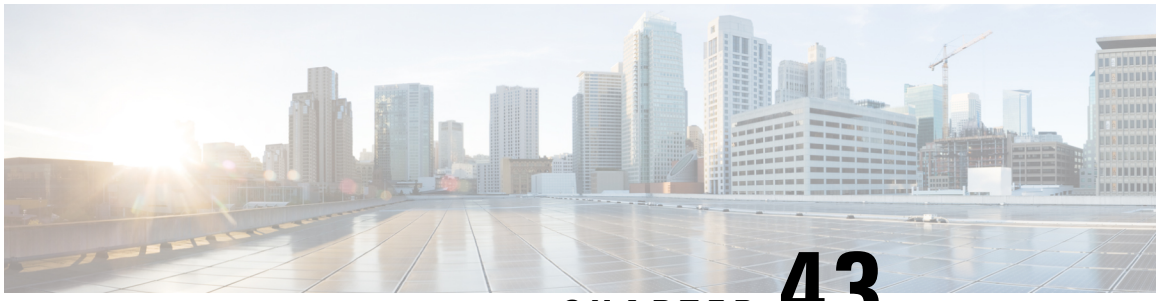
The following is an example configuration.

```
clear subscriber all rate 300
```

Configuration Verification

To verify the configuration:

```
show running-config amf-services service_name
relative-amf-capacity 100
```



CHAPTER 43

Retrieving IMEI from the UE

Feature Summary and Revision History

Summary Data

Table 150: 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 151: Revision History

Revision Details	Release
First introduced.	2022.02.0

Feature Description

Completion of the registration procedure includes retrieving the International Mobile Equipment Identity (IMEI) or International Mobile Equipment Identity – Software Version (IMEI-SV) from the UE. The AMF

retrieves the IMEI or IMEI-SV from the UE by sending the Identity Request or Security Mode Command message. The AMF communicates the retrieved IMEI or IMEI-SV to its peer NFs.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Registration Procedure Call Flow

This section describes the Registration Procedure call flow.

During the initial registration procedure, the PEI is obtained from the UE. The AMF operator may check the PEI with an EIR. After receiving the PEI (IMEI-SV), the AMF communicates it to the UDM, SMF, and PCF. The UDM stores the PEI in the UDR by sending the Nudr_SDM_Update message.

Figure 62: Registration Procedure Call Flow

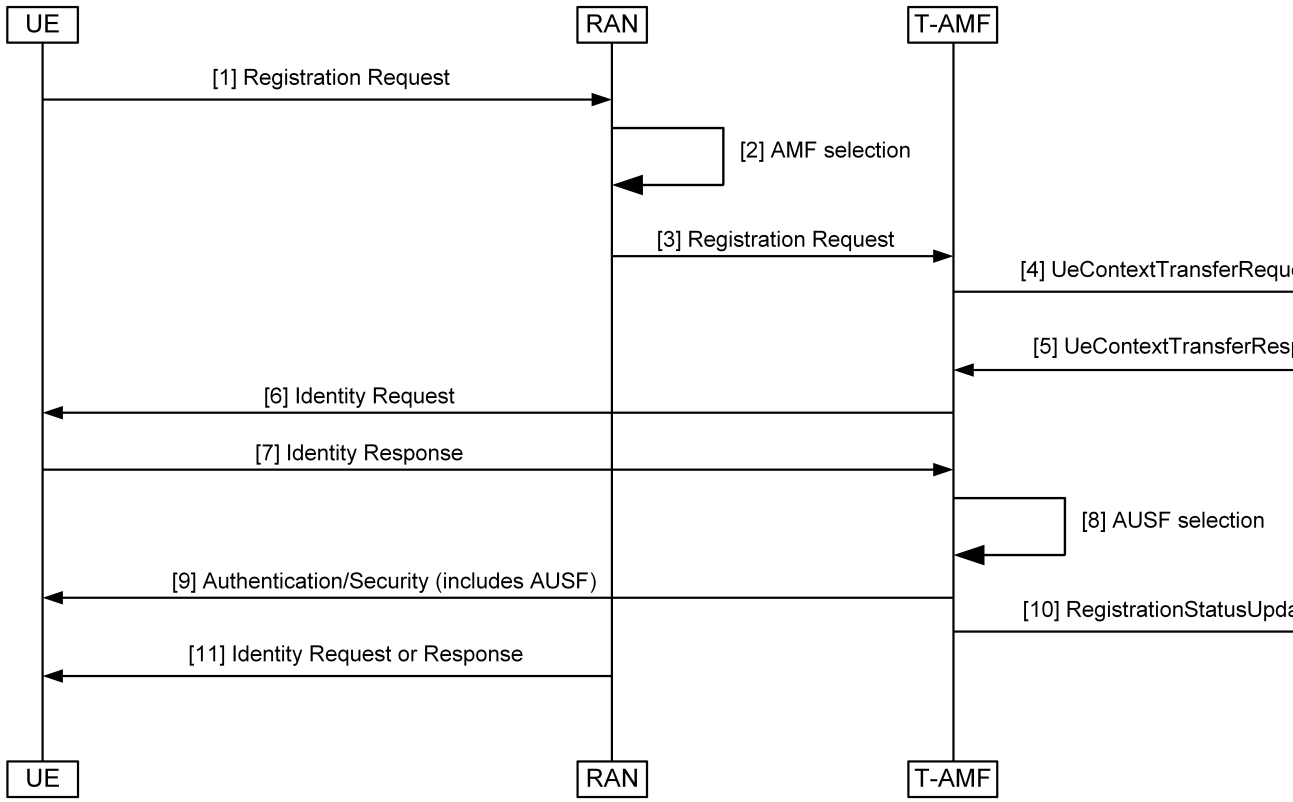


Table 152: Registration Procedure Call Flow Description

Step	Description
1	The UE sends a Registration Request to the RAN. The Registration Request message includes PEI as part of N2 information. If the PEI is not available, the AMF sends an Identity Request message to retrieve IMEI-SV.
2	The RAN performs the AMF selection procedure.
3	The RAN sends the Registration Request to the T-AMF.
4	The T-AMF sends a UeContextTransferRequest to the S-AMF.
5	The S-AMF responds to the AMF with UeContextTransferResponse.
6	The T-AMF sends the Identity Request message to the UE.
7	The UE sends the Identity Response message to the T-AMF.
8	The T-AMF performs the AUSF selection procedure.
9	The T-AMF sends the Authentication or Security message to the UE.
10	The T-AMF sends the RegistrationStatusUpdate message to the S-AMF.
11	The T-AMF sends the Identity Request or Response (PEI) message to the UE. The AMF initiates the Identity Request procedure by sending an Identity Request message to the UE to retrieve the PEI when: • The UE does not provide the PEI. • The UE cannot retrieve the PEI from the old AMF. The AMF transfers an encrypted PEI unless the UE performs an Emergency Registration. For Emergency Registration, the UE includes the PEI in the Registration Request so that the PEI retrieval step is skipped.

Idle or Connected Mode Mobility Call Flow

This section describes the Idle or Connected Mode Mobility call flow.

Figure 63: Idle or Connected Mode Mobility Call Flow

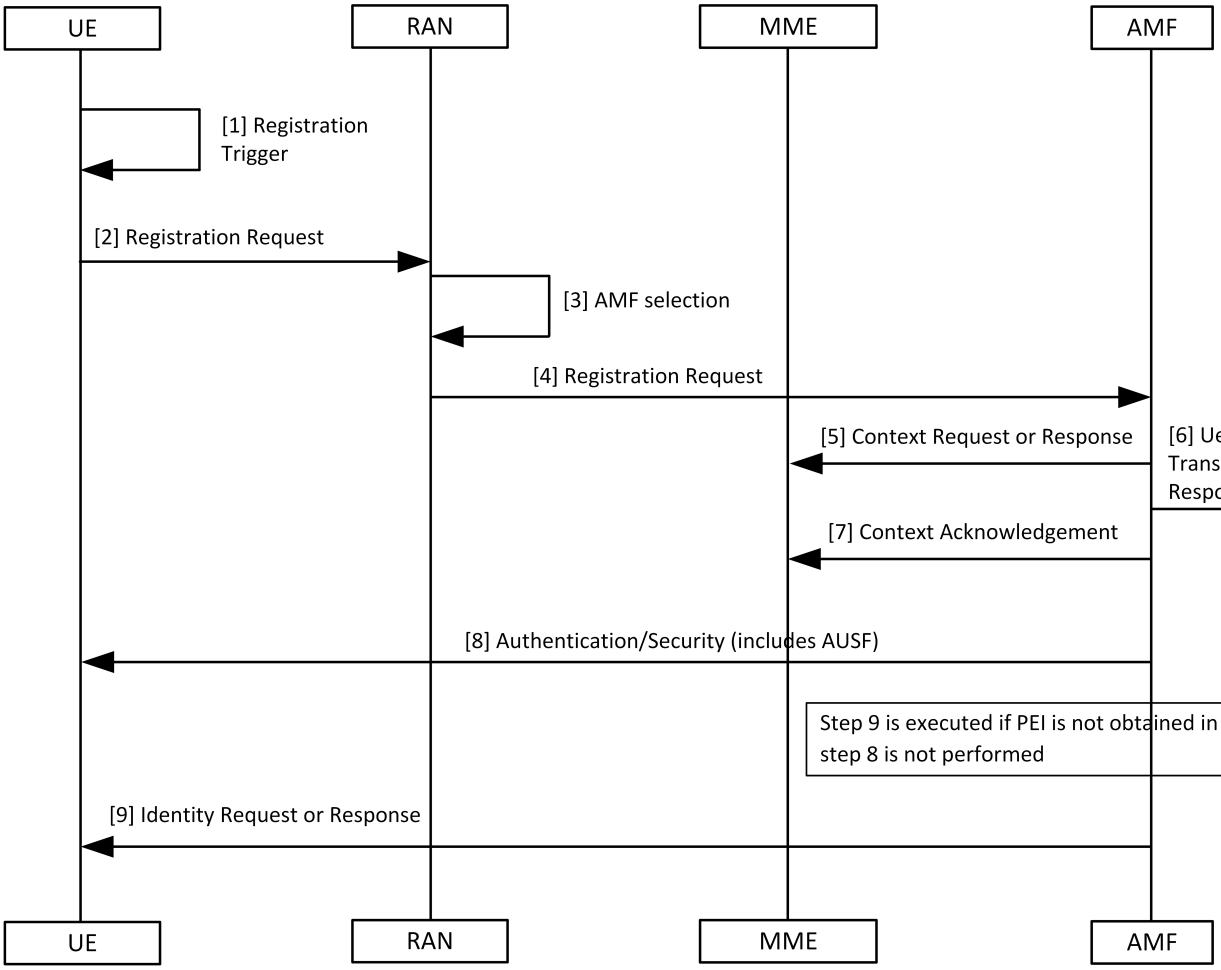


Table 153: Idle or Connected Mode Mobility Call Flow Description

Step	Description
1	The UE sends a Registration Trigger.
2	The UE sends a Registration Request to the RAN.
3	The RAN performs an AMF selection.
4	The RAN sends a Registration Request to the AMF.
5	The AMF sends a Context Request or Response message to the MME.
6	The AMF sends a UeContextTransfer Request or Response to the Old AMF.
7	The AMF sends the Context Acknowledgement message to the MME.
8	The AMF sends an Authentication or Security message to the UE.

Step	Description
9	The AMF sends the Identity Request or Response message to the UE.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP 29.502 "5G System; Session Management Services; Stage 3"*
- *3GPP 29.503 "5G System; Unified Data Management Services; Stage 3"*
- *3GPP 23.502 "Procedures for the 5G System (5GS)"*
- *3GPP 24.501 "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"*
- *3GPP 23.003 "Numbering, addressing and identification"*

Viewing the Retrieved IMEI

To view the IMEI or IMEI-SV that AMF retrieved:

```
show subscriber supi 123456789012345
subscriber-details
{
  "subInfo": {
    "Genericinfo": {
      "RanUeNGAPID": 12346,
      "AmfUeNGAPID": 201328650,
      "NGAPConnID": 21472,
      "Supi": "123456789012345",
      "Imei": "imei-352099001761480",
      "UeId": "supi:123456789012345",
```

```
show subscriber supi 123456789012345
subscriber-details
{
  "subInfo": {
    "Genericinfo": {
      "RanUeNGAPID": 12346,
      "AmfUeNGAPID": 201328650,
      "NGAPConnID": 21472,
      "Supi": "123456789012345",
      "Imei": "imeisv-3520990017614856",
      "UeId": "supi:123456789012345",
```

OAM Support

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

Bulk Statistics Support

The following statistic is supported for the Retrieving IMEI from the UE feature:

n1_service_stats

Description: The AMF UE service statistics.

Sample Query:

```
n1_service_stats{message_type="IdentityRequest_Imeisv",status="success",reason="key
Mismatch",slice_data="2-333333"}
```

Labels:

- Label: `message_type`

  Label Description: The message type associated with a UE service.

  Example: IdentityRequest_Imeisv, N1SecurityModeComplete, N1AuthenticationRsp, N1SecurityModeCommand, N1AuthenticationReq, N1AuthFail_SyncFailure, N1AuthenticationReject, N1AuthFail_MacFailure, IdentityRequest_Imei, IdentityRequest_Suci, N1DeRegAccept_UeTerminatedDereg, N1UeConfigurationUpdCmd.

- Label: `status`

  Label Description: Overall status.

  Example: success, failures, attempted

- Label: `reason`

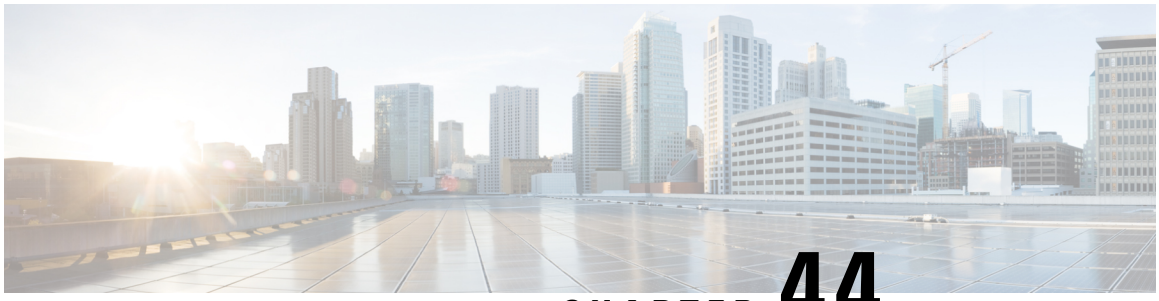
  Label Description: The reason associated with an UE service.

  Example: Suspend, Suspend for Async, Unable to get rsp, Unable to retrieve msg from rsp, Supi mismatch, Internal Error, Sync Failed, Timeout, Others, No Security Context from Peer, Peer Provided Sec Context Failed, NgKsi Already In Use, Scheduled ipc action in background, Unable to retrieve identity rsp, Unable to get Supi, key Mismatch

- Label: `slice_data`

  Label Description: Slice data.

  Example: 2-333333



CHAPTER 44

Roaming Support

Feature Summary and Revision History

Summary Data

Table 154: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Steering of Roaming, Roaming Restrictions, and Operator Policy Support, on page 413

Revision History

Table 155: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

AMF supports the following roaming types:

- Inter-operator roaming
- Roaming on N9 and S8 interface
- Steering of roaming, roaming restrictions and operator Policy Support

N9 and S8 Roaming

Feature Description

Table 156: Feature History

Feature Name	Release Information	Description
Local Break Out (LBO) Support for N9 Roaming	2024.01.1	AMF supports local breakout for N9 roaming irrespective of prsence of NRF configuration. This LBO support ensures a seamless network connectivity for roaming subscribers.

AMF checks if the subscriber is a roamer or homer, during registration. For a roamer subscriber, AMF selects one of the following roaming procedures:

- Home-routed roaming: This procedure enables the subscribers to access the visited network through the home PDN gateway (H-PGW) and obtain services provided by their home networks.
- Local Break Out (LBO) roaming: This procedure enables the subscribers to obtain visitor network provided services. LBO routes the traffic to the visited network, without routing through the home network before sending to or from the end destination.

AMF discovers the following NFs using NRF services, as per the selection of homer or roamer:

- AUSF
- PCF
- UDM
- SMF

Prerequisites

NRF configuration must be available.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

N9 Home Routed Roaming Call Flow

This section describes the N9 Home Routed Roaming call flow.

Figure 64: N9 Home Routed Roaming Call Flow

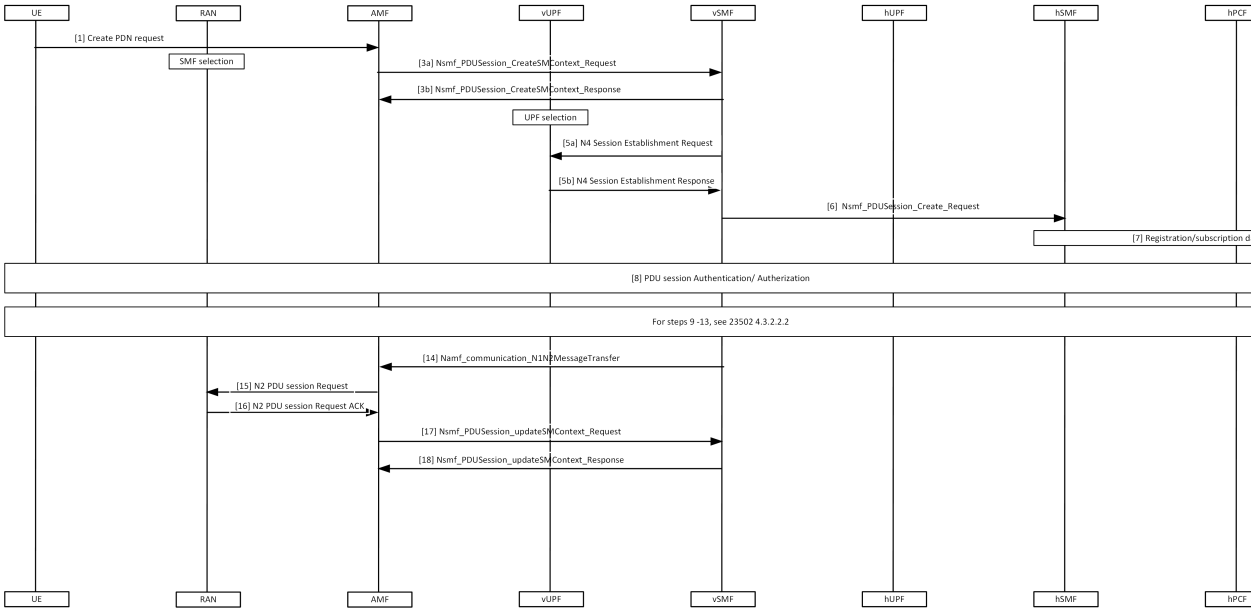


Table 157: N9 Home Routed Roaming Call Flow Description

Step	Description
1	The UE sends the Create PDN Request to AMF.
2, 3a, 3b	AMF performs the SMF selection and sends Nsmf_PDUSession_CreateSMContext_Request to vSMF and receives response.
4	vUPF performs the UPF selection.
5a, 5b	vSMF sends the N4 Session Establishment Request to vUPF and receives a response from it.
6	vSMF sends Nsmf_PDUSession_Create_Request to the hSMF.
7	Registration or subscription data retrieval is performed.
8	PDU session Authentication or Authorization procedure is performed.
9-13	See *3GPP TS 23502, version 15.4.0*, section *4.3.2.2.2*.
14	vSMF sends Namf_communication_N1N2MessageTransfer to SMF.
15, 16	AMF sends N2 PDU Session Request to RAN and receives a response.

Step	Description
17, 18	AMF sends Nsmf_PDUSession_updateSMContext_Request to vSMF and receives a response.

Note For Local Breakout, the AMF uses the local SMF configuration in the absence of an NRF configuration.

S8 Home Routing Call Flow

This section describes the S8 Home Routing call flow.

For the preparation phase, see *3GPP TS 23502, Release 15.4.0, section 4.11.1.2.2.2-1*—EPS to 5GS (4G to 5G) handover using N26 interface.

The home-routed roaming scenarios support the following functionalities:

- H-PLMN supports the following nodes:
  - PGW-C and SMF
  - UPF and PGW-U
- AMF selects a default vSMF per PDU session, and invokes the Nsmf_PDUSession_CreateSMContext service operation with the following:
  - UE PDN connection contexts
  - AMF ID
  - SMF
  - PGW-C address
  - S-NSSAI
- The S-NSSAI is configured for interworking and is associated with default vSMF.
- The default vSMF puts S-NSSAI in the N2 SM information container.
- AMF selects PGW-C and SMF through NRF from S8 FQDN (obtained from the MME).

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.501 "System Architecture for the 5G System"*
- *3GPP TS 23.502 "Procedures for the 5G System"*
- *3GPP TS 24.501 "Non-Access-Stratum (NAS) protocol for 5G System"*
- *3GPP TS 29.503 "Unified Data Management Services"*
- *3GPP TS 29.513 "Policy and Charging Control signalling flows and QoS parameter mapping"*
- *3GPP TS 29.518 "Access and Mobility Management Services"*

Feature Configuration

Configuring this feature involves the following steps:

- Configure the LBO—This configuration provides the commands to configure LBO roaming. For more information, refer to Configuring the LBO, on page 355.
- Configure the MNC digits in SUPI—This configuration provides the commands to configure the number of MNC digits in SUPI. For more information, refer to Configuring the MNC bits in SUPI, on page 356.

  Configure the MNC bits in SUPI to discover the exact peer NF in roaming.
- Configure the Globally Unique AMF ID (GUAMI) for AMF selection—This configuration provides the commands to configure the GUAMI. For more information, refer to Configuring the GUAMI for AMF Selection, on page 356.

Configuring the LBO

To configure Local Break Out, use the following configuration:

```
config
   amf-global
      dnn-policy policy_name
         lbo-roaming-allowed { true | false }
         end
```

NOTES:

- **dnn-policy** *policy_name*—Specify the DNN policy name.
- **lbo-roaming-allowed { true | false }**—Specify LBO roaming allowed or not. Configuring **lbo-roaming-allowed** has minimum priority. The priorities are as follows:

  1. When UE includes a DNN name in the PDU Establishment Request, the DNN name is validated with the UDM subscription data. The LBO flag in the UDM subscription data has maximum priority.
  2. When UE doesn't include DNN name in PDU Establishment Request, AMF checks for the default DNN in UDM subscription. If the default DNN is available in the UDM subscription, the LBO flag is considered from the UDM subscription data.
  3. When UE doesn't include DNN name and UDM doesn't provide any default DNN, AMF checks for the configured default DNN. The corresponding DNN policy is checked for the configured default DNN and the LBO is configured using *Configuring the LBO*.

  When **lbo-roaming-allowed** configured as true, or UDM sends this flag, LBO roaming is considered. Otherwise Home-routed roaming is considered.

Note AMF provides a **lbo-roaming-allowed** CLI within the DNN Policy. This CLI allows overriding the LBO flag sent in the UDM subscription. Specifically, when the LBO flag is false or missing, you can configure the override CLI to true.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      dnn-policy dn1
         lbo-roaming-allowed true
         end
```

Configuring the MNC bits in SUPI

To configure the MNC bits in SUPI, use the following configuration:

```
config
    amf-global
        call-control-policy policy_name
            supi
                mnc number_of_mnc_bits
                end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- **mnc** *number_of_mnc_bits*—Specify the number of MNC bits. Must be either 2 or 3.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy local
         supi
            mnc 2
            end
```

Configuration Verification

To verify the configuration:

```
show running-config amf-global call-control-policy local
amf-global
call-control-policy local
supi mnc 2
```

Configuring the GUAMI for AMF Selection

To configure the GUAMI for AMF selection, use the following configuration:

```
config
    profile network-element amf amf_name
        query-params guami
        end
```

NOTES:

- **profile network-element amf** *amf_name*—Specify AMF name. Must be a string.
- **query-params guami**—Specify query parameters as GUAMI.

Configuration Verification

To verify the configuration:

```
show running-config profile network-element amf amf1 query-params
profile network-element amf amf1
query-params guami
```

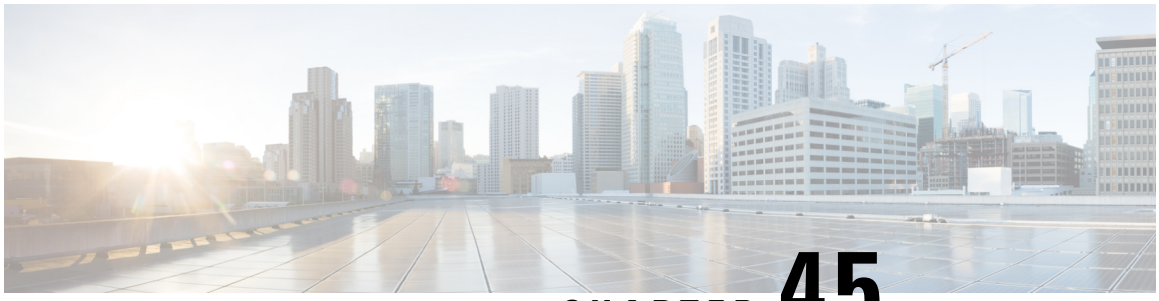
Configuring the 5GC Inter-PLMN Roaming

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
      local-cause-code-map registration-restriction cause-code-5gmm
plmn-not-found
      end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- **local-cause-code-map registration-restriction cause-code-5gmm plmn-not-found**—When the subscriber is a roamer and has registration restrictions, the AMF rejects the subscriber with the **plmn-not-found** cause setting.



CHAPTER 45

SCTP Multihoming and Stack Parameters Support

Feature Summary and Revision History

Summary Data

Table 158: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	

Revision History

Table 159: Revision History

Revision Details	Release
The following enhancements were introduced: • Support to configure SCTP stack parameters. • Support for multiple SCTP and protocol pod pairs • Support for show SCTP peers CLI	2022.01.0
First introduced.	2020.03.0

Stream Control Transmission Protocol (SCTP) Multihoming

Stream Control Transmission Protocol (SCTP) is a message-oriented, reliable, transport protocol. SCTP directly supports multihoming transport protocol that runs on top of an IP network. SCTP used as a protocol with pods, services, and network policy.

Multihoming is the ability of an SCTP association to support multiple IP paths to its peer endpoint.

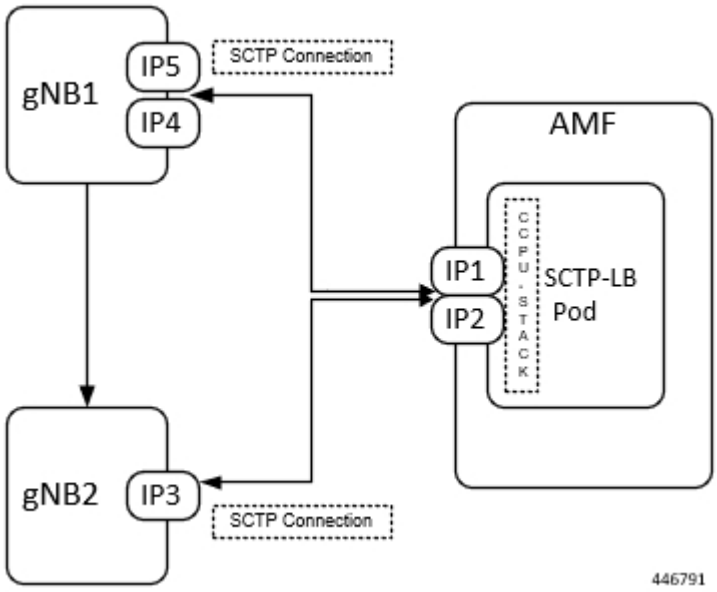
Feature Description

AMF supports a single SCTP pod (single instance) for SCTP multihoming, where the SCTP stack comes up with a list of supported host IPs. As part of the association formation, the association ID corresponds to the list of IPs, instead of a single IP.

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

The following figure represents the support structure for SCTP Multihoming:

Figure 65: SCTP Multihoming Support



Based on the represented figure, the following SCTP associations are formed:

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

Limitations

The SCTP multihoming feature has the following limitations:

- Currently not supported:
  - Dynamic addition or removal of IPs from the multihoming configuration without the pod restart
  - Dynamic service config delete and also dynamic IP change
- Currently observed and recommended:
  - If both member of the pair goes down, there's no redundancy.
  - Even though multiple protocol pairs are supported, there's a limitation with multiple protocol pairs. As a best practice, recommended to configure only one protocol pod pair.
  - One gNB can have only one association with AMF. Multiple associations with same gNB aren't supported.

SCTP Multihoming and Stack Parameters Support

This section describes support for the following features:

- SCTP Configurable Stack Parameters
- Multiple SCTP and Protocol Pod Pairs

Feature Description

Before implementing this feature, AMF needs separate deployment of the following five namespaces for scalability. Each AMF namespace supports the following:

- A pair of SCTP pods (active-standby)
- A pair of Protocol pods (active-standby)
- Extra pods getting deployed on Ops Center and ETCD

A single AMF namespace supports and deploys multiple SCTP pods and protocol pods. SCTP pods support multihoming and some SCTP stack-related parameters are configurable.

SCTP Configurable Stack Parameters

SCTP uses the multihomed host to provide fast failover and associated endurance during hardware failures. Using the associated parameters, the following activities are supported:

- Creating and customizing the required stack
- Configuring the resources by modifying the parameter values, which are later used in the stack template.
- No need to enter hardcoded values in multiple templates to specify different settings.

Multiple SCTP and Protocol Pod Pairs

Pods are tagged with one or more labels. The labels are later used to select and manage groups of pods in a single operation. The labels are stored in a key-value format in the metadata hash.

How it Works

This section describes how this feature works.

Multihoming Support

Supports multiple IP addresses for the SCTP stack.

Multiple SCTP and Protocol Pod Pairs

In a single AMF namespace, multiple SCTP pairs can be configured. This way on same AMF, SCTP pods can be scaled up, as per the requirement.

Configurable SCTP Endpoint Stack Parameter

Provides the option to configure multiple SCTP Endpoint stack parameters which includes the following:

- RTO
- Association
- Sack
- MTU Size

Feature Configuration

Configuring this feature includes the following steps:

- Configuring Multiple SCTP and Protocol Pod Pairs
- Configuring SCTP Endpoint Parameters

Configuring Multiple SCTP and Protocol Pod Pairs

To configure multiple SCTP and Protocol pod pairs use the following configuration:

```
config
    instance instance_id instance_id
    endpoint endpoint_name
    replicas replicas_per_node
    service service_name
        interface interface_name instancetype instance_type
        internal-port internal_port_config
        vip-ip ip_address vip-port port_number
        offline vip-interface vip_interface_name
        vip-ip6 ip_address vip-ipv6-port port_number
        offline vip-interface
        end
```

NOTES:

- **instance instance_id** *instance_id*—Specify the endpoint instance ID. Must be an integer in the range of 1-4.

- **endpoint** *endpoint_name*—Specify the endpoint name.

Note In this release, it is recommended not to configure any service under NGAP. Currently, only one service can be configured under NGAP.

- **replicas** *replicas_per_node*—Specify the number of replicas per node.
- **service** *service_name*—Specify the service name.
- **interface** *interface_name*—Specify the endpoint interfaces, as the name of the SCTP in this multiple SCTP configuration. **sctp-1-sctp-primary** is an example.
- **instancetype** *instance_type*—Specify the instance type. Must be one of the following:
  - Dual
  - IPv4
  - IPv6

  The default value is Dual.
- **internal-port** *internal_port_config*—Specify the internal base-port to start the endpoint. It includes your required internal-ports and their ID from the list of available ports.
  - admin—Admin port for SCTP. The default value is 7879.
  - ipc—IPC port for SCTP. The default value is 9005.
  - keepalived—keepalived port for SCTP. The default value is 29000.
  - metrics—metrics port for SCTP. The default value is 7083.
  - pprof—pprof port for SCTP. The default value is 7850.

Note It is mandatory to configure the internal-ports CLI when more than one SCTP service is configured or more than one AMF is deployed on the same k8 cluster.

- **vip-ip** *ip_address* **vip-port** *port_number* **offline**—Specify the IPv4 address of the pod on which the VIP is enabled. Also, specify the interface and port number. This configuration marks vip-ip as offline or standby.

Note When AMF receives SCTP INIT from IPv4 address and no address is included in INIT chunk address list, AMF responds with all IPv4 and IPv6 addresses in SCTP INIT_ACK.

- **vip-interface** *vip_interface_name* —Specify the VIP interface and port number. This configuration marks **vip-ip** as offline or standby.

Note To support multi-homing, AMF listens on multiple IP address as configured.Currently, AMF uses VIP to support high availability of SCTP pods. For multi-homing, multiple VIP addresses should be configured.

It is recommended to use different physical interfaces for each different VIP so that AMF can have different routes for each VIP address.

- **vip-ip6** *ip_address* **vip-ipv6-port** *port_number*—Specify the new IPv6 address and port number.

Note When AMF receives SCTP INIT from IPv6 address and no address is included in INIT chunk address list, AMF respond with only IPv6 addresses in SCTP INIT_ACK.

After the VIP-IP and VIP-Ports are up, modify the gNBs configuration to refer to the new VIP-IP and port.

Configuration Example

The following is an example configuration.

- CLI at endpoint level: If more than one AMF is deployed in same cluster with one single SCTP service.

```
config
  instance instance-id 1
    endpoint sctp
     replicas 2
     internal-port metrics 9705 admin 9703 ipc 9701 pprof 9707 keepalived 29001
     vip-ip 209.165.201.15 vip-port 1000
     end
```

- CLI at SCTP service level: If more than one SCTP service is configured.

```
config
 instance instance-id 1
  endpoint sctp
   replicas 2
   nodes    2
   parameters mtu-size 1500
   service sctp-1 interface sctp instancetype Dual
    internal-port metrics 9705 admin 9703 ipc 9701 pprof 9707 keepalived 29001
    vip-ip 209.165.201.15 vip-port 1000
   service sctp-2 interface sctp instancetype Dual
    internal-port metrics 9715 admin 9713 ipc 9711 pprof 9717 keepalived 29011
    vip-ip 209.165.201.16 vip-port 1000
    end
```

Configuration Verification

To verify the configuration:

```
show running-config instance
```

Configuring SCTP Endpoint Parameters

To configure the SCTP endpoint parameters, use the following configuration:

```
config
   instance instance_id instance_id
   endpoint endpoint_name
      replicas number_of_nodes
         parameters rto initial rto_initial
         parameters rto min rto_min
         parameters rto max rto_max
         parameters association valid-cookie-life valid_cookie_life
         parameters association heartbeat-interval heartbeat_interval
         parameters association path-max-retry-count path_max_retry_count
         parameters sack sack-period sack_period
         parameters sack sack-frequency sack_frequency
         parameters mtu-size mtu_size
         end
```

NOTES:

- **instance instance_id** *instance_id*—Specify the endpoint instance ID. Must be an integer in the range of 1-4.
- **endpoint** *endpoint_name*—Specify the endpoint as SCTP.
- **replicas** *number_of_nodes*—Specify the number of node replicas that must be configured for resiliency. The minimum or default value is 2.
- **parameters**—SCTP tuning parameters.
- **rto**—Retransmission timeout parameters.
- **association**—Association parameters.
- **mtu-size**—Maximum SCTP fragment or MTU size for data packets.
- **sack**—Configures the way delayed SACKs are performed.
- **initial** *rto_initial*—Specify the initial timeout in milliseconds. Must be an integer in the range of 100-60000. The default value is 3000.
- **min** *rto_min*—Specify the minimum timeout in milliseconds. Must be an integer in the range of 100-60000. The default value is 1000.
- **max** *rto_max*—Specify the maximum timeout in milliseconds. Must be an integer in the range of 100-60000. The default value is 60000.
- **valid-cookie-life** *valid_cookie_life*—Specify the cookie life in milliseconds. Must be an integer in the range of 5000-120000. The default value is 60000.
- **heartbeat-interval** *heartbeat_interval*—Specify the heartbeat interval in milliseconds. Setting the value to zero, disables the heartbeat. Must be an integer in the range of 0-60000. The default value is 30000.
- **path-max-retry-count** *path_max_retry_count*—Specify the path maximum retry count. Must be an integer in the range of 0-20. The default value is 5.

Note When single path/IP address is available, **path-max-retry-count** parameter defines maximum number of retransmissions of the DATA packets before the address is marked unreachable by sending ABORT (when only single path).

When multiple paths/IP addresses are available, **path-max-retry-count** parameter is not applicable. The parameter checks only for DATA packet and not HEARTBEAT packet sent in SCTP.

It is recommended not to change **path-max-retry-count** parameter value and use the default value.

- **sack-period** *sack_period*—Specify the delayed sack time in milliseconds. Must be an integer in the range of 200-500. The default value is 200.

Note This parameter is effective when no data packets are flowing.

- When no data packets are flowing, separate SACK message is sent to acknowledge the data to the sender.
- If data packets are already flowing, then SACK is sent along with the data.

- **sack-frequency** *sack_frequency*—Specify the delayed SACK frequency. Must be an integer in the range of 1-5. The default value is 2.

Note Changing the frequency to 1, disables the delayed SACK algorithm.

This parameter is effective when no data packets are flowing.

- When no data packets are flowing, separate SACK message is sent with all TSNs in one SACK message to acknowledge the data to the sender.
- If data packets are already flowing, then SACK is sent along with the data.

- **mtu-size** *mtu_size*—Specify the MTU size for the data packet. Must be an integer in the range of 512-1500. The default value is 1452.

Configuration Example

The following is an example configuration.

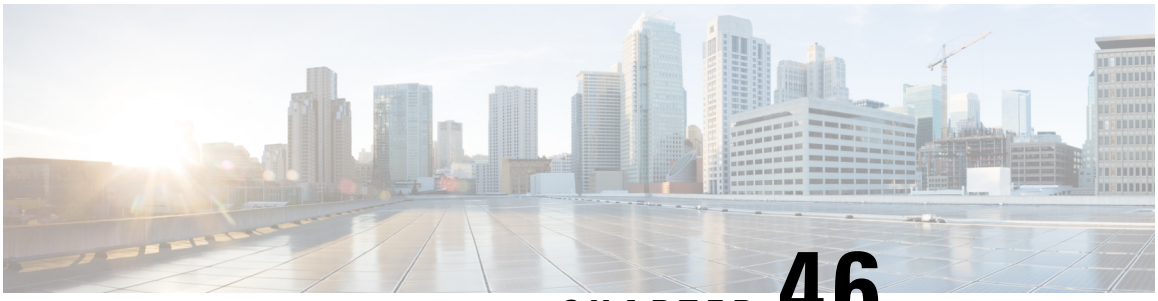
```
config
    instance 1
    endpoint sctp
        replicas 2
        parameters rto initial 30
        parameters rto min 10
        parameters rto max 600
        parameters association valid-cookie-life 60000
        parameters association heartbeat-interval 30000
        parameters association path-max-retry-count 5
```

```
parameters sack sack-period 2000
parameters sack sack-frequency 2
parameters mtu-size 1500
end
```

Configuration Verification

To verify the configuration:

```
show running-config instance
```



CHAPTER 46

Service Area Restriction

Table 160: Feature History

Feature Name	Release Information	Description
Service Area Restriction	2023.04	Cisco AMF supports the service area restriction for the UE to enforce restrictions on the services that UE can access based on location and tracking area codes. Default Setting: Disabled – Configuration Required

Feature Summary and Revision History

Summary Data

Table 161: 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 162: Revision History

Revision Details	Release
First introduced.	2023.04.0

Service Area Restriction

Service Area Restriction (SAR) is a mechanism that allows the network operators to define specific geographic areas where a User Equipment (UE) is either allowed or restricted to access services. The SAR enables fine-grained control over the availability of services based on the location of the UE.

Feature Description

The SAR involves configuring the 5G core network to enforce restrictions on the services that a UE can access based on its location, often identified by specific geographical identifiers such as Tracking Area Codes (TACs). The Service Area Restrictions (SAR) within subscription data can be configured by the Unified Data Management (UDM).

How it Works

The Access and Mobility Management Function (AMF) enhances its capabilities to provide robust service area restrictions handling, aligning with the access control information provided in subscriber data by the Unified Data Management (UDM) entity. This feature ensures that access restrictions based on subscription data are efficiently enforced for all subscribers.

Following are the capabilities of the service area restriction feature in the AMF:

- The AMF is equipped to receive and store the ServiceAreaRestriction data provided by the UDM in the subscriber's User Equipment (UE) context. This data encompasses information regarding allowed or not allowed areas for the subscriber.
- To enforce the defined service area restrictions, the AMF provisions the restriction information to the UE using registration accept and UE configuration update command message. The AMF communicates these restrictions to the Gnb using initial context setup request, handover request and downlink NAS transport messages.
- In mobility scenarios involving AMF changes, where a subscriber transitions from one AMF (S-AMF) to another (T-AMF), the service area restrictions provided by the UDM are transferred along with the UE context.

UDM based Service Area Restrictions

When the UDM provides the subscriber data, the AMF automatically implements and enforces access restrictions based on subscription data for all subscribers. The UDM can provide either a list of Tracking Area Codes (TACs) or Area Codes to the AMF as part of service area restrictions. However, this feature exclusively supports TAC lists provided by the UDM.

If the UDM includes Area Codes in the Service Area Restriction (SAR) data, the AMF doesn't apply any service area restrictions and ignores the SAR data. In cases where the UDM provides TACs, it's expected that these TACs align with the Tracking Area Identity (TAI) list configured within the AMF.

The AMF anticipates the UDM to provide up to 16 TACs, either per area or across multiple areas. However, even if the UDM sends more than 16 TACs for a particular area or across multiple areas, the AMF relays a maximum of 16 TACs (starting from the first area) in NGAP/NAS messages.

AMF supports service area list types 00,01, and 11.

If the initial two TACs in an area are consecutive in sequence in the SAR IE, then AMF assumes that all TACs in that specific area are in consecutive sequence, and uses TYPE 01 service area list.

When the UDM specifies the restriction type as "ALLOWED_AREAS" and doesn't specify any areas, it signifies that the UE is allowed in all areas. In such cases, the AMF sets the type-list as 11 in the registration accept message, and in N2 messages, the AMF doesn't fill any service area restrictions. The AMF doesn't incorporate any service area restrictions in this area.

When the UDM specifies the restriction type as "NOT_ALLOWED_AREAS" and doesn't provide any areas, it indicates that the UE is not allowed in any areas. In this case, registration area is filled as not allowed TACs.

If UDM removes the existing service area restrictions through data change notification, The AMF triggers the UE configuration update procedure with service area list type 11 and sends the mobility restrictions IE to Gnb without service area information.

If UDM sends an invalid restriction type during registration, the SAR content is dropped by the AMF.

UDM Data Change Notification

When AMF detects a change in Service Area Restriction (SAR) due to a Data Change Notification from UDM:

- If the UE is in connected mode, AMF triggers a UE Configuration update command to the UE.
- If the UE is in idle mode, AMF triggers paging.

The AMF updates UE context with the SAR information from UDM instantly and it doesn't wait for a response from the UE.

Enforcing Service Area Code Restrictions at AMF

The AMF enforces service area restrictions, if it determines that the UE is in a non-allowed area or is not in an allowed area. The AMF doesn’t enforce any service area restrictions for emergency services. Following are the procedures for enforcing the service area restrictions at AMF.

- Registration procedure
  - During registration procedure, if AMF detects that UE has moved into a non-allowed area, and if UE is requesting to reactivate any non-emergency PDU using the uplink data status IE, then the AMF fills “28 "Restricted service area" as cause in the PDU reactivation result error for the corresponding PDUs in registration accept.
  - During registration procedure with UE being in connected mode, For example - Mobility registration post handover, if AMF detects UE has moved into a restricted service area, and if PDU session status IE indicates presence of any non-emergency PDUs , the AMF initiates the release of the PDU by sending SM update context with release IE set as true towards SMF.

- Service Request procedure
  - During service request, if the service type IE in the service request message is set to "signaling" or "data", then the AMF sends a service reject message with the 5GMM cause value set to #28 "Restricted service area";

Note #28 "Restricted service area" is default cause value. If any specific cause is configured under local cause code mapping CLI, the same cause code is used.

  - If service type is "mobile terminated services", and service request contains uplink data IE indicating non-emergency PDUs to be reactivated, the AMF fills “28 "Restricted service area" as cause in the PDU reactivation result error.

- Handover procedure
  - In case of handovers like Xn, and N2 , if applicable, the AMF enforces the restrictions when mobility registration is received as part of the handover procedure.
  - In case of scenarios involving AMF change like registration, N2 handovers:
    - If service area restrictions are available in the source AMF (S-AMF), the S-AMF forwards them to the target AMF (T-AMF).
    - In case of N2 handover, T-AMF forwards the service area restriction received from the S-AMF's handover request to the target gNB.
    - T-AMF retrieves subscription data from the UDM as part of registration procedure. The SAR information received from the UDM supersedes the SAR details sent by the S-AMF and the same is updated to UE and gNB Accordingly.
  - In case of N26 idle mode 4g to 5g HO:
    - AMF doesn't consider the PDU session status IE for any PDU synchronization.
    - If the UE is in a restricted area, the AMF refrains from sending the CreateSMContext to the SMF.
    - PDU creation and reactivation occur simultaneously, AMF doesn't populate the reactivation result or error cause, but it always fills the PDU session status IE in registration accept.

- While UE is in restricted area, upon receiving uplink 5G-SM message from UE which is not forwarded due to service area restrictions; the AMF sends back the 5GSM message to the UE with cause code as #28 "Restricted service area".
- The AMF rejects the N1N2 messages with a message class of SM from the SMF for non-emergency PDN when it is in a restricted service area.
- When UE is in idle mode, and if UE is in non-allowed area, the AMF pages the UE only for emergency services, MT SMS, and for other mobility related messages.

Note The AMF detects whether the UE is in allowed or non-allowed area based on the last known location. On the basis of this information, the AMF decides whether to proceed with paging or not.

- In case of UDM data change notification received when UE is in connected mode, the AMF triggers the UE configuration update procedure immediately towards UE. The restrictions are enforced only when mobility registration request is sent by UE.

Configuring Local Cause Code Mapping for Service Area

This configuration supports the mapping of local-defined cause code to restricted area restrictions. To configure the local cause code mapping for the service area, following is an example configuration:

```
config
   local-cause-code-map local-cause-code-map_name
      restricted-zone-code cause-code-5gmm
      possible completions [no-suitable-cells-in-tracking-area |
5GS-services-not-allowed | no-suitable-cells-in-tracking-area |
plmn-not-allowed | restricted-service-area |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed ]
      end
```

If a local cause code is configured for service area restriction (SAR), the AMF uses the configured cause code from the CLI. Otherwise, the default cause code #28 "Restricted service area" is used.

Note The AMF uses the mapped cause code CLI only while sending the service reject messages.

Show Subscriber to indicate UE in Serving Area

When there is no Service Area Restriction (SAR) information available from the UDM, the AMF designates the "In Serving Area" status as "Unknown Area." On the other hand, if the UDM provides valid SAR data, the AMF assesses the UE's location by comparing its Tracking Area Code (TAC) with the UDM's response SAR. Based on this comparison, the AMF determines the UE's state as either allowed or not allowed in the given area. Following is the example of the output.

```
show subscriber supi xyz

"InServingArea": "ALLOWED"

"serviceAreaRestriction": {
"restrictionType": "ALLOWED_AREAS",
"areas": [
{
"tacs": [
"1e",
"14"
]
},
{
"tacs": [
```

```
"0a",
"ABCD"
]
},
{
"tacs": [
"FFFE",
"FFFF"
]
}
]
}
```

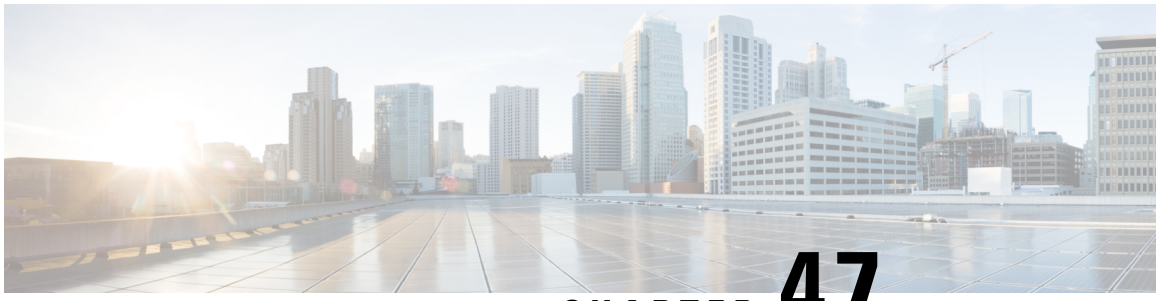
Here are the possible outcomes:

- If the UE's TAC is not allowed - "In Serving Area": "NOT_ALLOWED"
- If the UE's TAC is allowed - "In Serving Area": "ALLOWED"
- If the AMF is unable to evaluate the service area restriction from the UDM's response - "In Serving Area": "UNKNOWN_AREA"

Limitations

This feature has the following limitations:

- The AMF doesn't support the area code received as a part of service area restrictions from the UDM.
- The AMF doesn't support the implementation of Policy Control Function (PCF) interaction for Service Area Restriction (SAR) information.
- The AMF doesn't support the event exposure services for service area restriction changes notification to other NF.



CHAPTER 47

Service Request Procedure

Feature Summary and Revision History

Summary Data

Table 163: 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 164: 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

The following is the known limitation of this feature.

- 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 66: Idle Mode Call Flow

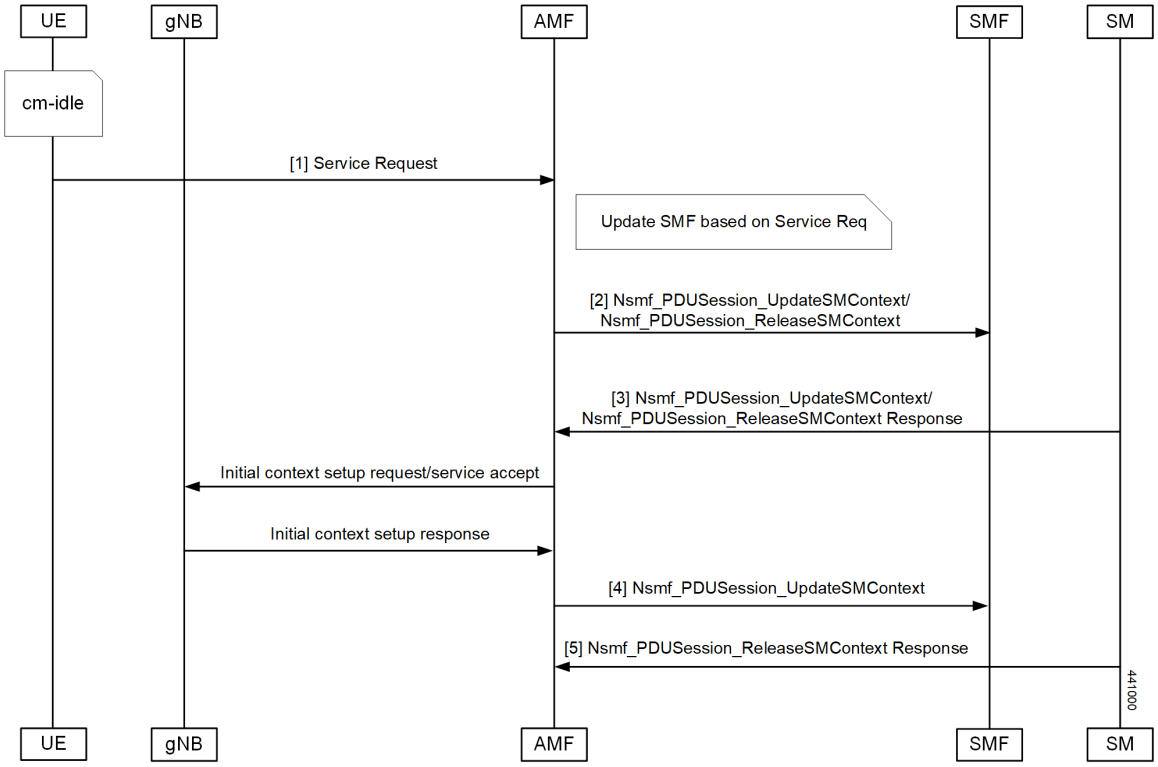


Table 165: Idle Mode Call Flow Description

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 67: Connected Mode Call Flow

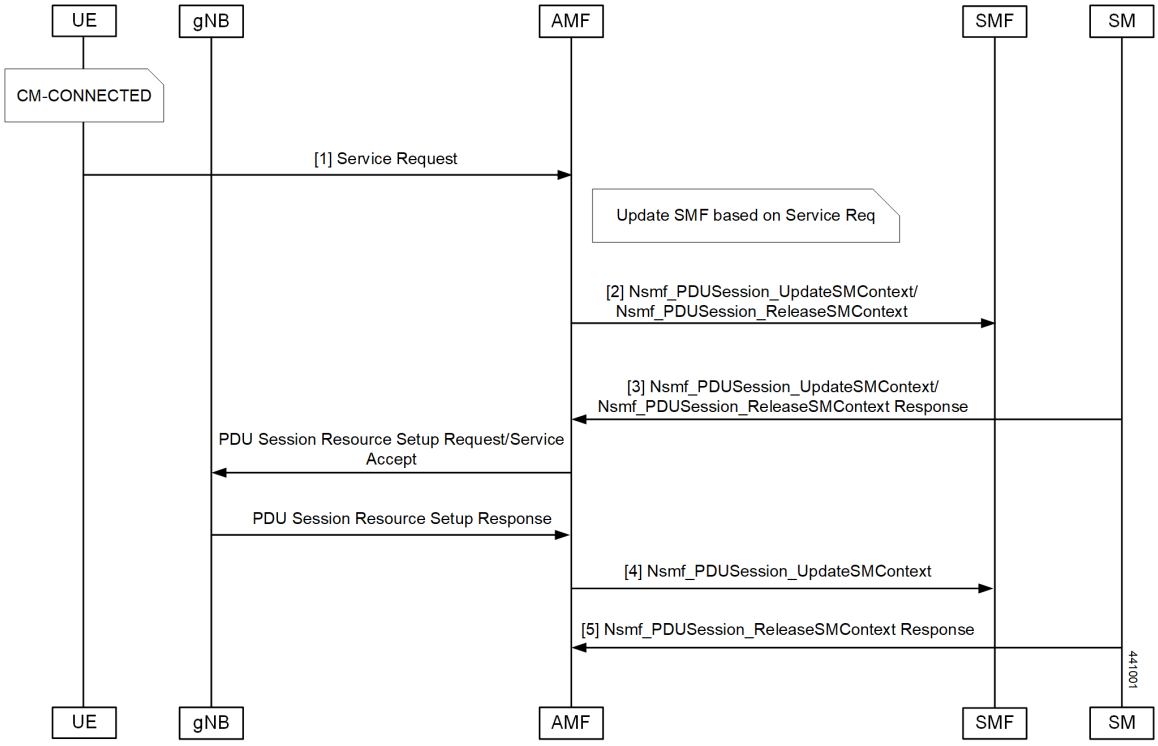


Table 166: Connected Mode Call Flow Description

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

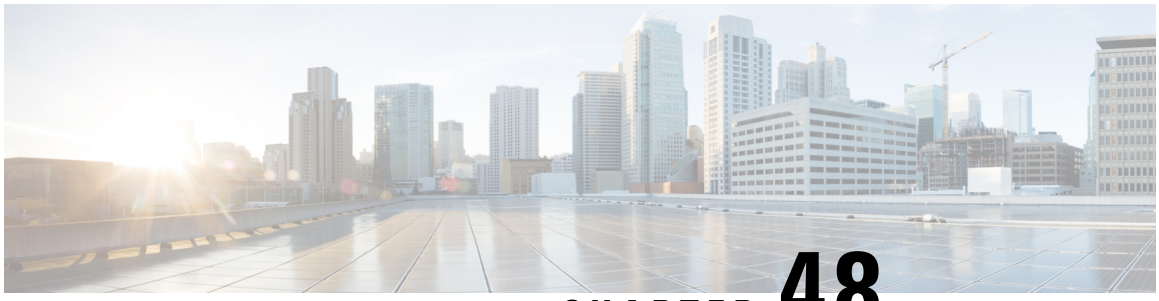
This section describes operations, administration, and maintenance information for this feature.

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 48

Session Timers

Feature Summary and Revision History

Summary Data

Table 167: 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 168: Revision History

Revision Details	Release
The following enhancement was introduced: • Timer T3346	2022.04.0
The following enhancements were introduced: • Non-3GPP timer configurations	2022.01.0
First introduced.	2021.04.0

Feature Description

AMF supports the following timers:

- **T3346** (t3346): It operates in NAS-CONGESTION state. AMF uses this timer value to encode t3346 IE in Registration / Service reject, and to encode back-off timer IE for rejection of session management message.
- **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** (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
- **UE Context Transfer** (context-transfer-guard): AMF uses this timer to keep the individual UE Context resources until the timer expires. AMF starts this timer when UeRegStatusUpdateReqData message contains transferStatus as TRANSFERRED. Upon expiry, it clears the PDUs locally.
- **Tidle** (tidle): When the UE moves to the CONNECTED state, tidle timer is started and it's reset when any signalling occurs for the subscriber.

  On expiry of tidle timer, AMF checks:
  - If the UE Configuration Update is enabled and if new configuration is available to send to the UE, AMF triggers the UE Config Update Command to UE and resets the tidle timer.

  - If the UE Configuration Update isn't enabled or there's no configuration update to send the to UE, the UE is moved to the IDLE state. AMF triggers the Context Release Command towards the gNB and the SM Context Update towards the SMF accordingly.

- **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.
- **Tn2** (tn2): It functions in AMF-initiated N2 messages, specifically for the AMF that waits for the response.
- **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.
- **Procedural Timeout** (proc-timeout): It starts when AMF receives Registration Request. After expiry, AMF sends the Registration Reject message to the UE.

For information on the timer configurations, refer to Feature Configuration, on page 394.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for the AMF timers.

T3346 Call Flow

This section describes the T3346 call flow.

Figure 68: T3346 Timer Call Flow

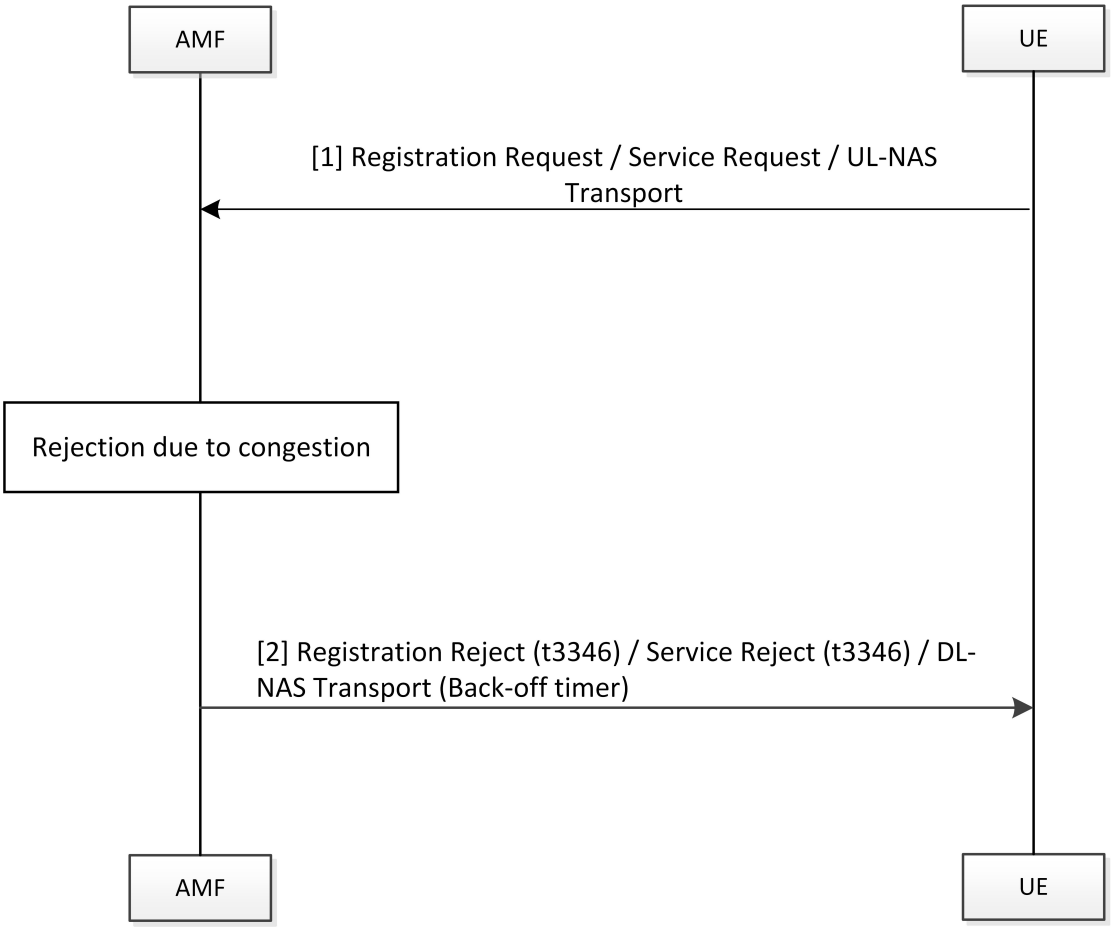


Table 169: T3346 Timer Call Flow Description

Step	Description
1	The UE sends registration request/service request.
2	With AMF in congestion state: • For registration request, AMF rejects the message with cause as congestion and includes t3346 timer. • For UL-NAS transport (Payload container type: N1 SM information), AMF sends DL-NAS message with cause as congestion and includes back-off timer.

T3502 Call Flow

This section describes the T3502 timer call flow.

Figure 69: T3502 Timer Call Flow

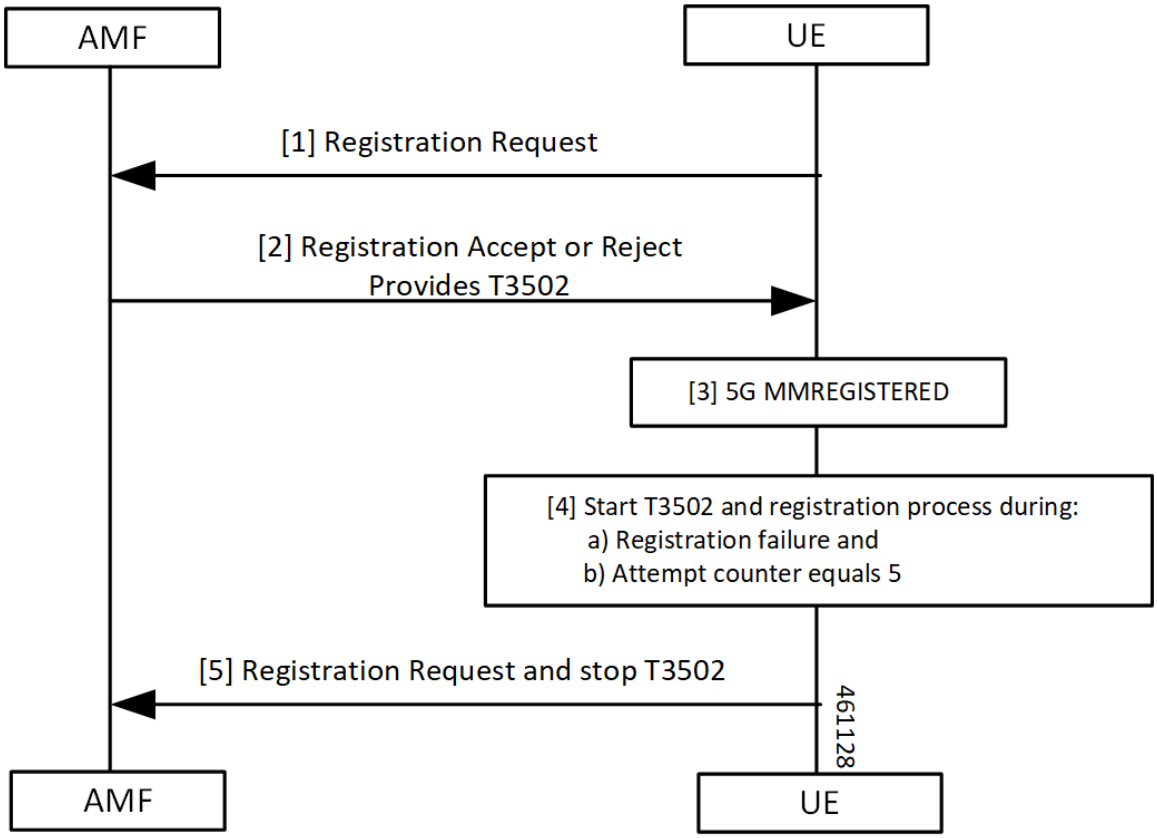


Table 170: T3502 Timer Call Flow Description

Step	Description
1	The UE sends the Registration Request to the AMF. The UE starts the T3502 timer.
2	The UE receives a response of reject or accept from the AMF.
3	The UE performs the 5G MM registration procedure.
4	The UE starts the T3502 timer and the registration process during one of the following: • Registration failure • Attempt counter equals 5
5	The UE sends the Registration Request to the AMF and stops the T3502 timer.

T3512 Call Flow

This section describes the T3512 timer call flow.

Figure 70: T3512 Timer Call Flow

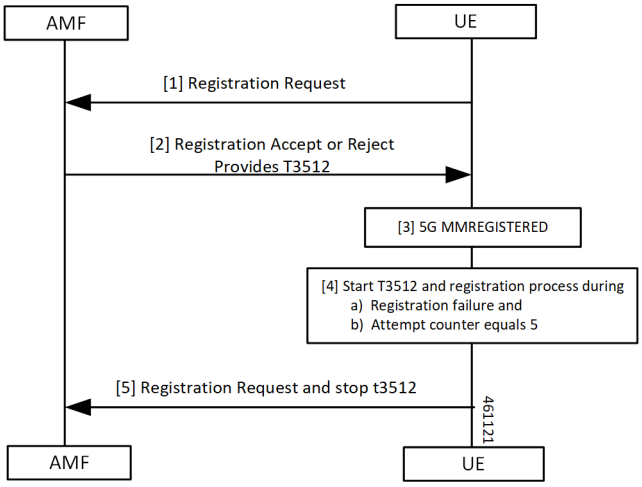


Table 171: T3512 Timer Call Flow Description

Step	Description
1	The UE sends the Registration Request to the AMF.
2	The UE receives a response of reject or accept from the AMF. The UE starts the T3512 timer.
3	The UE performs the 5G MM Registration procedure.
4	The UE starts the T3512 timer and the registration process during one of the following: • Registration failure • Attempt counter equals 5
5	The UE sends the Registration Request to the AMF and stops the T3512 timer.

T3522 Call Flow

This section describes the T3522 timer call flow.

Figure 71: T3522 Timer Call Flow

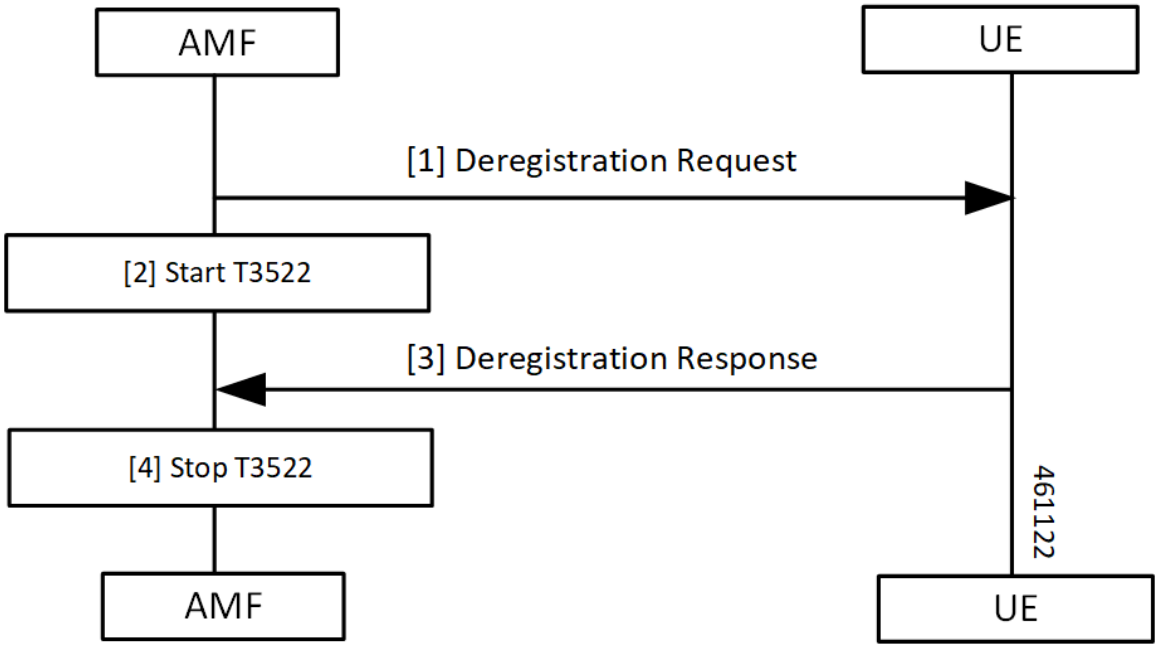


Table 172: T3522 Timer Call Flow Description

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 72: T3550 Timer Call Flow

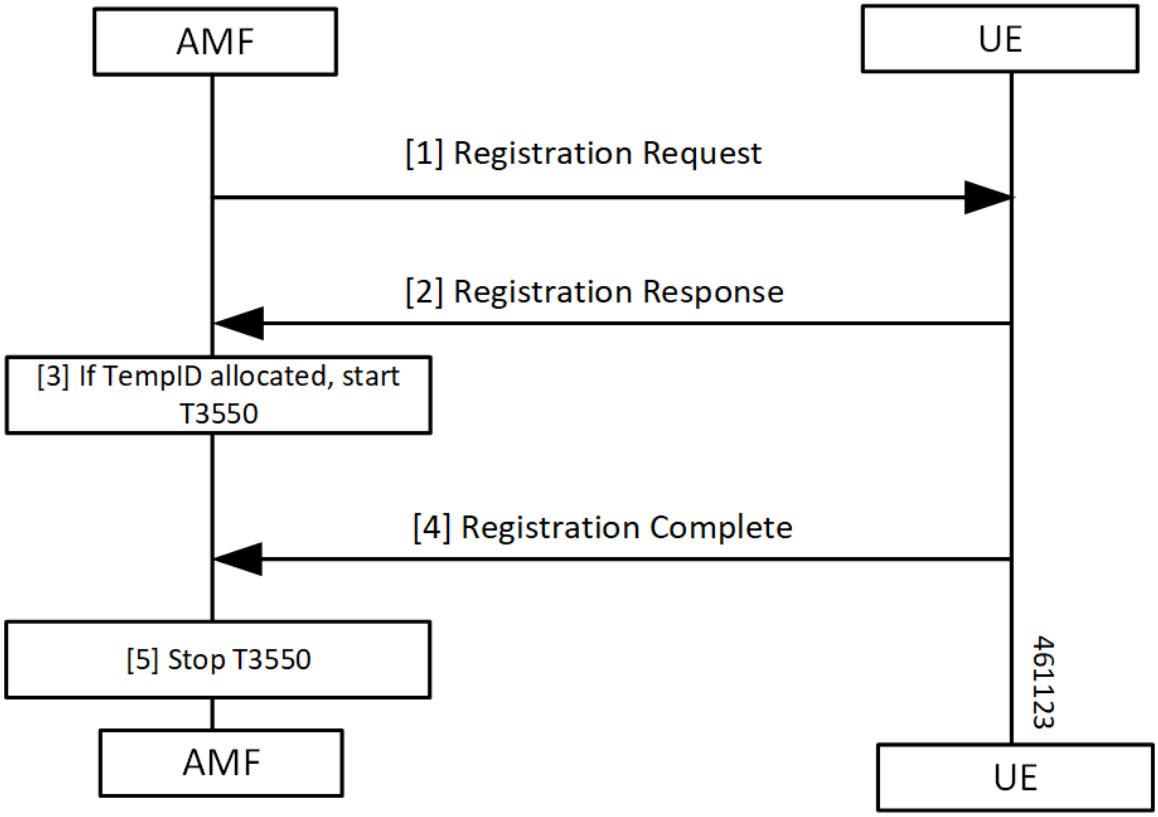


Table 173: T3550 Timer Call Flow Description

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 73: T3555 Timer Call Flow

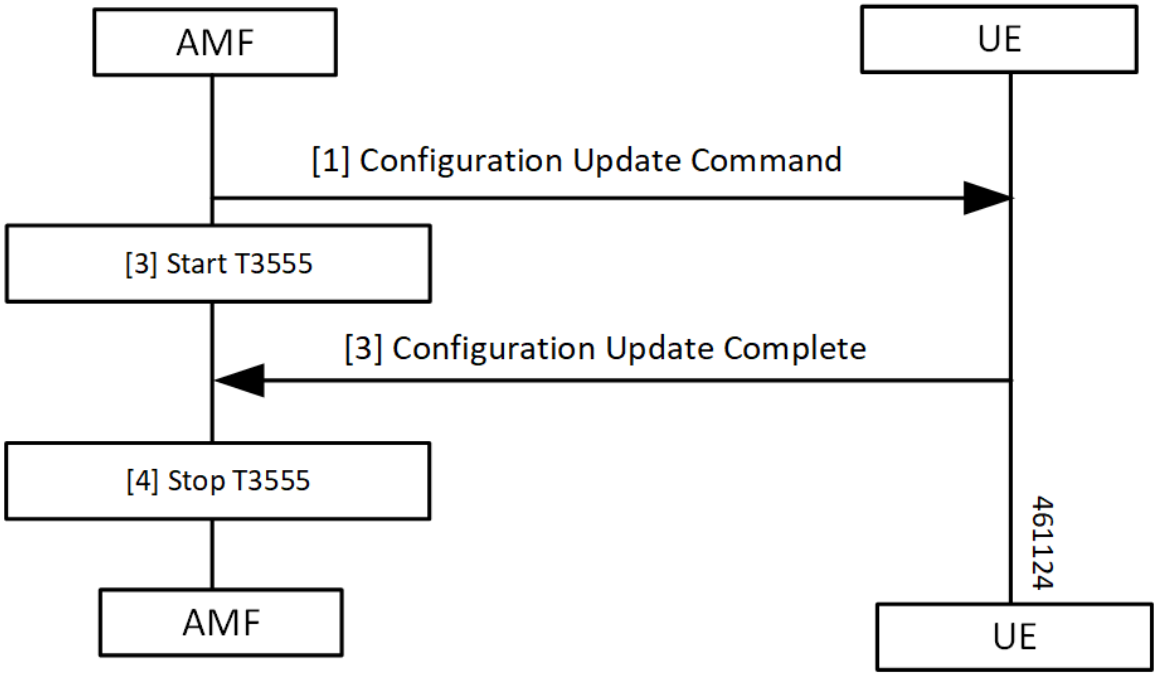


Table 174: T3555 Timer Call Flow Description

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 74: T3560 Call Flow

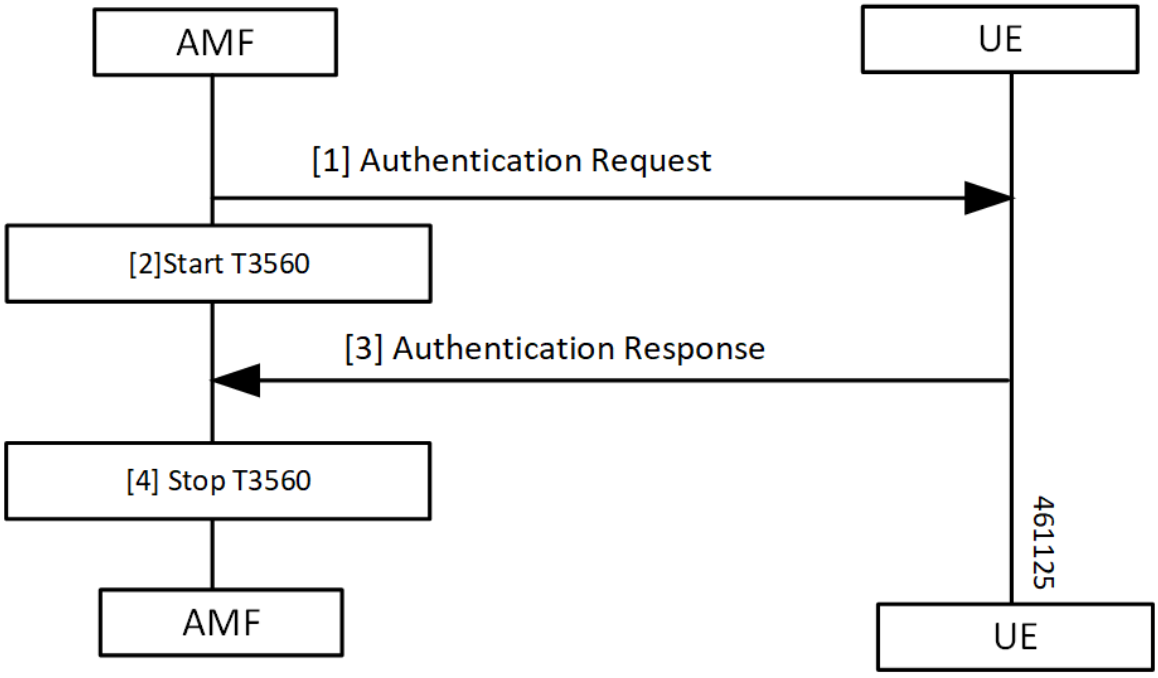


Table 175: T3560 Timer Call Flow Description

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 75: T3570 Call Flow

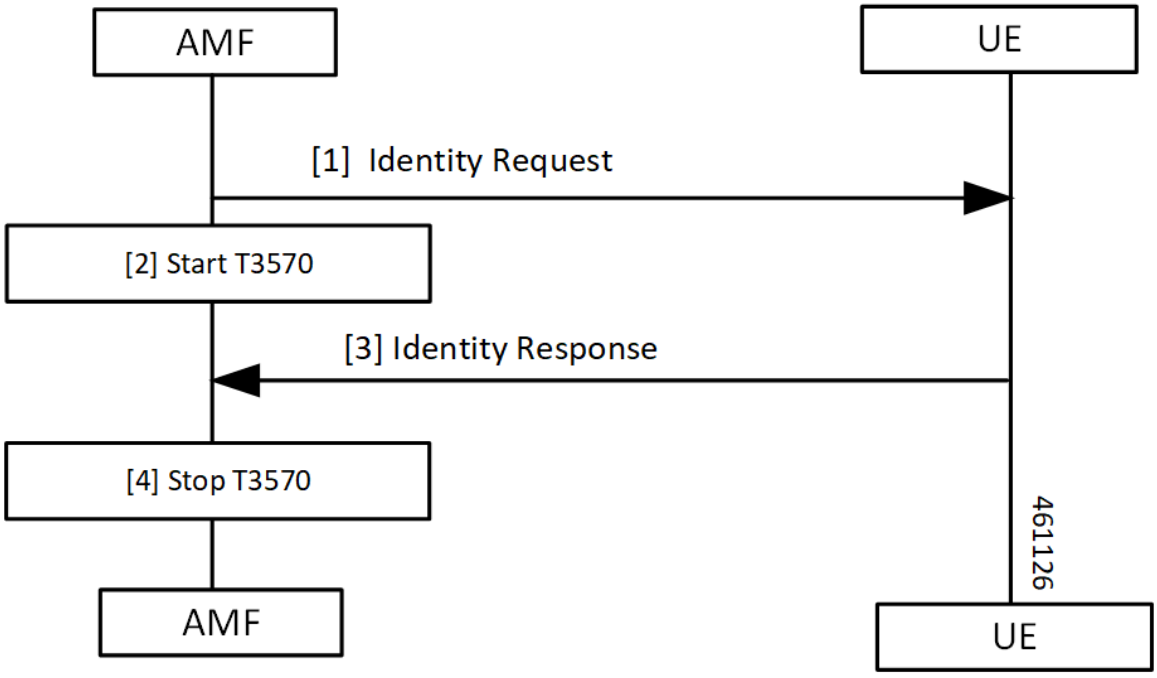


Table 176: T3570 Timer Call Flow Description

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.

Tidle Timer Call Flow

This section describes the Tidle timer call flow.

Tidle timer call flow is a sample call flow. Tidle timer expiry can happen post various signalling procedures, not just registration procedure.

Figure 76: Tidle Timer Call Flow

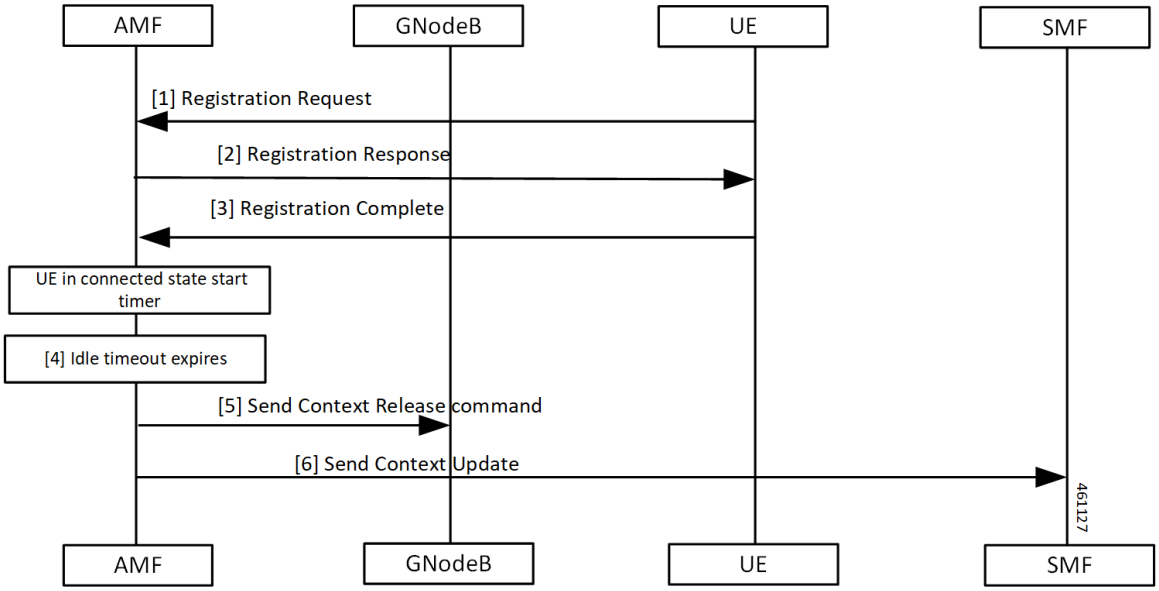


Table 177: Tidle Timer Call Flow Description

Step	Description
1	The UE sends the Registration Request to the AMF
2	The UE receives Registration Response from the AMF.
3	The UE sends the Registration Complete to the AMF. When UE moves to CONNECTED state, the AMF starts the configured timer. The value ranges between 30 seconds to seven hours.
4	The AMF waits for the Tidle timer expiry.
5	The AMF sends the Context Release Command to the gNodeB.
6	The AMF sends the Context Update to the SMF.

Procedural Timer Call Flow

This section describes the procedural timer call flow.

Figure 77: Procedural Timer Call Flow

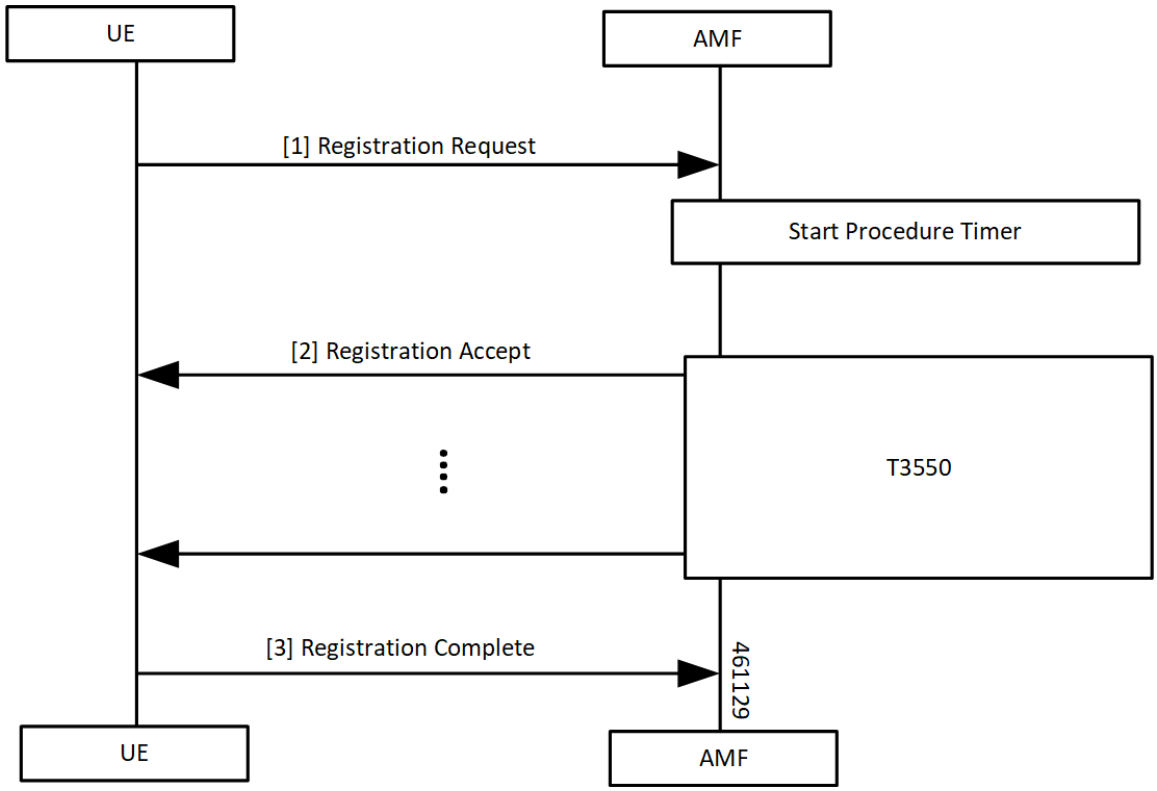


Table 178: Procedural Timer Call Flow Description

Step	Description
1	The AMF starts the Procedure timer upon receiving Registration Request per UE basis.
2	AMF starts the T3550 timer when it sends the Registration Accept to UE and stops after receiving the Registration Complete. When the timer expires before sending Registration Accept towards the UE, the following actions takes place: • Clear context locally, on UDM and PCF. • Registration Reject procedure. When Registration Accept to the UE is successful, AMF updates t3550 (retry and timeout) based on remaining time and retry count.
3	The UE sends Registration Complete to the AMF.

Standards Compliance

This feature complies with the following standards specification:

- *3GPP TS 24.501 " Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"*

Feature Configuration

Configuring this feature involves the following steps:

- 3GPP timer configurations—These commands support in configuring 3GPP timers. For more information, refer to Configuring the 3GPP Timers, on page 394.
- Non-3GPP timer configurations—These commands support in configuring non-3GPP timers. For more information, refer to Configuring the Non-3GPP Timers, on page 396.

Configuring the 3GPP Timers

To configure the GPP timers, 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 179: 3GPP Timers and Values

Timer	Retry Count or Attempt 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.
tpurge	Not Applicable	Must be an integer in the range of 0–35712000 seconds. The default value is 86400.

Timer	Retry Count or Attempt Count	Timeout Value
t3346	Not Applicable	Must be an integer in the range of 1–11160 seconds. The default value is 900 seconds. While processing the t3346 timer towards UE, AMF adds a random offset to the configured timer value. This random offset is based on the configured timer value. If timer value is: • Greater than or equal to 0 seconds, random offset is in the range of 0–30 seconds. • Greater than 62 seconds, random offset is in the range of 0–300 seconds. • Greater than 1860 seconds, random offset is in the range of 0–1000 seconds. Maximum value of the recomputed timer value is 11160 seconds.
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	This parameter defines the number of paging attempts. 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	This parameter defines the number of paging retries. 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	This parameter defines the number of paging retries. 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.

Timer	Retry Count or Attempt Count	Timeout Value
t3555	This parameter defines the number of paging retries. 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	This parameter defines the number of paging retries. 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	This parameter defines the number of paging retries. 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.

To configure the t3513 timer, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         timers t3513  { attempts paging_attemps_count | value timeout_value }
         end
```

NOTES:

- **timers t3513 attempts** *paging_attemps_count*—Specify the number of paging attempts.
- **timers t3513 value** *timeout_value*—Specify the t3513 timeout value.

  For the t3513 timer configuration values, refer to the *3GPP Timers and Values* table.

Configuring the Non-3GPP Timers

To configure the Non-3GPP timers, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         timers timer_type value timer_value
         end
```

NOTES:

- **timers** *timer_type* **value** *timer_value*—Specify the timeout value.

  For the timer_type, refer to the following table.

Table 180: Non-3GPP Timers and Values

Timer	Timeout Value
context-transfer-guard	Must be an integer in the range of 0–35712000 seconds. The default value is zero seconds.
proc-timeout ue-registration	Must be an integer in the range of 10–120 seconds.
tidle	Must be an integer in the range of 30–25200 seconds.
tn2	Must be an integer in the range of 0–35712000 seconds. The default value is six seconds.

Configuring the IDLE Timer

To configure the IDLE timer, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         timers tidle value timeout_value
         end
```

NOTES:

- **timers tidle value** *timeout_value*—Specify the IDLE timeout value in seconds.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy local
         timers tidle 2
         end
```

Configuring the Procedural Timer

To configure the Procedural timer for AMF, use the following configuration:

```
config
   amf-global
      timers proc-timeout ue-registration value timeout_value
      end
```

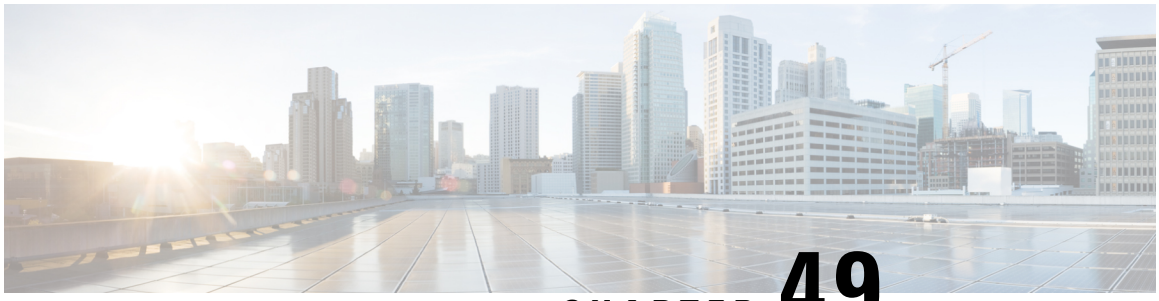
NOTES:

- **timers procedure-timeout ue-registration value** *timeout_value*—Specify the UE Registration procedure timeout value in seconds. Must be an integer in the range of 10-120 seconds.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy local
         timers proc-timeout pdu-create value 20
         end
```



CHAPTER 49

SMF Feature Updates without SMF IEs

Feature Summary and Revision History

Summary Data

Table 181: 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 182: 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
```

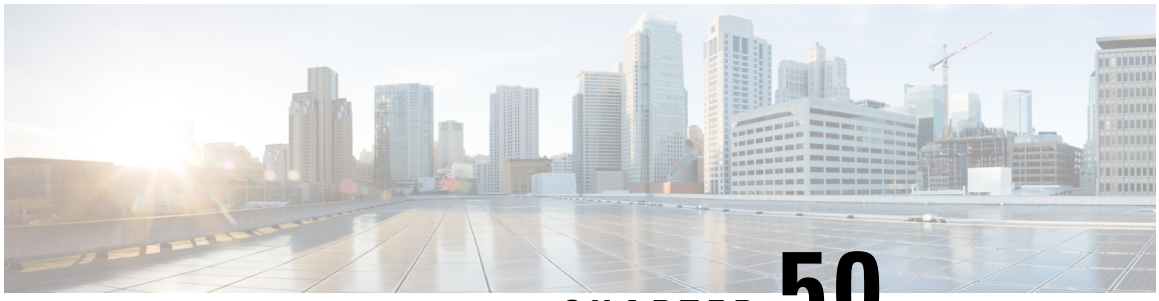
NOTES:

- **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 50

SMS over the Non-Access Stratum Procedures

Feature Summary and Revision History

Summary Data

Table 183: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	

Revision History

Table 184: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

In 5G, the AMF sends and receives the SMS payloads from the UE over the NAS messages. The AMF and SMSF entities within the 5G core provide and utilize services provided by each other to enable the delivery of SMS over Non-Access Stratum (NAS).

For more information, refer to the UCC 5G AMF Configuration and Administration Guide > SMS over the Non-Access Stratum Procedures chapter.

How it Works

This section describes how this feature works.

The SMS over NAS feature supports the following procedures:

- **Registration procedures for SMS over NAS**—This procedure involves the following steps:
  - During registration, if the UE requests for SMS support and the feature are enabled at AMF, the AMF fetches the SMS subscription data and UE context in the SMSF data along with the AM and SMF selection data. The AMF also subscribes to the UDM notifications.
  - If the UE has the SMS subscriptions enabled, the AMF sends the Activate Request to the SMSF.
  - The AMF supports the target PLMN and instance ID-based SMSF selection based on the NRF discovery. The instance ID received from the UDM is preferred over the instance ID received from the peer AMF.

    Depending on these steps, the AMF notifies the SMS status as allowed or not allowed to the UE as part of the Registration Accept message.

- **Deregistration procedures for SMS over NAS**—The AMF triggers the SMS Deactivation Request towards SMSF during the following scenarios:
  - UE-initiated deregistration
  - Network-initiated deregistration
  - The SMS was activated in the previous Registration Requests and the UE did not request for the SMS support in the subsequent Registration Request.
  - Whenever the SMS state at AMF changes from allowed to not allowed, and if the SMS was previously activated, the AMF sends the Deactivation Request to SMSF.

- **MO SMS over NAS in CM-IDLE or CM-CONNECTED**
- **MT SMS over NAS in CM-IDLE or CM-CONNECTED state through 3GPP access**—This procedure involves the following steps:
  - As part of MT SMS, the AMF supports handling of the EnableReachability Requests from the SMSF.
  - If the UE is in the CONNECTED state, the AMF immediately responds with the UE as REACHABLE.
  - If the UE is in the IDLE state and the PPF flag is set, the AMF triggers the paging procedure and updates the SMSF based on the paging response.

Notifications using the UE Configuration Update Command

The UE Configuration Update Command is responsible for communicating the modification in the SMS state to the UE. The SMS state, such as allowed and not allowed is modified when the AMF CLI is modified or the AMF receives the subscription change notification through the UDM data change notification.

When the AMF detects changes in the SMS state for a UE, and the UE requested in the previously sent Registration Request for the SMS, the AMF notifies the new SMS state through the UE Configuration Update Command.

If the UE had requested the SMS based on CLI configuration or SMS subscription, the AMF marks the SMS as allowed or not allowed and informs the UE through the Registration Accept message. Later, when the SMS state changes at AMF; for example, the UDM subscriptions change the SMS state from allowed to not allowed. In that case, the UE Configuration Update Command notifies the UE with the SMS IE indication as not allowed.

For the UDM notifications, when the UE is in the CONNECTED state, the UE Configuration Update Command is triggered instantly. However, paging is triggered based on the AMF configuration if the UE is in the IDLE state.

Whenever the SMS state at AMF changes from allowed to not allowed, and if the SMS was previously activated, the AMF sends the Deactivation Request to SMSF.

Paging

The AMF starts a paging procedure when the SMSF sends the UE Reachability event for the MT SMS, and the UE is in the IDLE state. The AMF determines the paging profile specific to the SMS based on the configured trigger type. AMF uses the default paging profile when the paging profile is not configured.

When AMF receives the UDM notification containing the new data, and the UE is in the IDLE state, the AMF pages the UE to send the UE configuration update.

Failure Handling

The AMF has implemented strategies to handle the following failure scenarios:

- When the SMSF activation process fails, the AMF sets the SMS Allowed value to false in the Registration Accept message.
- If the failure is observed during the deactivation or when sending uplink SMS, the AMF does not perform any action.
- When the SMSF is deactivated, the AMF marks the SMS state as not allowed irrespective of the deactivation result from SMSF.
- On the incoming response messages, the AMF does not perform any validations, such as when the mandatory IE missing.

Note The failure handling profile configuration determines the retry and retransmission of messages. For the SMSF failures, the AMF supports only retry and ignore as the failure actions.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.501 "System architecture for the 5G System (5GS)"*
- *3GPP TS 23. 502 "Procedures for the 5G System (5GS)"*
- *3GPP TS 24.501 "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"*
- *3GPP TS 29.503 "5G System; Unified Data Management Services; Stage 3"*
- *3GPP TS 29.518 "5G System; Access and Mobility Management Services; Stage 3"*
- *3GPP TS 29.540 "5G System; SMS Services; Stage 3"*

Limitations

This feature has the following limitations in this release:

When the SMS over NAS CLI is enabled, the AMF always fetches the SMS subscriptions data from UDM along with AM and SMF selection data. If the feature CLI is not enabled during initial registration, the SMS subscription data is not fetched for the UE. Later, when the UE requests for the SMS support in the subsequent Periodic or Mobility Registration message, AMF does not have the SMS subscription data, and the SMS is not activated.

Feature Configuration

Configuring this feature involves the following steps:

- Configure AMF to support the SMS messaging over NAS. For more information, refer to Configuring AMF to send SMS over NAS, on page 405.
- Configure AMF to perform SMSF selection based on data from the NRF-based discovery. For more information, refer to Configuring NRF Discovery for SMSF, on page 405.
- Configure AMF to follow appropriate failure handling techniques. For more information, refer to Configuring Failure Handling, on page 406.
- Configure AMF to initiate paging when the SMSF sends an Enable UE Reachability message for MT SMS and if the UE is in the IDLE state. For more information, refer to Configuring the Paging Profile, on page 407.
- Configure the AMF to page the UE when it sends a UE Configuration Update message. The AMF sends this update message on receiving a UDM notification that contains the new data and if the UE is in the IDLE state. For more information, refer to Configuring Paging for the UDM Notifications, on page 407.
- Configure the time zones parameters for the Tai-group or Tai-list. When configured, the AMF uses this time zone information in the ueTimeZone IE messages sent to SMSF. For more information, refer to Configuring the Time Zone, on page 407.

Configuring AMF to send SMS over NAS

To enable the transfer of SMS over NAS, use the following configuration:

```
config
  amf-global
    call-control-policy policy_name
      policy sms-over-nas { true | false }
      end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the Call Control Policy name.
- **policy sms-over-nas { true | false }**—Configure the capability that is responsible to send the SMS over the NAS protocol.

Configuring NRF Discovery for SMSF

To configure the NRF discovery, use the following configuration:

```
config
   amf-global
      operator-policy policy_name
         ccp-name ccp_name
         network-element-profile-list [ smsf ]
         end
   profile
      network-element [ smsf ]
         nf-client-profile nf_profile_name
         failure-handling-profile failure_handling_profile_name
         query-params [ target-plmn | instance-id ]
         end
      nf-client nf-type [ smsf ]
         smsf-profile smsf_profile_name
            locality locality
            priority profile_priority
            service name type [ nsmsf-sms ]
               endpoint-profile endpoint_profile_name
                  capacity profile_capacity
                  priority endpoint_priority
                  uri-scheme [ http ]
                  version
                     uri-version version
                  endpoint-name endpoint_name
                     priority endpoint_priority
                     primary ip-address primary_ip_address
                     primary ip-address port primary_port_numer
                     secondary ip-address secondary_ip_address
                     secondary ip-address port secondary_port_numer
                     end
      nf-pair nf-type [ smsf ]
```

```
nrf-discovery-group
   locality
      client client_locality
      preferred-server server_name
      geo-server geo_server_name
      end
```

NOTES:

- **operator-policy** *policy_name*—Specify the operator policy name.
- **ccp-name** *ccp_name*—Specify and configure the Call Control Policy name.
- **capacity** *profile_capacity*—Specify the endpoint profile capacity.
- **nrf-discovery-group**—Specify the NRF discovery group name.
- **priority** *endpoint_priority*—Specify the node priority for endpoint.
- **client** *client_locality*—Specify the client locality information.
- **preferred-server** *server_name*—Specify the Geo service locality information.
- **geo-server** *geo_server_name*—Specify the preferred server locality information.

Configuring Failure Handling

To configure the failure handling profile, use the following configuration:

```
config
   profile
      nf-client-failure nf-type [ smsf ]
         profile failure-handling profile_name
            service
              name type [ nsmsf-sms ]
              responsetimeout timeout_interval
              message type
                 SmsfActivationReq { status-code [ httpv2 ] | action [
retry-and-ignore ] | retry retry_count }
                 SmsfDeactivationReq { status-code [ httpv2 ] | action [
 retry-and-ignore ] | retransmit  retransmit_count | retransmit-interval
retransmit_interval }
                 SmsfSendSms { status-code [ httpv2 ] | action [
retry-and-ignore ] | retransmit  retransmit_count | retransmit-interval
retransmit_interval }
                 end
```

NOTES:

- **failure-handling-profile** *failure_handling_profile_name*—Specify the failure handling profile.
- **responsetimeout** *timeout_interval*—Specify the timeout interval in milliseconds. The default value is 2000.
- **range** *range*—Specify the range value. Must be an integer in the range of 0–599.

- **retransmit** *retransmit_count*—Specify the retransmit interval in milliseconds.

Configuring the Paging Profile

To configure the paging profile, use the following configuration:

```
config
  amf-global
   paging-map paging_map_name
    precedence paging_precedence
    paging-profile-name paging_profile_name
    trigger-type [ sms ]
    end
```

NOTES:

- **paging-map** *paging_map_name*—Specify the paging map name. Must be string in the range of 1–64.
- **precedence** *paging_precedence*—Specify the precedence level. Must be an integer in the range of 1–255 with 1 indicating the highest and 255 the lowest.
- **paging-profile-name** *paging_profile_name*—Specify the paging profile name. Must be a character string in the range of 1–64.
- **trigger-type [sms]**—Specify the type of paging trigger.

Configuring Paging for the UDM Notifications

To configure the paging feature, use the following configuration:

```
config
   amf-global
      call-control-policy ccp_name
       policy idle-mode udm-notification initiate-paging [ SMS ]
       end
```

NOTES:

- **policy idle-mode** —Configure the UE configuration for the idle mode paging parameters.
- **udm-notification initiate-paging [SMS]** —Configure the paging for the UDM notification.
- By default, the paging feature is disable for the UDM notifications.

Configuring the Time Zone

To configure this feature, use the following configuration:

```
config
  tai-group name { name tai_group_name | range range }
     timezone { + | - } hours value [ minutes { 0 | 15 | 30 | 45 } |
daylight-savings-time-increment { 0 | 1 | 2 } ]
   tais { name tai_list_name | range range | preference preference }
```

```
     timezone { + | - } hours value [ minutes { 0 | 15 | 30 | 45 } |
daylight-savings-time-increment { 0 | 1 | 2 } ]
     end
```

NOTES:

- To modify or update the time zone entry, use the following configuration:
  1. Configure no time zone using the **no timezone** command.

     For example:

     ```
     amf(config-tai-group-xxx)# no timezone
     ```

  2. Configure the new time zone values.

- The AMF uses the configured time zone in the messages that are sent to the SMSF as part of ueTimeZone IE. When the time zone is configured at both tai-group and tai-list levels, the preference is configured under the tai-list.
- **preference** *preference*—Specify the preference. The time zone configured within the TAI list gets the preference.
- **timezone { + | - } hours value [minutes { 0 | 15 | 30 | 45 } | daylight-savings-time-increment { 0 | 1 | 2 }]**—Specify the time zone for the TAI list. The variables included the following:
  - **{ + | - }**—Specify the offset direction from the Universal Time (UTC).
  - **hours value**—Specify the offset from UTC in hours. Accepted value must be an integer 0—14.
  - **[minutes { 0 | 15 | 30 | 45 }**—(Optional) Specify the offset minutes that are added to the hours value.
  - **daylight-savings-time-increment { 0 | 1 | 2 }**—Specify the number of hours during which the time zone should be offset due to daylight savings time.

Configuration Example

The following is an example of the time zone configuration.

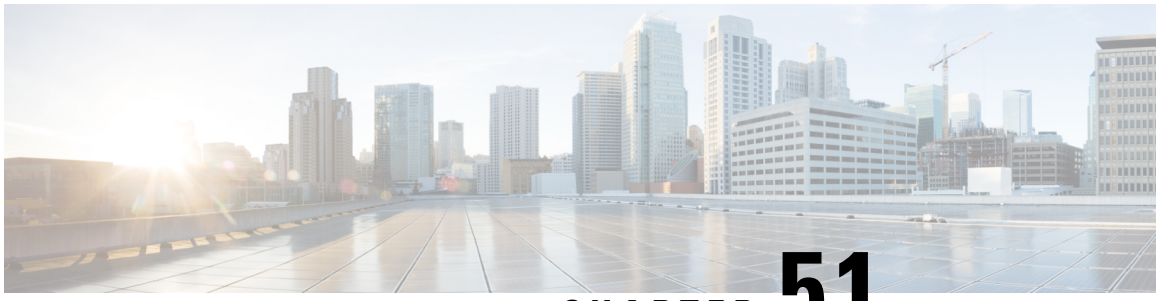
```
config
   tai-group name test1
      timezone offset + hours 11 minutes 45 daylight 2
         tais name tailist2
         timezone offset - hours 14 minutes 45 daylight 1
            mcc 123 mnc 456
            tac list [ 21 22 ]
            exit
            exit
            exit
```

Configuration Example

The following is an example configuration.

```
config
   amf-global
      operator-policy local
      ccp-name local
```

```
   network-element-profile-list smsf smsf1
   end
profile
   network-element [ smsf ]
      nf-client-profile SMSF1
      failure-handling-profile FH1
      query-params [ target-plmn instance-id ]
      end
   nf-client nf-type smsf
      smsf-profile SMSF1
         locality LOC1
         priority 56
         service name type nsmsf-sms
            endpoint-profile EP1
               capacity   30
               priority   30
               uri-scheme http
               version
                  uri-version v2
                  end
               endpoint-name EP1
                  priority 30
                  primary ip-address ipv4 209.165.201.1
                  primary ip-address port 5182
                  seconday ip-address ipv4 209.165.201.2
                  seconday ip-address port 5084
                  end
   nf-pair nf-type SMSF
      nrf-discovery-group udmdiscovery
         locality client  LOC1
         locality preferred-server LOC1
         locality geo-server GEO
         end
```



CHAPTER 51

S-NSSAI based SMF Selection

Feature Summary and Revision History

Summary Data

Table 185: 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 186: 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

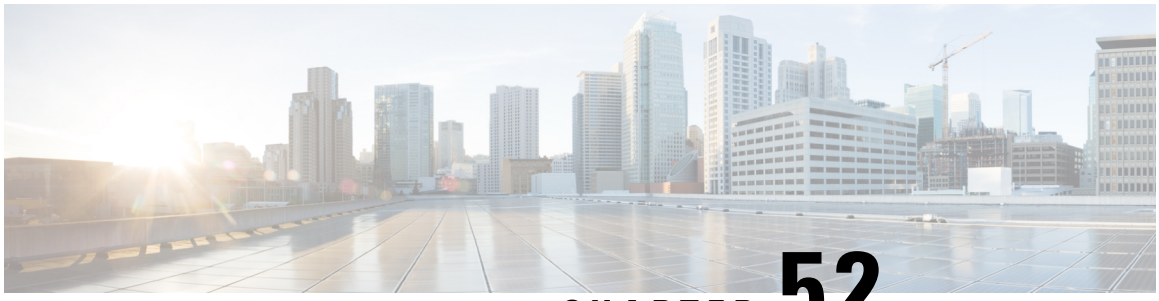
The following is an example configuration.

```
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 52

Steering of Roaming, Roaming Restrictions, and Operator Policy Support

Feature Summary and Revision History

Summary Data

Table 187: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Roaming Support

Revision History

Table 188: Revision History

Revision Details	Release
Added the support for service area restriction.	2023.04.0
First introduced.	2022.02.0

Feature Description

The AMF supports the following functionalities:

- Steering of Roaming, on page 415
- Roaming Restriction and Operator Support, on page 422
- Operator Policy, on page 431

Relationships

The following attributes are associated with this feature:

- Initial, mobility registration, and periodic registration
- PDU establishment
- N26
- N2HO with or without AMF change
- Service request

Note By default, the RAT type is NR and the core network type is 5GC, for an AMF subscriber.

Feature Configuration

Configuring this feature involves the following subfeatures and steps:

- **Local Cause Code to Restricted Area Restrictions**—This configuration supports the mapping of local-defined cause code to Restricted area restrictions. For more information, see Configuring the Core Network Type Restriction, on page 420.
- **Inter-PLMN Roaming**—This configuration supports the commands to configure inter-PLMN restrictions to restrict the roamer subscriber. For more information, see Configuring the 5GC Inter-PLMN Roaming, on page 357.
- **RAT Restriction**—This configuration supports the commands to configure restrictions for RAT types such as EUTRA, NR, Virtual, and WLAN, while accessing the network. For more information, see Configuring the RAT Restriction, on page 429.
- **Local Cause Code to RAT Type Restrictions**—This configuration supports the mapping of local-defined cause code to RAT restrictions. For more information, see Configuring the RAT Type Restriction, on page 429.
- **Operator Policy**—This configuration supports the commands to configure operator-defined policies. For more information, see Feature Configuration, on page 434.

Steering of Roaming

Steering of Roaming (SOR) is a technique where an HPLMN indicates a roaming UE to roam to a preferred roamed-to-network.

How it Works

This section describes how this feature works.

The SOR consists of the following HPLMN protected information:

- An indication of whether the UDM requests an acknowledgment from the UE for a successful SOR reception.
- It supports one of the following:
  - Indication of the included list of preferred PLMN or access technology combinations.
  - A secured packet with an indication, whether it is included or not.
  - The HPLMN indication, when there are no changes in the operator-controlled PLMN selector, with access technology from the stored list in the needed UE.

As a result, no list of the preferred combinations for the PLMN or the access technology is provided.

Note The secured packet contains the list of preferred PLMN and access technology combinations. These combinations are encapsulated within a security mechanism as described in *3GPP TS 31.115 [67]*.

For more on SOR protected information, see *3GPP TS 33.501 [66]*.

Call Flows

This section describes the key call flows for this feature.

SOR During the UE Registration Call Flow

This section describes the SOR during the UE Registration call flow.

Figure 78: SOR During the UE Registration Call Flow

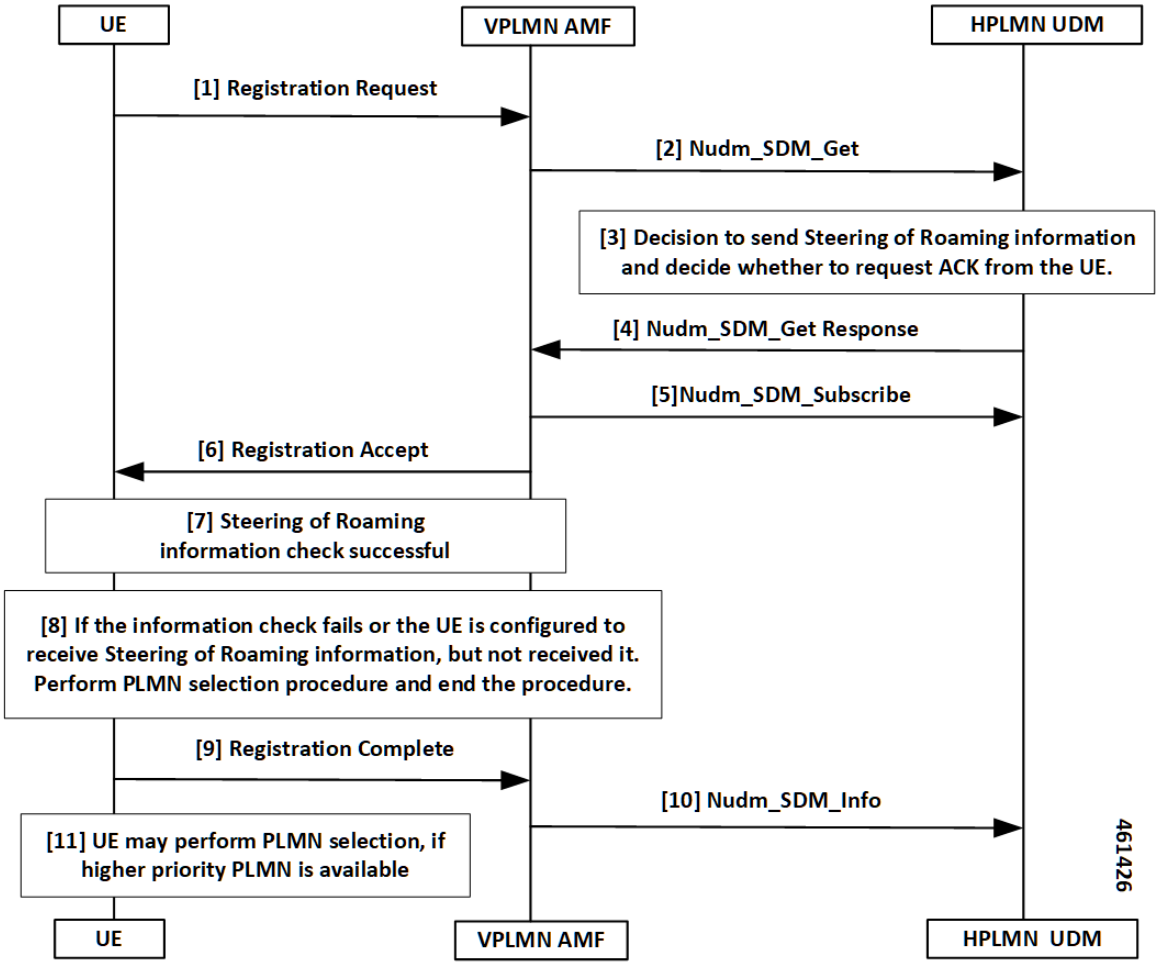


Table 189: SOR During the UE Registration Call Flow Description

Step	Description
1	UE sends the Registration Request to the VPLMN AMF.
2	The VPLMN AMF executes the registration procedure as defined in subclause *3GPP TS 23.502 [63], section 4.2.2.2.2*. As part of the registration procedure, the VPLMN AMF invokes the **Nudm_SDM_Get** service operation message to the HPLMN UDM. This service operation helps in getting the Access and Mobility Subscription data for the UE.
3	The following are the responses from the HPLMN UDM, reciprocating to the **Nudm_SDM_Get** service operation message: • Sending SOR • Requesting ACK from the UE

Step	Description
4	When the HPLMN UDM sends the response using the **Nudm_SDM_Get** service operation to the VPLMN AMF, the following are the next substeps: • This response includes the SOR information in the Access and Mobility Subscription data. **Note** The Access and Mobility Subscription data type defined as in *3GPP TS 23.502, section 5.2.3.3.1*. • The HPLMN requests the UE to ACK the successful security check of the received SOR information. • The HPLMN requests this ACK with an indication in the **Nudm_SDM_Get** service operation of SOR information.
5	As part of the registration procedure, the VPLMN AMF invokes the **Nudm_SDM_Subscribe** service operation to the HPLMN UDM: • To subscribe to the subscription data notification changes received in Step 4. • To include the notification of SOR updates in the Access and Mobility Subscription data.
6	The VPLMN AMF sends the received SOR information to the UE in Registration Accept.
7	The SOR security check procedure takes place at UE.
8	The UE performs the PLMN selection procedure and ends the procedure, when: • The information check fails. • Although the UE is configured to receive the SOR information, but it does not receive.
9	UE sends Registration Complete to the serving AMF with an SOR transparent container including the UE ACK: • When the UDM requested an ACK from the UE. • When the UE verifies the HPLMN SOR information from Step 7.
10	AMF uses the **Nudm_SDM_Info** service operation to provide the received SOR transparent container to the UDM in Registration Complete: • If the HPLMN decides that the UE must ACK with the successful security check for the received SOR information from Step 4, then the verification process begins. • If the UDM verifies the ACK provided by UE specified in *3GPP TS 33.501*.
11	UE performs the PLMN selection when a high priority PLMN is available.

SOR After the UE Registration Call Flow

This section describes the SOR after the UE Registration call flow.

Figure 79: SOR After the UE Registration Call Flow

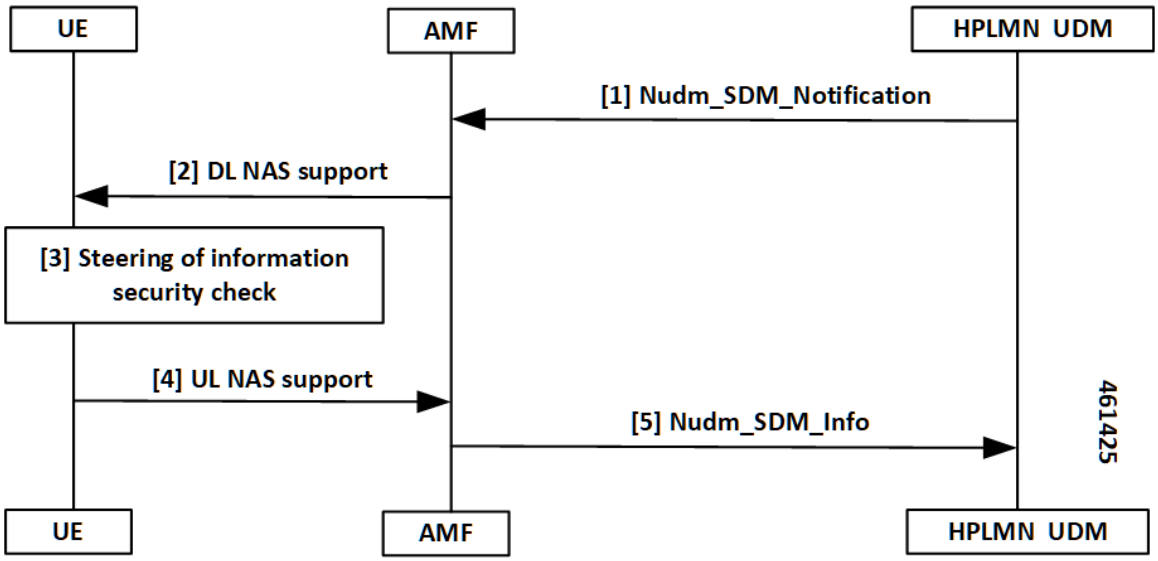


Table 190: SOR After the UE Registration Call Flow Description

Step	Description

1	UDM notifies the changes of the user profile using **Nudm_SDM_Notification** service operation to the affected AMF. The following are the substeps:
	• The **Nudm_SDM_Notification** service operation contains the SOR which must be delivered to the UE over NAS in the Access and Mobility Subscription data.
	• When the HPLMN decides the following:
	  • The UE must ACK the successful security check of the received SOR, including the **Nudm_SDM_Notification** service operation.
	  • It contains an indication which represents UDM requests as an ACK from the UE as part of the SOR.

2	The AMF sends DL NAS TRANSPORT to the served UE. The AMF includes the SOR information as received from the UDM in DL NAS TRANSPORT.
3	The SOR security check procedure takes place at UE.
4	UE sends UL NAS TRANSPORT to the serving AMF with an SOR: • When the UDM requested an ACK from the UE in the DL NAS TRANSPORT message. • When the security check-in at Step 2 is successful.

Step	Description
5	If UL NAS TRANSPORT with an SOR transparent container is received, the AMF uses the **Nudm_SDM_Info** service operation to forward the received SOR to the UDM. If the HPLMN decides the following: • The UE must ACK the successful security check for the received list of preferred PLMN or access technology combinations from Step 1. • The UDM verifies the ACK provided by UE.

Standards Compliance

This feature complies with the following standards specifications:

- *TS 23.501, "System Architecture for the 5G System (5GS)"*
- *TS 23.502, "Procedures for the 5G System (5GS)"*
- *TS 29.274, " 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control Plane (GTPv2-C); Stage 3"*
- *TS 29.503, "5G System; Unified Data Management Services; Stage 3"*
- *TS 29.518, "5G System; Access and Mobility Management Services; Stage 3"*
- *TS 38.413, "NG-RAN; NG Application Protocol (NGAP)"*

Limitations

This feature has the following limitations in this release:

- No support for non-3GPP specification or emergency registration SOR.
- No support for multiple UDM data changes NotificationRequest at the time for SOR.
- No support when the UDM sends data change notification for SMS, SOR, or RAT restriction all-together. In this scenario, the AMF ignores the SOR and the RAT restriction data changes and notifications.
- No support when the service request is received with PDU sync request. In this scenario, the response paging request is ignored from the AMF, due to SOR UDM data changes and notifications.
- No support when the AMF starts accepting the service with PDU sync up, and the UE context setup procedure. In this scenario, it later sends DL NAS Transport for SOR changes and notifications.

Feature Configuration

Configuring this feature involves the following steps:

- Configuring the Core Network Type Restriction, on page 420
- Configuring the 5GC Inter-PLMN Roaming, on page 357
- Configuring the Idle Mode for Steering, on page 421

Configuring the Core Network Type Restriction

When the UE requests access to a restricted area, the AMF configures the cause code to send to a UE. This restriction can be one of the following:

- UDM service area restrictions
- Local configuration-based area code restrictions

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         core-network-type-restriction 5gc override-udm-restrictions
         local-cause-code-map rat-type-restriction 5gmm-cause-code {
5GS-services-not-allowed | no-suitable-cells-in-tracking-area |
plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed | restricted-service-area }
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name to apply the RatType restriction at AMF.
- **core-network-type-restriction 5gc override-udm-restrictions**—When the core network restriction is configured as 5GC, the AMF restricts the 5GC access to subscribers associated with the Call Control Policy. When 5GC is configured with **override-udm-restrictions**, the AMF ignores the UDM defined restrictions and considers the locally configured restrictions.
- **local-cause-code-map rat-type-restriction 5gmm-cause-code { 5GS-services-not-allowed | no-suitable-cells-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | restricted-service-area }**—Specify the 5GMM cause code.

Configuring the 5GC Inter-PLMN Roaming

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
      local-cause-code-map registration-restriction cause-code-5gmm
plmn-not-found
      end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- **local-cause-code-map registration-restriction cause-code-5gmm plmn-not-found**—When the subscriber is a roamer and has registration restrictions, the AMF rejects the subscriber with the **plmn-not-found** cause setting.

Configuring the Idle Mode for Steering

To configure this feature, use the following configuration:

```
config
   amf-global
      paging-map paging_map_name_1
         precedence precedence_name_1
         trigger-type trigger_type_sor
      paging-profile-name paging_profile_name_pp3
      end
```

NOTES:

- **paging-map** *paging_map_name_1*—Specify the paging map and related values.
- **precedence** *precedence_name_1*—Specify the type or value of precedence.
- **trigger-type** *trigger_type_sor*—Specify the type of trigger.
- **paging-profile-name** *paging_profile_name_pp3*—Specify the name of the paging profile to apply the idle mode for steering restriction at the AMF.

OAM Support

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

Statistics for Steering

The following are different types of statistics for steering and their associated examples:

num_sdm_info API Type

```
n8_service_stats{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",
message_type="NudmSdmSorAckInfoReq",
reason="No-Content",service_name="amf-service",
status="success"}1
```

```
n8_service_stats{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",
message_type="NudmSdmSorAckInfoRsp",
reason="gateway-Timeout",service_name="amf-service",
slice_data="2-051615"status="failures"}5
```

```
n8_service_stats{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",
message_type="NudmSdmSorAckInfoRsp",
reason="No-Content",service_name="amf-service",
slice_data="2-051615"status="success"}1
```

Paging TriggerType SOR

```
amf_nas_message_total{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",message_direction="outbound"
message_type="Paging_TriggerType_sor",
service_name="amf-service"}31
```

Paging Statistics for SOR—When the Paging Trigger Type is Configured in the CLI

```
amf_nas_message_total{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",message_direction="outbound"
message_type="Paging_TriggerType_sor",
service_name="amf-service",slice_data="2-333333"} 21
```

```
amf_nas_message_total{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",message_direction="outbound"
message_type="Paging_Trigger_SOR_PAGING",
service_name="amf-service",slice_data="2-333333"}75
```

Paging Statistics for SOR—When the Paging Trigger Type is Not Defined in the CLI

```
amf_nas_message_total{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",message_direction="outbound"
message_type="Paging_TriggerType_default",
service_name="amf-service",slice_data="2-333333"} 21
```

```
amf_nas_message_total{app_name="AMF",cluster="clu1",
data_center="dc1",instance_id="0",message_direction="outbound"
message_type="Paging_Trigger_SOR_PAGING_default",
service_name="amf-service",slice_data="2-333333"}75
```

Roaming Restriction and Operator Support

The AMF provides the mobility restriction functionality handling, enforcement, and management. It provides mobility roaming restrictions along with operator support.

The mobility restriction consists of RAT restriction and core network type restriction.

The UDM provides RAT and core network type restriction in the subscription data that are provided as in **am-data** during and after the registration process.

How it Works

This section describes how this feature works.

Standards Compliance

This feature complies with the following standards specifications:

- *TS 23.501, "System Architecture for the 5G System (5GS)"*
- *TS 23.502, "Procedures for the 5G System (5GS)"*
- *TS 29.274, " 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control Plane (GTPv2-C); Stage 3"*
- *TS 29.503, "5G System; Unified Data Management Services; Stage 3"*
- *TS 29.518, "5G System; Access and Mobility Management Services; Stage 3"*
- *TS 38.413, "NG-RAN; NG Application Protocol (NGAP)"*

Limitations

This feature has the following limitations in this release:

- No support for UE reachability notifications to NFs.
- No support for forbidden area and service area restrictions.
- No support when N26 consigns and hands over from 5G to 4G. In this scenario, the AMF only updates the mobility restriction IEs in MMContext toward the MME in Forward Relocation Request (for connected mode HO) or Context Response (for idle mode HO).
- No support when N26 consigns and hands over from 4G to 5G. In this scenario, the AMF only enforces the mobility restriction IEs received in MMContext from the MME in Forward Relocation Request (for connected mode HO) or Context Response (for idle mode HO).
- No support when N2 HO updates with any of the changes in AMF or inter-AMF UE Context Transfer. In this scenario, the AMF acts only as a target node. The AMF does not support and does not enforce the mobility restriction IEs received in ueContext from the source AMF.
- No support for index-based ADD operation in UDM data changes NotificationRequest for a new core or RAT restriction type.
- No support when the target AMF applies only for those applicable enforcement-based parameters on the restrictions. In this scenario, these parameters are based on the restrictions that are received from the UDM. They are only from the locally configured setup at the target AMF.

Relationships

The following subfeatures are associated with this feature:

- UDM Subscription, on page 423
- Restrictions Enforcement at AMF, on page 425
- Mobility Restriction IEs, on page 427

UDM Subscription

The AMF validates the parameters for RAT Restrictions, Core Network Type Restrictions, and Local Cause Code Mapping. The AMF performs these activities, when it receives the subscription data as am-data. The AMF checks whether the UE is allowed or any enforcement is applicable.

The UDM provides RAT and Core Network Type restrictions in subscription data during and after registration.

When the requested data is modified, the UDM notifies the registered AMF subscribers. The AMF sends the modified mobility list to the UE. If the subscriber is already registered, the AMF continues to serve the UE or deregister based on the updated restrictions.

UDM subscription data configures the AMF with restrictions using RAT type restrictions or local configuration in the Call Control Policy. When the UDM provides the restrictions, the AMF uses and enforces them accordingly. When the UDM doesn't provide restrictions, the AMF uses and implements the available local policy configuration from the Call Control Policy based restriction.

On receiving the updated subscription data and am-data change notification from UDM, the AMF performs the following:

- Processes the data change notifications
- Saves the RAT and Core Network values in the UE context
- Applies the enforcements, if applicable

Note UE rejects the call at any time during a restriction. During an emergency registration, the AMF doesn't check the restrictions.

The following subfeatures are associated with this feature:

- RAT Restrictions, on page 424
- Core Network Type Restrictions, on page 424
- Local Cause Code Mapping, on page 425

RAT Restrictions

In a restricted RAT, the UE can’t access the network for that PLMN.

The UDM subscription data configures restrictions for AMF using RatTypeRestrictions or local configuration in the Call Control Policy.

The AMF enforces the restriction or policy configuration in the following scenarios:

- When the UDM provides RatTypeRestrictions, the AMF enforces the restrictions.
- When the UDM doesn’t provide RatTypeRestrictions, the AMF uses the available local policy configuration from Call Control Policy.
- When the UDM provides the available RatTypeRestrictions and local policy is configured, the AMF uses only the UDM-provided RatTypeRestrictions. You can also override the UDM-based RatTypeRestrictions with local configuration using the **override-udm-restrictions** command.

Core Network Type Restrictions

The AMF supports the Core Network Type restrictions to restrict the core network access to the subscriber.

The AMF enforces the restrictions in the following scenarios:

- The UDM subscription data configures restrictions for the AMF using CoreNetworkTypeRestrictions or local configuration in the Call Control Policy.
- The AMF utilizes the UDM-provided CoreNetworkTypeRestrictions. If UDM doesn't provide CoreNetworkTypeRestrictions, the AMF uses the restrictions based on the local policy configuration from the Call Control Policy.
- The Call Control Policy is configured when the availability of CoreNetworkTypeRestrictions is defined.
- The AMF uses only the UDM-provided CoreNetworkTypeRestrictions.
- You can also override the UDM-based CoreNetworkTypeRestrictions with local configuration using the **override-udm-restrictions** command.

Local Cause Code Mapping

Local Cause Code Mapping provides the operator with the flexibility to configure a preferred GMM cause code, which must be sent to the UE in response to various failures.

The following subfeatures are associated with this feature:

- Core Network Type Restriction, on page 425
- RAT Type Restriction, on page 425

Core Network Type Restriction

The local Cause Code Mapping enables the operator to configure a preferred 5GS Mobility Management Cause Code, by ignoring the default cause code values.

The local cause code mapping can be configured in the Call Control Policy configuration, which is associated with the Operator Policy configuration.

You can configure different cause codes for different types of area restrictions. The following are a few examples:

- Reject cause code for the area which isn’t part of the `Allowed` list, can be configured using the type `not-in-allowed`.
- Reject cause code for the area where the UE access is part of the `Not Allowed` or `Restrict` types, can be configured using the `Not Allowed` type.

The local cause code mapping configuration for the registration is rejected due to the Core Network Type restrictions configured in the AMF. The 5GMM cause code is used for both UDM-based or local configuration restrictions.

RAT Type Restriction

The local cause code mapping configuration for the registration is rejected due to the Core Network Type restrictions configured in the AMF. The 5GMM cause code is used for both UDM-based and local configuration restrictions.

Restrictions Enforcement at AMF

The 5GC AMF receives all connection and session-related information from the UE.

The following subfeatures are associated with this feature:

Enforcement during or after Registration

To authenticate the UE, control integrity protection, and encoding, you can use the 5GMM procedures. These procedures are used for tracing, following, and identifying the address, locality, and the vicinity of the UE.

The following procedures are used during this process:

- When the subscriber interacts for the first time with the AMF and if restrictions are applicable, the AMF enforces the restrictions by sending Registration Reject with a cause code value towards the UE.
- When the subscriber is already registered, a required change in RAT or Core Network Type restriction is triggered through the UDM data change notification. This data notification requires the AMF to apply fresh enforcements.
- If these restrictions are applicable, the AMF deregisters the subscriber or else continues to allow the subscriber to be in the network.
- The AMF saves the changed RAT and Core Network Type restrictions in the UE context.
- The AMF sends the changed RAT and Core network restriction values in the next outgoing Handover Request or Initial Context Setup Request (ICSR).

Enforcement during Mobility

The following options are associated with this subfeature:

N2HO

When the N2HO option is selected, the AMF performs the following actions:

- During N2HO, the AMF encodes and sends the Restricted RAT list and Restricted Core Network list in the UE context transfer request.
- On receiving the UE context transfer request from the source AMF, the AMF decodes the Restricted RAT list and Restricted Core Network list.
- The AMF saves the Restricted RAT list and Restricted Core Network list in the UE context am-data subscription.
- The AMF checks whether the UE is 5GC restricted or not. If the UE is 5GC restricted, the AMF sends a failure note for the N2HO with and without change.

N26HO

When the N26HO option is selected, the AMF performs the following actions:

- When the N26 connected mode handover is from the AMF to the MME, the AMF checks whether the UE is EPC restricted or not. If the UE is EPC restricted, the AMF sends a **HANDOVER_REQUIRED_MSG** failure to source gNB.
- When the N26 connected mode handover is from the MME to the AMF, the AMF checks whether the UE is 5GC restricted or not. If the UE is 5GC restricted, the AMF rejects the UE.

Enforcement at AMF for Emergency PDU

During the triggering process of enforcement for a RAT or a core restriction type, the AMF performs the following actions:

- The AMF starts the deregistration process toward the PCF or the UDM, when the UE has an emergency PDU established before.
- The AMF initiates the release only for non-emergency PDU, whereas the emergency PDU remains active.
- The AMF moves the UE as an option of emergency registered.

Enforcement at N26 Call Flow

The enforcement restriction at N26 call flow type is also known as a handover process from 5G to 4G. During this handover process, the following observations are noted:

- Restriction enforcement received from the UDM subscription, responses to the am-data part.
- This response is a specific core type restriction which is equivalent only to EPC.
- The AMF rejects the EBI assignment request from the SMF with a restricted EBI cause.

Enforcement at Idle Mode Handling from UDM

During UE transaction in an idle mode, the AMF processes the following:

- Receives the UDM data change notification from the UDM for restriction, which must be imposed.
- Initiates the paging as per the configured paging profile.
- Triggers the **init dereg** trigger type.
- Starts the paging activities toward the UE.

Mobility Restriction IEs

Mobility Restrictions are included in the AMF when:

- Restrictions are applicable to a UE and the registration type isn't Emergency Registration.
- Emergency Registration is sent in Downlink NAS Transport with the message type as Registration Accept.

Note This procedure as specified in *TS 23.502, "Procedures for the 5G System (5GS)."*

The AMF encodes the following mobility restrictions IEs:

- Downlink NAS Transport
- Handover Request
- Initial Context Setup Request (ICSR)

Note The AMF supports only the serving PLMN.

Downlink NAS Transport

The AMF performs the following activities:

- NG-RAN with a Mobility Restriction List having the last E-UTRAN PLMN Identity and the Return preferred indication.

Note The Mobility Restriction List contains a list of PLMN IDs as specified in *TS 23.501, "System architecture for the 5G System (5GS)."*

Handover Request

The AMF performs the following activities:

- The AMF sends a Handover Request with a Mobility Restriction List to the NG-RAN.

  The AMF provides the NG-RAN with a PLMN list in the Mobility Restriction List containing the serving PLMN and the last E-UTRAN PLMN Identity.

Note The Mobility Restriction List contains the PLMN IDs as specified in *TS 23.501, "System architecture for the 5G System (5GS)"*

- The AMF sends the Handover Request from the T-AMF (Target AMF) to the T-RAN (Target RAN) with the following parameters:
  - Source to Target transparent container
  - N2 MM Information
  - N2 SM Information list
  - Tracing Requirements

  If the target AMF has the Mobility Restriction List, the same list is sent in N2 MM Information.
- The AMF sends N2 MM Information from AMF to RAN with the following parameters:
  - Security context
  - Mobility Restriction List
  - List of recommended cells

- Tracing Area
- NG-RAN node identifiers

Initial Context Setup Request (ICSR)

During Service Request and PDU establishment, the AMF sends the ICSR IE.

Feature Configuration

Configuring this feature involves the following steps:

- Configuring the RAT Restriction, on page 429
- Configuring the RAT Type Restriction, on page 429

Configuring the RAT Restriction

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy call_control_policy_name
         rat-type-restrictions { EUTRA | NR | VIRTUAL | WLAN |
override-udm-restrictions }
         local-cause-code-map rat-type-restriction 5gmm-cause-code {
5GS-services-not-allowed | no-suitable-cells-in-tracking-area |
plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed | restricted-service-area }
         end
```

NOTES:

- **call-control-policy** *call_control_policy_name*—Specify the call control policy name to apply the restriction at AMF as **RatType**.
- **rat-type-restrictions { EUTRA | NR | VIRTUAL | WLAN | override-udm-restrictions }**—Specify the RAT type. The default RAT type is NR. Configuring the RAT restriction is optional. The AMF restricts the NR access to the subscribers using or associating with the Call Control Policy.

  When the RAT type is configured as **override-udm-restrictions**, the AMF ignores the UDM defined restrictions and considers the locally configured restrictions.
- **local-cause-code-map rat-type-restriction 5gmm-cause-code { 5GS-services-not-allowed | no-suitable-cells-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | restricted-service-area }**—Specify the 5GMM cause code.
- The default option for RAT type restrictions is **plmn-not-allowed** for the **rat-type-restrictions** command.

Configuring the RAT Type Restriction

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         rat-type-restrictions { EUTRA | NR | VIRTUAL | WLAN |
override-udm-restrictions }
         local-cause-code-map restricted-zone-code cause-code-5gmm {
5GS-services-not-allowed | no-suitable-cells-in-tracking-area |
plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed | restricted-service-area }
         end
```

NOTES:

- **rat-type-restrictions { EUTRA | NR | VIRTUAL | WLAN | override-udm-restrictions }**—Specify the RAT type.
- **local-cause-code-map restricted-zone-code cause-code-5gmm { 5GS-services-not-allowed | no-suitable-cells-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | restricted-service-area }**—Specify the local cause code map restricted zone code cause-code-5gmm type.

OAM Support

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

Roaming Restriction Statistics

The following are examples of statistics for roaming restriction:

Disconnect Statistics Mobility/Service Reject: After Dereg Trigger Due to Restriction

```
amf_disconnect_stats{app_name="AMF",
cluster="clu1",data_center="dc1",instance_id="0",
reason="Dereg_RESTRICTED",service_name="amf-service"}1
** No UE Terminared Dereg
```

UDM Data Change Notification Trigger Disconnect and Dereg Statistics

```
amf_disconnect_stats{app_name="AMF",
cluster="clu1",data_center="dc1",instance_id="0",
reason="Dereg_UDM_RESTRICTED",
service_name="amf-service"}1
```

```
amf_nas_message_total{app_name="AMF",
cluster="clu1",data_center="dc1",instance_id="0",
message_direction="outbound",
message_type="N1DeRegReq_UeTerminatedDereg_UDM_RESTRICTED",
service_name="amf-service",slice_data="2-333333"} 1
```

Operator Policy

This section describes the operator policy and the various sets of subscribers mapping, in the AMF operator center.

Operator policy supports various configurations specific to the following features:

- Operator Policy Infrastructure and Subscriber Map
- Regional Area Code Restrictions
- Local Cause Code Mapping
- UE Access (Core Network type) Restrictions

The AMF operator center supports configurations for operator policies, under the Call Control Policy and the paging profile.

How it Works

Operator policy can be selected using one of the following methods:

Single Stage Selection

This selection type can be opted after the security mode command selects between IMSI or IMEI.

Multiple Stage Selection

This selection type consists of the following options:

- After authentication (SUPI)
- After security mode command (IMEI)
- After MSIDN (known from UDM procedures)

Note The newly selected operator policy comes into effect and it does not affect or revert to any of the existing configurations, due to the selection of the previous operator policy.

Call Flows

This section describes the key call flows for this feature.

Initial Registration Call Flow

This section describes the Initial Registration call flow.

Figure 80: Initial Registration Call Flow

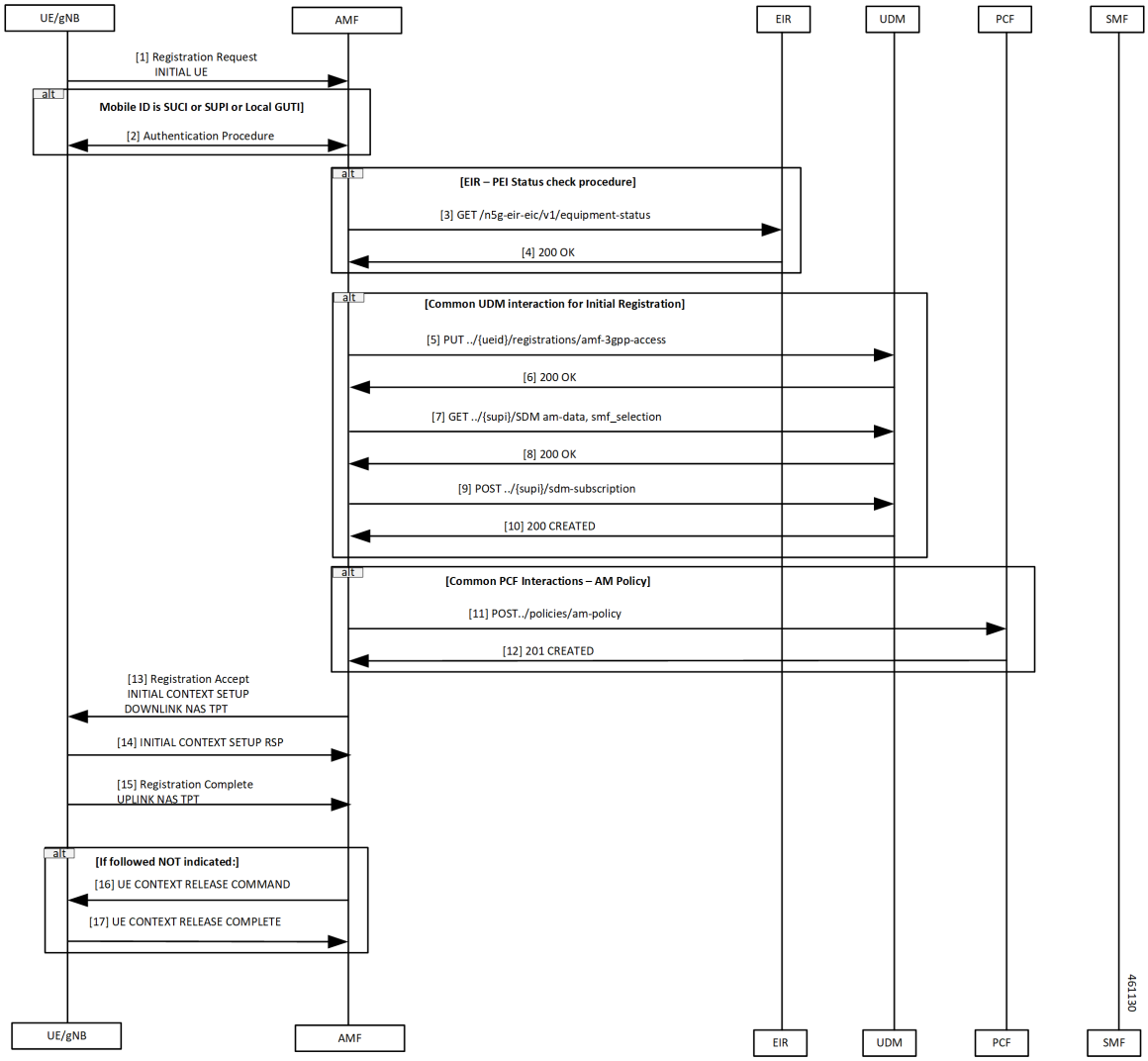


Table 191: Initial Registration Call Flow Description

Step	Description
1	The UE sends Registration Request to the AMF.
2	The authentication procedure occurs between the UE and the AMF.
3	The AMF performs the equipment status check with the EIR using the GET command.
4	The AMF receives 200 OK from the EIR.
5	The AMF requests the Access and Mobility subscription from the UDM. The UDM responds to the AMF request and the AMF stores the subscription information for RAT and core network type in UeContext.

Step	Description
6	The AMF receives 200 OK from the UDM.
7	The AMF requests the SMF selection subscription data from the UDM.
8	The AMF receives 200 OK from the UDM.
9	The AMF requests the UDM for the notifications when data is modified.
10	The UDM registers the AMF and responds to the AMF for subscription with 201.
11	The AMF selects the PCF based on PLMN, slice information, and performs Policy Association Establishment. The PCF sends the policy data to the AMF with restrictions and other policies to be applied for the UE.
12	The PCF responds to the AMF request along with am-policy configurations for the subscriber.
13	The AMF sends Registration Accept to the UE in Initial Context Setup Downlink NAS TPT indicating that Registration Request is accepted. The AMF fills in the Mobility Restriction List IE with RAT and core restrictions as per the UDM or local configuration settings. Registration Accept contains the following: • 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 gNB sends Initial Context Setup Response to the AMF.
15	When a new 5G-GUTI is included in Registration Accept, the UE sends Registration Complete to the AMF in Uplink NAS TPT. This message acknowledges that a new 5G-GUTI is assigned.
16	If the UE doesn't include a follow-on indication in the request: • The AMF sends UE Context Release Command to the gNB. • AMF releases the UE.
17	The gNB responds with UE Context Release Complete to the AMF.

Relationships

The following subfeatures are associated with this feature:

- Subscriber Maps, on page 434
- Operator Policy Selection, on page 434

Subscriber Maps

You can create and manage subscriber maps. These maps are created by using the AMF Subscriber Map configuration mode. These maps have the following usages:

- Applying and associating operator policy configurations to individual subscribers and groups of subscribers.
- UE identity information such as the PLMN of UE, SUPI, or PEI.

The system uses the first matching criteria precedence from the ordered list to associate an operator policy with the UE.

Operator Policy Selection

Based on the configuration, the AMF selects or reselects the operator policy on the subscriber-map using the available criteria (PLMN, SUPI, PEI, and so on) in the following procedures for an individual subscriber:

- Initial Registration
- Registration—GUTI, Mobility with AMF change
- N2 Handover with AMF change
- 4G to 5G handovers

Feature Configuration

Configuring this feature involves the following steps:

- Configuring under AMF Services, on page 434
- Configuring RAT Restrictions under Call Control Policy, on page 435
- Configuring Core Network Restrictions under Call Control Policy, on page 435

Configuring under AMF Services

To configure this feature, use the following configuration:

```
config
   amf-services
      amf-name amf_name
         [ no ] operator-policy-name operator_policy_name
         end
```

NOTES:

- **amf-name** *amf_name*—Specify the name of AMF services.
- **operator-policy-name** *operator_policy_name*—Specify the name of the operator policy.
- The association of operator policy with the AMF service is a default global policy, which applies to all the subscribers under this service.

Configuring RAT Restrictions under Call Control Policy

To configure this feature, use the following configuration:

```
config
   amf-global
      amf-name amf_name
         call-control-policy call_control_policy_name
            rat-type-restriction rat_type_restriction_option { EUTRA | NR |
VIRTUAL | WLAN | override-udm-restrictions }
               paging-profile paging_profile_name
               end
```

NOTES:

- **amf-name** *amf_name*—Specify the name of AMF global services.
- **call-control-policy** *call_control_policy_name*—Specify the name of the call control policy.
- **rat-type-restriction** *rat_type_restriction_option* **{ EUTRA | NR | VIRTUAL | WLAN | override-udm-restrictions }**—Specify the options for RAT network type restriction in the call control policy. Select the RAT type as **override-udm-restrictions** as the option.
- **paging-profile** *paging_profile_name*—Specify the name of the paging profile.
- The association of operator policy with the AMF service is a default global policy, which applies to all the subscribers under this service.

Configuring Core Network Restrictions under Call Control Policy

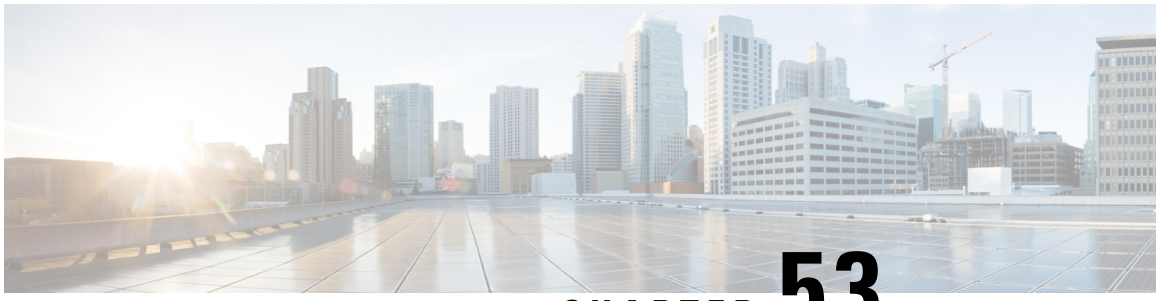
To configure this feature, use the following configuration:

```
config
   amf-global
      amf-name amf_name
         call-control-policy call_control_policy_name
            core-network-type-restriction { 5gc |
override-udm-restrictions }
            end
```

NOTES:

- **amf-name** *amf_name*—Specify the name of AMF global services.
- **call-control-policy** *call_control_policy_name*—Specify the name of the call control policy.
- **core-network-type-restriction { 5gc | override-udm-restrictions }**—Specify the options for core network type restriction in the call control policy.

- The association of operator policy with the AMF service is a default global policy, which applies to all the subscribers under this service.



CHAPTER 53

Subscription Concealed Identifier Profile

Feature Summary and Revision History

Summary Data

Table 192: 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 193: Revision History

Revision Details	Release
Content enhanced with 5G-AMF to support the PSI Profile-A/Profile-B feature.	2023.02.0
First introduced.	2021.04.0

Feature Description

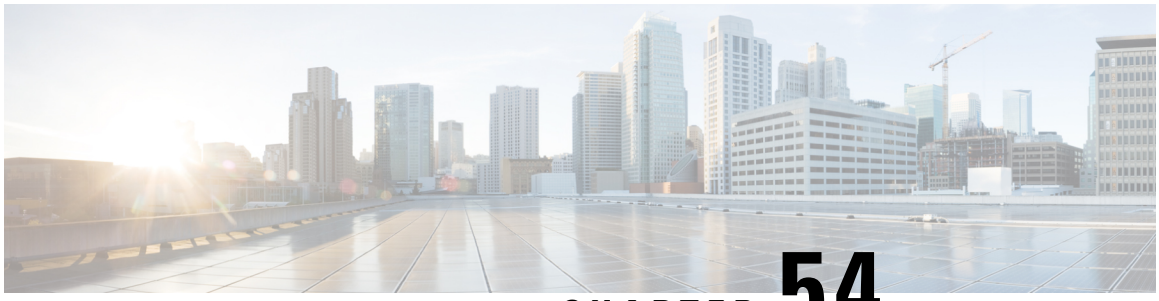
A Subscription Concealed Identifier (SUCI) is a unique identifier designed to protect the privacy of the subscriber's identity. It's generated by the User Equipment (UE) using an Elliptic Curve Integrated Encryption Scheme (ECIES)-based protection scheme. The UE encrypts the Subscriber Permanent Identifier (SUPI) in a concealed method with the public key of the Home Network. It's securely provisioned to the Universal Subscriber Identity Module (USIM) during the registration process.

How it Works

The protection scheme used in generating the SUCI only conceals the Mobile Subscriber Identification Number (MSIN) part of the SUPI, while the Mobile Country Code (MCC) and Mobile Network Code (MNC) that constitute the Home Network Identifier are transmitted in plain text. The SUCI data fields include the following in the chronological order:

- **SUPI Type Field**—This field is a numeric value ranging 0–7, which indicates the type of SUPI concealed in the SUCI. The following values are currently defined:
  - **0**—International Mobile Subscriber Identity (IMSI)
  - **1**—Network Access Identifier (NAI)
  - **2–7**—Reserved for future use
- **Home Network Identifier Field**—This field identifies the home network of the subscriber. When the SUPI Type is IMSI, the Home Network Identifier is composed of the MCC and the MNC that uniquely identify the home network. When the SUPI Type is a NAI, the Home Network Identifier is a variable-length string of characters that represents a domain name. For example, in the form of `user@domain.com`
- **Routing Indicator Field**—This field is a numerical value consisting of 1–4 decimal digits. It’s assigned by the home network operator and securely provisioned within the Universal Subscriber Identity Module (USIM).
- **Protection Scheme Field**—This field is a 4-bit value ranging 0–15, which identifies the protection scheme used to generate the SUCI. The following values are currently defined:
  - **Null Scheme**—0x0
  - **Profile <A>**—0x1
  - **Profile <B>**—0x2
  - **Other Values (3–15)**—Reserved for future use
- **Home Network Public Key ID Field**—This field is an 8-bit value ranging 0–255, which identifies the public key provisioned by the Home Public Land Mobile Network (HPLMN) and used for SUPI protection. When the Null Scheme is used, this field is set to 0.
- **Protection Scheme Output Field**—This field is a variable-length string of characters or hexadecimal digits, depending on the protection scheme used to generate the SUCI.

Note When the Null Scheme is supported, the AMF can derive the SUPI value from the SUCI. However, if a protection scheme other than Null is used, the AMF needs to obtain the SUPI value through interaction with the AUSF.



CHAPTER 54

TLS Transport Support

Feature Summary and Revision History

Summary Data

Table 194: 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 195: 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 442.
- Server Certificates configuration—This configuration provides the commands to configure the server certificates. For more information, refer to Configuring the Server Certificates, on page 442.
- TLS Enable Configuration—This configuration enables the TLS. For more information, refer to Enabling the TLS, on page 443.

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 209.165.200.224 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

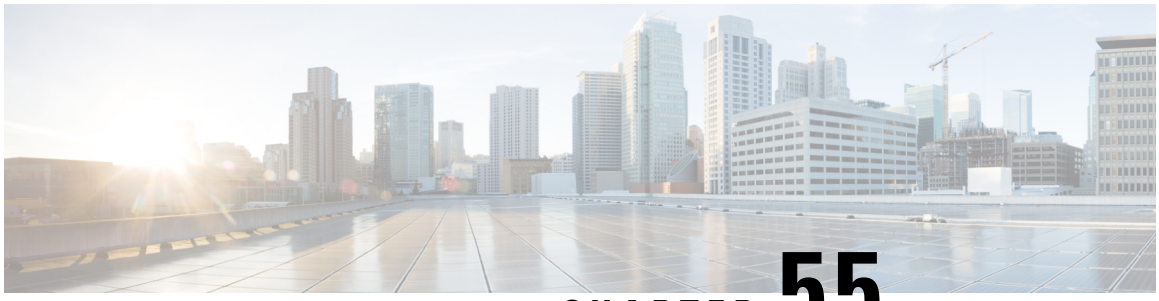
This section describes troubleshooting information for this feature.

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 55

UE Context Transfer Support

Feature Summary and Revision History

Summary Data

Table 196: 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 197: Revision History

Revision Details	Release
Updated the context-transfer-guard timer details	2023.02.0
First introduced.	2022.01.0

Feature Description

AMF supports the UE Context Transfer message at source and target AMF. The following CLI configurations are added:

- `allow-interplmn-supi-transfer`
- `horizontal-key-derivation`
- `use-source-key`
- `use-source-pcf`

UE Context Transfer at Source AMF:

- Sends UE Context with SUPI value to target AMF as per the CLI configuration, when source AMF and target AMF are in different PLMN
- Uses either existing keys or generates new keys, and sends the keys to target AMF during context transfer as per the CLI configuration
- Starts context-transfer-guard timer (configured with greater than zero (0)), when UeRegStatusUpdateReqData contains transfer status as TRANSFERRED

  On expiry of the context-transfer-guard timer, source AMF performs the following:

  - Triggers the UDM Deregistration internally to clear the local ueContext
  - When the UE Context Transfer reason is INIT_REG, it updates the SMF to release the PDU context

- It releases PDU sessions in the toReleaseSessionList
- The UE-validation reason is handled as follows:
  - Without registration request
  - By omitting integrity check
  - Responding with appropriate data to target AMF
- Clears PCF association, when target AMF sends pcfReselectedInd in transfer update
- Handles reject indication received from target AMF
- Performs horizontal key derivation as per the CLI configuration
- Transfers URI with SUPI as ueContextId to target AMF
- Sends DRX, GMM capability IEs to target AMF
- Increments transfer failure counters including NOT_TRANSFERRED counters
- Doesn't send SeafData in transfer response in MOBI_REG_UE_VALIDATED when the Individual ueContext is identified with SUPI

UE Context Transfer handling at Target AMF:

- Sends Reject Indication to source AMF through StatusUpdate message when authentication or security fails

  The security algorithm mismatch is handled as follows:

  - Authenticates when integrity check fails
  - Recomputes the keys as per the algorithm received from AUSF
  - Regenerates all the keys and ignores the keys received from source AMF.

- Sends failure to source AMF when authentication or security check fails
- The SUPI as UeContextID is handled as follows:
  - Sends Identity request to UE when message integrity check fails
  - Performs UE authentication with obtained SUPI from UE
  - Sends SUPI as UeContextId, and UE-validated in UeContextTansferReq to source AMF
- Ignores the PCF information obtained from the source AMF and selects the new PCF based on the CLI configuration. Informs the selection of new PCF using pcfReselectedInd to source AMF in UeRegStatusUpdateReq.

How It Works

This section describes how this feature works.

Call Flows

This section describes the key call flow for this feature.

UE Context Transfer Call Flow

This section describes the UE Context Transfer call flow.

Figure 81: UE Context Transfer Call Flow

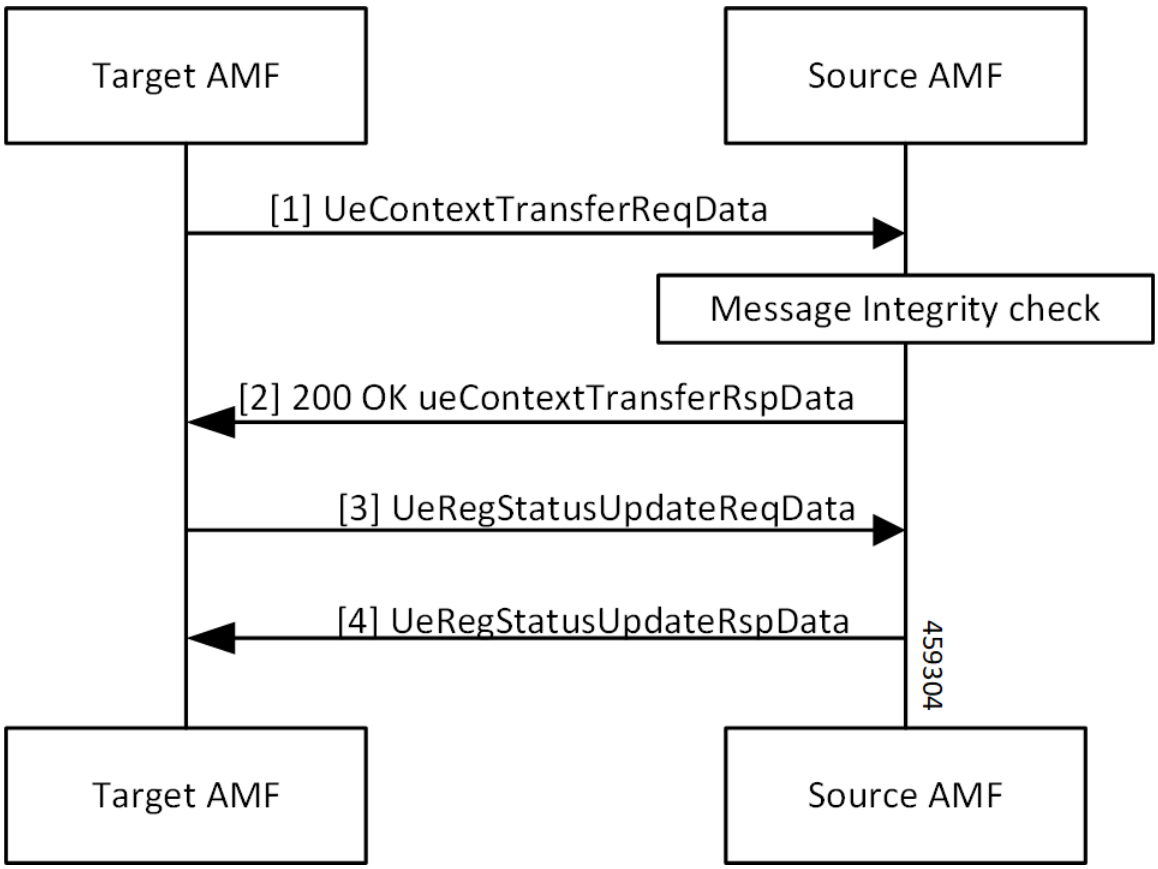


Table 198: UE Context Transfer Call Flow Description

Step	Description
1	The target AMF sends the UeContextTransferReqData to the source AMF.
2	The source AMF performs message integrity check. It responds with 200 OK UeContextTransferRspData to the target AMF.
3, 4	The target AMF sends UeRegStatusUpdateReqData to the source AMF and receives a response.

Limitations

This feature has the following limitations in this release:

- Non-3GPP access, trace requirements and event subscriptions are not supported.
- In this release, source and target AMF (T-AMF) are expected to have same S-NSSAI configured. As a result, any PDU sessions that belong to S-NSSAIs not supported on T-AMF are not validated are not dropped.

- Target AMF selects new PCF and sends PcfReselectedInd as true even if CLI is configured to use PCF provided by source AMF.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         policy ue-ctx-transfer
            allow-interplmn-supi-transfer { true | false }
            horizontal-key-derivation { true | false }
            use-source-key { true | false }
            use-source-pcf { true | false }
            exit
         timers
            context-transfer-guard
               n14-interface value guard_time_value
               end
```

NOTES:

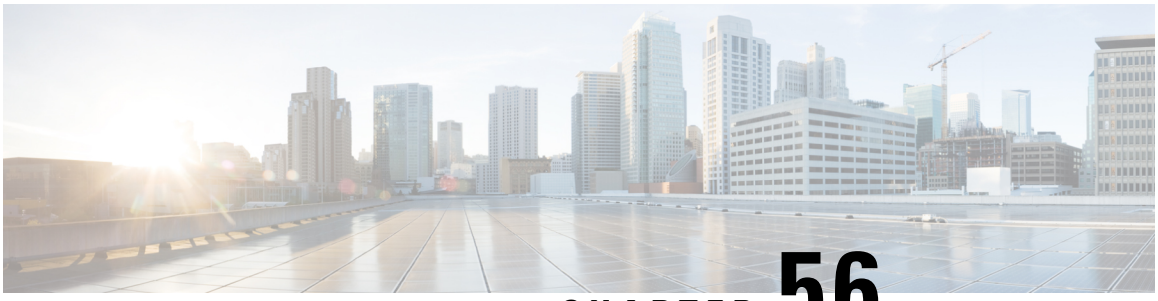
- **call-control-policy** *policy_name*—Configure the Call Control Policy.
- **policy ue-ctx-transfer**—Configure the ue-ctx-transfer Policy.
- **allow-interplmn-supi-transfer { true | false }**—Specify true or false. If configured true, the source AMF sends UE context with SUPI. The default value is **false**.
- **horizontal-key-derivation { true | false }**—If configured true, the source AMF generates a new key every time. The default value is **false**
- **use-source-key { true | false }**—If configured true, the target AMF uses a key received from the source AMF. The default value is **true**
- **use-source-pcf { true | false }**—If configured false, the target AMF sends **pcfReselectedInd** as true in TransferUpdate and the source AMF clears the PCF association. The default value is **true**
- **context-transfer-guard**—Specify the context transfer guard timer. The AMF starts this timer on receiving the TransferUpdate. On expiry, the AMF clears the PDUs locally.
- **n14-interface value** *guard_time_value*—Specify the interface n14-interface value in seconds. It must be an integer in the range of 0—35712000. The default value is zero (0).

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy CCP1
         policy ue-ctx-transfer
            allow-interplmn-supi-transfer true
```

```
   horizontal-key-derivation true
   use-source-key true
   use-source-pcf true
   exit
timers
   context-transfer-guard value 50
   end
```



CHAPTER 56

UE Configuration Management Procedures

Feature Summary and Revision History

Summary Data

Table 199: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	

Revision History

Table 200: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

The AMF supports the generic UE configuration procedure by sending the Configuration Update Command message to the UE when certain parameters are modified. The AMF supports the following parameters in the Configuration Update Command message:

- 5G-GUTI
- TAI list
- SMS indication

For more information, refer to the UCC 5G AMF Configuration and Administration Guide > UE Configuration Management Procedures chapter.

How it Works

This section describes how this feature works.

The AMF initiates the Configuration Update Command procedure when it observes a change in the configuration that was previously sent to a UE. Depending on the nature of the configuration that is modified, the AMF communicates with the UE to send an acknowledgment indicating that the configuration has changed or request the UE to register with AMF again.

The AMF checks for the configuration changes and starts the Configuration Update Command after the following procedures are completed:

- PDU establishment
- Xn-based handover
- N2 handover without the AMF change
- UE-initiated service request in the IDLE state without ICSR or without PDU.
- UE-initiated service request in the IDLE state with ICSR.
- Data change notifications from UDM

Timers

The AMF uses timers to detect configuration changes for UEs in the IDLE mode and UEs in the CONNECTED mode without any signaling activity. If AMF detects changes in configuration for UE in the IDLE mode, the UE is paged. Based on the response, the AMF sends the Configuration Update Command.

- T3555—The AMF transmits the Configuration Update Command message with an acknowledgment request to the UE. While waiting for a response from the UE, AMF starts the T3555 timer. If the timer expires, the AMF retransmits the Configuration Update Command message.
- T3512—When the UE moves to the IDLE mode, the AMF starts an internal timer which is derived from T3512 timer value subtracted by 4 minutes. The resulting value must be greater than 60 seconds. When the timer expires, the AMF checks for any configuration changes and triggers Paging if required.

- Tidle—The tidle timer allows AMF to monitor the UE in the CONNECTED mode without any signaling activity for a defined period. On the expiry of this timer, the AMF performs one of the following actions:
  - If the configuration is modified and the feature is enabled, the AMF initiates the UE Configuration Update Command and restarts the tidle timer.
  - If the configuration has not changed or the feature is disabled, the AMF moves the UE to the IDLE state by sending the respective messages towards gNB and SMF.

TAI List Changes

When the AMF does not receive a response from the UE for the Configuration Update Command triggered due to the changes in the TAI list, then the AMF considers old and new TAI list as valid. When the UE is in the IDLE state, the AMF pages the UE using the old TAI list first. If the UE does not respond and all the paging stages are exhausted, the AMF pages the new TAI list as the final step.

The paging profile for paging the new TAI list is as follows:

```
Action = PAGING_ALL_GNB_ALL_TAI
```

The Action is hardcoded and timeout and MaxPagingAttempts are derived from the T3513 value configured under the call control profile.

Call Flows

This section describes the key call flows for this feature.

Sending the New GUTI to UE Call Flow

This section describes the Sending the New GUTI to UE call flow.

Note The newly allocated GUTI value is sent to the UE using the Configuration Update Command message. The allocation of a new GUTI is possible after the Service Request procedure is complete.

The following call flow describes the 5G GUTI reallocation during the Service Request procedure.

Figure 82: Sending the New GUTI to UE Call Flow

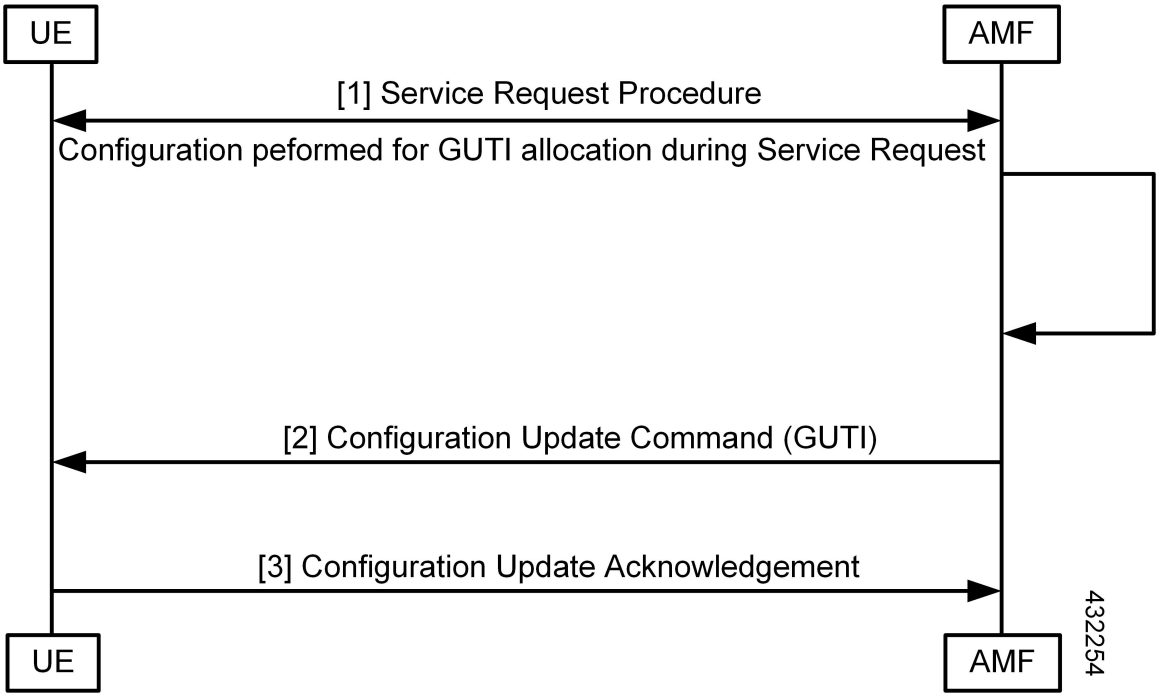


Table 201: Sending the New GUTI to UE Call Flow Description

Step	Description
1	The UE sends the Service Request procedure to the AMF to perform both or one of the following: • Establish the N1 NAS signaling connection. • Establish the UP resources for PDU sessions which are activated without UP resources.
2	After the Service Request procedure is complete, and the AMF is configured to reallocate a new GUTI, then the new GUTI is allocated and sent in the Configuration Update Command message to UE.
3	The UE acknowledges the new GUTI by sending the Configuration Update Acknowledgment message.

UE Configuration Update Call Flow

This section describes the UE Configuration Update call flow.

Figure 83: UE Configuration Update Call Flow

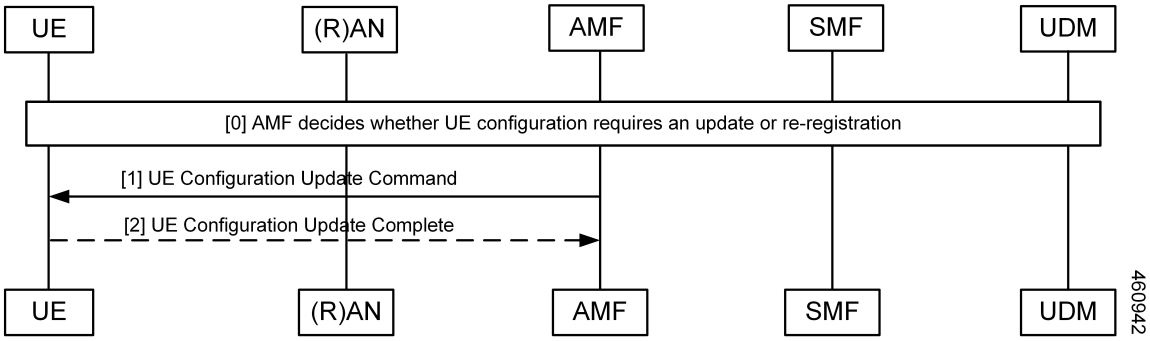


Table 202: UE Configuration Update Call Flow Description

Step	Description
1	When the AMF detects configuration changes for an UE, it sends a UE Configuration Update Command message to the UE. If the UE is in the idle mode, the AMF triggers paging based on the configuration.
2	As a response, the UE acknowledges the request and sends the configuration updates to the AMF.

UDM Notification Interaction Call Flow

The UE Configuration Update command is also triggered when UDM notifies AMF about change in subscription data.

This section describes the UDM Notification Interaction call flow.

Figure 84: UDM Notification Interaction Call Flow

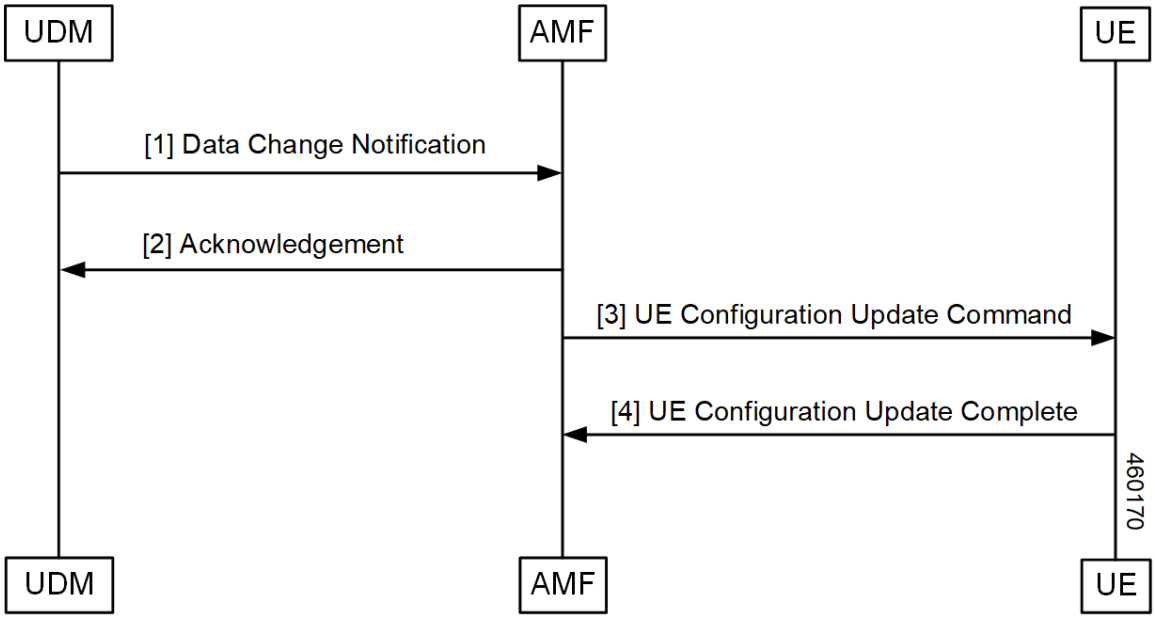


Table 203: UDM Notification Interaction Call Flow Description

Step	Description
1	UDM notifies the subscription data change to AMF. **Note** In this release, AMF only supports detection of changes to SMS subscription data as a part of UDM Data change notification.
2	As a response, the AMF acknowledges the change.
3	AMF compares new subscription data with the existing data. If any change is detected and: • If UE is in CONNECTED mode, AMF triggers UE Configuration Update Command to UE. • If UE is in IDLE mode, AMF triggers paging based on the configuration. Post paging response from UE, AMF may trigger UE Configuration Update command.
4	UE sends UE Configuration Update Complete to AMF.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.501 "System architecture for the 5G System (5GS)"*
- *3GPP TS 23.502 "Procedures for the 5G System (5GS)"*
- *3GPP TS 24.501 "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"*

Configuring Support for UE Configuration Update Command

Configuring this feature involves the following steps:

- Enable the AMF to send the new GUTI allocation requests. For more information, refer to Configuring New GUTI Allocation, on page 456.
- Enable the AMF to send the UE Configuration Update Command. For more information, refer to Enabling UE Configuration Update, on page 456.

Configuring New GUTI Allocation

To configure the GUTI allocation, use the configuration provided in the AMF Authentication and GUTI Reallocation Configuration Control chapter.

Enabling UE Configuration Update

To enable the UE configuration update feature, use the following configuration:

```
config
   amf-global
      call-control-policy policy
         policy ue-cfg-update { on-sms-change [ true | false ] |
on-tai-change [ true | false ] }
         end
```

NOTES:

- **policy ue-cfg-update**—Enters the UE configuration mode.

  This command includes the follow subcommands:

  - **on-sms-change**—Starts the UE Configuration Update procedure when changes to SMS configuration is detected.
  - **on-tai-change**—Starts UE configuration update procedure when the TAI list is modified.

Configuring Paging

Configuring this feature involves the following steps:

- Configure paging so that when the UE is in the IDLE state, the AMF starts the timer for UE configuration. For more information, refer to Configuring the Paging Feature, on page 457.
- Configure the paging profile specific to UE configuration. The AMF uses this profile for paging. For more information, refer to Configuring the Paging Profile, on page 458.
- Enable AMF to page the new TAI list when UE doesn't respond to AMF when it pages using the old TAI list. For more information, refer to Configuring AMF to Page the New TAI List, on page 458.
- Configure the T355 timer. The AMF starts this timer while waiting for a UE response. For more information, refer to Configuring the T3555 Timer, on page 459
- Enable the tidle timer to monitor if the UE is in the CONNECTED mode without any signaling activity for a defined period. For more information, refer to Enabling the Tidle Timer for Inactive UEs in the Connected Mode, on page 459.

Configuring the Paging Feature

To configure paging, use the following configuration:

```
config
   amf-global
      call-control-policy ccpolicy_name
         policy idle-mode
            paging use-new-tailist
            udm-notification initiate-paging SMS
            ue-cfg-update initiate-paging
            end
```

NOTES:

- **policy idle-mode paging use-new-tailist**—Configures AMF to page using the new TAI list as the last step.
- **policy idle-mode udm-notification initiate-paging**—Configures paging which is triggered when the AMF detects configuration changes as part of the UDM data change notification received for UEs in the IDLE mode.
- **policy idle-mode ue-cfg-update initiate-paging**—Configures the AMF to start the internal timer when the UE moves to the IDLE mode, for detecting configuration changes and trigger paging, if required.

Configuring the Paging Profile

To configure this feature, use the following configuration:

```
config
   amf-global
      paging-map pagingmap_name
         precedence paging_precedence
            trigger-type [ uecfg ]
               paging-profile-name profile_name
               end
```

NOTES:

- **paging-map** *pagingmap_name*—Specify the paging map name. Must be a string in the range of 1–64 characters.
- **precedence** *paging_precedence*—Specify the precedence level. Must be an integer in the range of 1–255, where 1 indicates the highest precedence and 255 indicates the lowest precedence.
- **trigger-type [uecfg]** —Specify the paging trigger type.
- **paging-profile-name** *profile_name*—Specify the paging profile name. Must be a string in the range of 1–64 characters.

Configuring AMF to Page the New TAI List

To configure the AMF to page the new TAI list, use the following configuration:

```
config
   amf-global
      call-control-policy ccpolicy_name
         policy idle-mode paging
            use-new-tailist
            end
```

NOTES:

- **policy idle-mode paging**—Configures the paging for UE configuration for the IDLE mode paging.
- **use-new-tailist**—Configures AMF to page using the new TAI list.

Configuring the T3555 Timer

To configure the timer, use the following configuration:

```
config
  amf-global
    call-control-policy ccpolicy_name
      timers [ t3555 ]
         retry retry_count
         value value
         end
```

NOTES:

- **timers [t3555]**—Configure the t3555 timer for the Configuration Update Command message.
- **retry** *retry_count*—Specify the number of retransmission attempts that AMF must perform on expiry of the timer. Must be an integer in the range of 0-5. The default value is 4.

Note On expiry of the timer, AMF attempts retransmission of the Configuration Update Command message.

- **value** *value*—Specify the timer value in seconds. Must be an integer in the range of 0-30. The default value is 6 seconds.

Enabling the Tidle Timer for Inactive UEs in the Connected Mode

To configure the tidle timer, use the following configuration:

```
config
   amf-global
      call-control-policy ccpolicy_name
         timers [ tidle ]
            value tidle_value
            end
```

NOTES:

- **timers [tidle]** —Configure the tidle the timers. Tidle indicates the duration for which the UE is in the CONNECTED mode without any activity.
- **value** *tidle_value*—Specify the duration for which the UE can stay in the CONNECTED mode without the signaling activity. AMF monitors the UE for the configured amount of time which is the tidle. Must be an integer in the range of 30–25200 seconds.

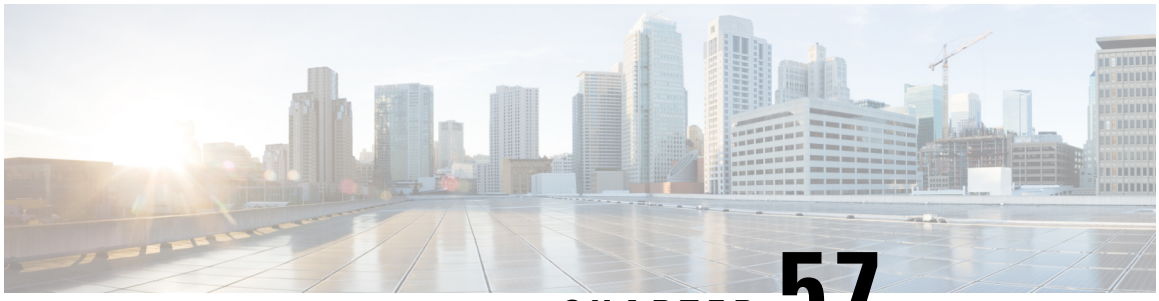
OAM Support

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

Statistics

The following statistics are supported for the User Equipment Configuration Management Procedures feature.

- configuration_update_command—Captures the number of Configuration Update Command messages sent.
- configuration_update_complete—Captures the number of Configuration Update Acknowledgment messages received.



CHAPTER 57

Voice over New Radio (VoNR) Support

Feature Summary and Revision History

Summary Data

Table 204: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Emergency Services: Disabled – Configuration required to enable Emergency Voice Fallback: Disabled – Configuration required to enable
Related Documentation	

Revision History

Table 205: Revision History

Revision Details	Release
Enhancement introduced. The Emergency Services Fallback feature allows the UE to reconnect to EUTRAN either through 5GC (4G radio, 5G core) or EPC (4G radio, 4G core).	2022.04.0
Enhancement introduced. Introduced the emergency services.	2022.01.0
First introduced.	2021.04.0

Feature Description

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

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

Voice over New Radio (VoNR) Support

Feature Description

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

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

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

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

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

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Initial or Mobility Registration—IMS VoNR Support Procedure Call Flow

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

Figure 85: Initial or Mobility Registration—IMS VoNR Support Procedure Call Flow

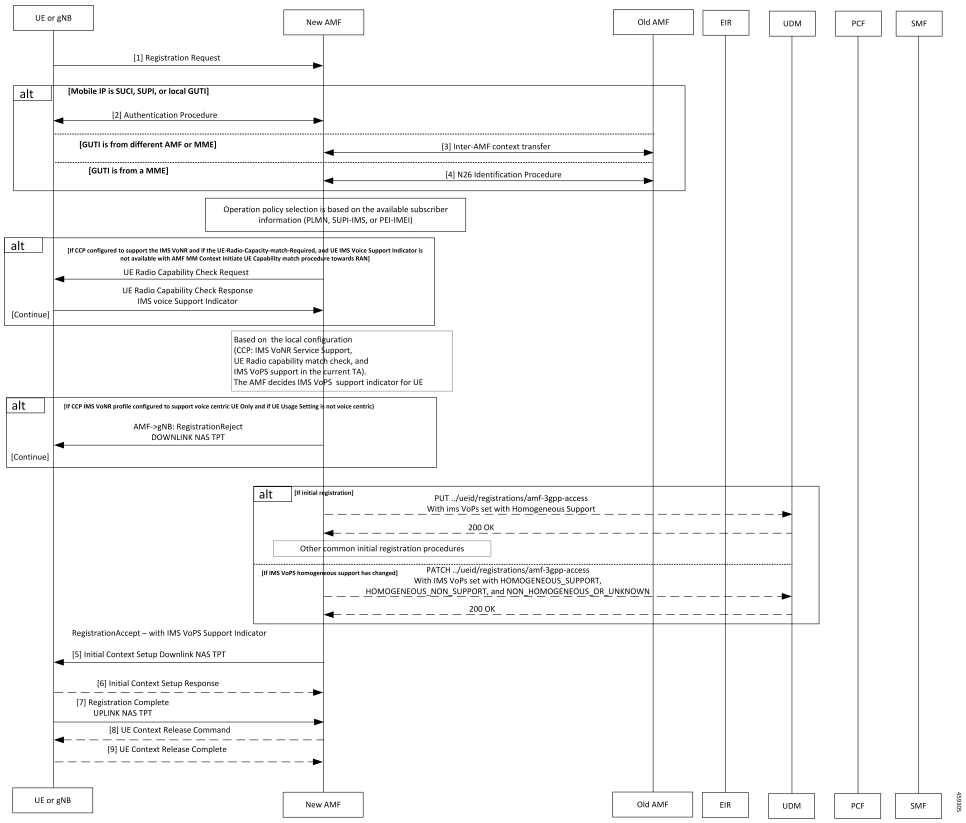


Table 206: Initial or Mobility Registration—IMS VoNR Support Procedure Call Flow Description

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

Provide UE Information for Terminating Domain Selection Call Flow

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

Figure 86: Provide UE Information for Terminating Domain Selection Call Flow

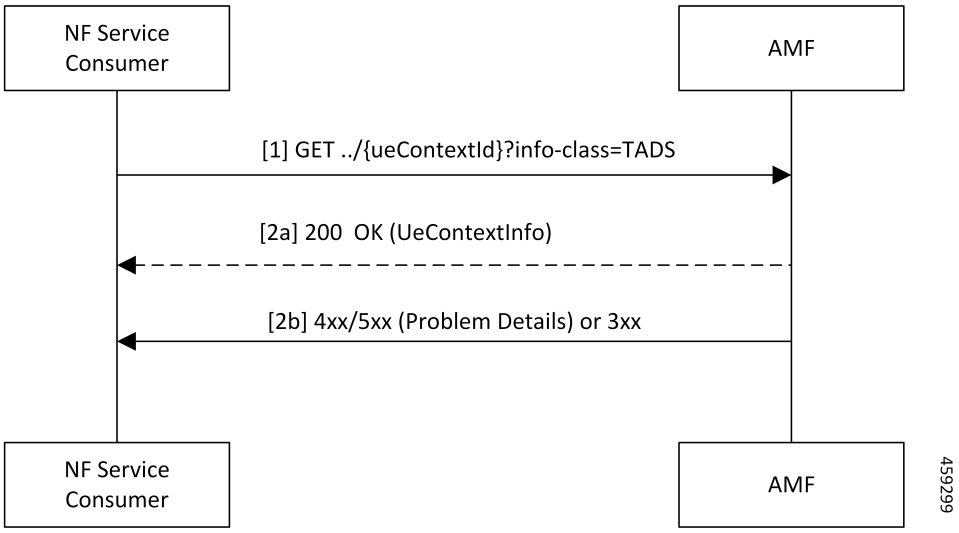


Table 207: Provide UE Information for Terminating Domain Selection Call Flow Description

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

Standards Compliance

This feature complies with the following standards specifications:

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

Limitations

This feature has the following limitations in this release:

- The AMF doesn’t support IMS services over non-3GPP access.

- The IMS VoPS support indication is applicable only for the voice-centric UE usage setting type.

Feature Configuration

Configuring this feature involves the following steps:

1. Enable AMF to indicate if the UE is capable to handle IMS Voice over Packet-Switched (VoPS) sessions. For more information, refer to Configuring Support to Indicate IMS VoPS Support, on page 466.
2. Configure IMS VoPS service for the configured TALs. For more information, refer to Configuring the TAL-level IMS VoPS, on page 466.

Configuring Support to Indicate IMS VoPS Support

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

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

NOTES:

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

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

Configuring the TAL-level IMS VoPS

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

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

```
config
   amf-global
     call-control-policy policy_name
        tai-group tai_group_name
```

```
tais tai_value
  ims-voice-over-ps-supported { false | true }
  end
```

NOTES:

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

OAM Support

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

Statistics

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

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

Emergency Services

Feature Description

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

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

How it Works

This section describes how this feature works.

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

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

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

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

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

Call Flows

This section describes the key call flows for this feature.

Node-level Call Flow

This section describes the Node-level call flow.

Figure 87: Node-level Call Flow

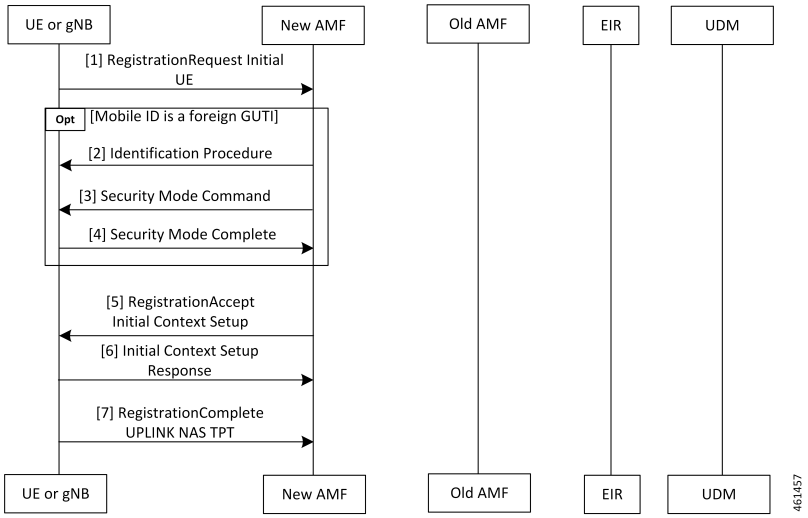


Table 208: Node-level Call Flow Description

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

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

Standards Compliance

This feature complies with the following standards specifications:

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

Limitations

AMF does not support the emergency services in the following scenarios:

- E-call interactions
- Congestion interactions
- Identification, authentication, EIR and UDM interaction
- Configuration change in emergency profile communication to UE
- Security procedure failure scenario for normal registration
- Support for EPS type of service request is not available

Feature Configuration

Configuring this feature involves the following steps:

- Configure the emergency services to enable the UE to handle the emergency requests through the Registration Accept message on per-TA and per-RAT basis. For more information, refer to Associating the Emergency Profile with the AMF Services or Global Configuration, on page 470.

- Configure the emergency profile to define the emergency parameters of the NF. For more information, refer to Configuring Emergency Profile, on page 470.

Configuring Emergency Profile

To configure this feature, use the following configuration:

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

NOTES:

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

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

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

Associating the Emergency Profile with the AMF Services or Global Configuration

To configure this feature, use the following configuration:

```
config
  amf-global
     operator-policy local
     ccp-name ccp_value
     emergency-profile-name profile_name
     network-element-profile-list [ amf | ausf | nssf | pcf | udm | smf
```

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

NOTES:

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

Configuration Verification

To verify the configuration:

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

Sample Output

```
profile emergency-profile e911
  dnn starent1.com
  slice name emergency sst 2 sdt 000003
  ue-validation-level none
  local-emergency-num 100 police
  exit
amf-global
amf-name cisco-amf
```

```
dnn-policy starent.com
  network-element-profile-list smf smf1
exit
dnn-policy starent1.com
  network-element-profile-list smf smf1
exit
operator-policy local
  ccp-name local
  network-element-profile-list ausf ausf1
  network-element-profile-list smf smf1
  network-element-profile-list pcf pcf1
  network-element-profile-list udm udm1
  network-element-profile-list nssf nssf1
  emergency-profile-name e911
exit
exit
 amf-services am1
amf-name AMF
emergency-profile-name e911
exit
```

PDN Creation, Modification, and Release

Feature Description

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

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

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

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

How it Works

This section describes how this feature works.

Standards Compliance

This feature complies with the following standards specifications:

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

Call Flows

This section describes the key call flows for this feature.

SM Context Update Call Flow

This section describes the SM Context Update call flow.

Figure 88: SM Context Update Call Flow

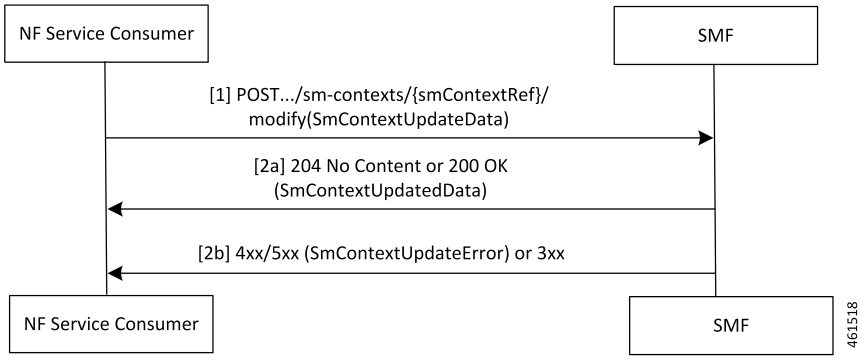


Table 209: SM Context Update Call Flow Description

Step	Description
1	The AMF service consumer performs both or one of the following: • Updates a particular SM context • Provides N1 or N2 SM information to the SMF through the HTTP POST method (modify custom operation). The POST request contains the following information: • The release IE is set to true. • The cause IE is set to REL_DUE_TO_REACTIVATION.

Step	Description
2a	The SMF responds with the SmContextUpdatedData data type that contains the following response codes: • 204 No Content—The SM context is successfully updated when the SMF does not return information in the response. • 200 OK—The SM context is successfully updated when the SMF returns information in the response.
2b	When the SM Context Update fails, the SMF reports an error. For a 4xx or 5xx response, the message body contains an SmContextUpdateError structure.

Feature Configuration

Configuring this feature involves the following steps:

1. Configure the UDM initiated PCSF restoration procedure at AMF. For more information, refer to Configuring the PCSF Restoration Feature, on page 474.
2. Configure the IMS for identifying the PDU session with DNN name. For more information, refer to Configuring the IMS for DNN, on page 474.
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 475.

Configuring the PCSF Restoration Feature

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

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

NOTES:

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

Configuring the IMS for DNN

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

```
config
   amf-global
```

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

NOTES:

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

Configuring the Query Selection Parameter

To configure the query parameter, use the following configuration:

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

NOTES:

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

Emergency Voice Fallback

Feature Description

The Emergency Services Fallback feature allows the UE to reconnect to EUTRAN either through 5GC (4G radio, 5G core) or EPC (4G radio, 4G core). The fallback occurs when the 5G radio does not support the NR. Depending on the network capabilities, the UE selects 5GC or EPC. If the 5G core is unable to support emergency services, the UE falls back on 4G radio on the 4G core.

AMF supports UE Context Transfer messages for subscribers that are registered for emergency services or nonemergency services with emergency PDU sessions.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Inter AMF (N2_Idle) Scenario Call Flow

This section describes the Inter-AMF (N2_Idle) Scenario call flow.

Figure 89: Inter AMF (N2_Idle) Scenario Call Flow

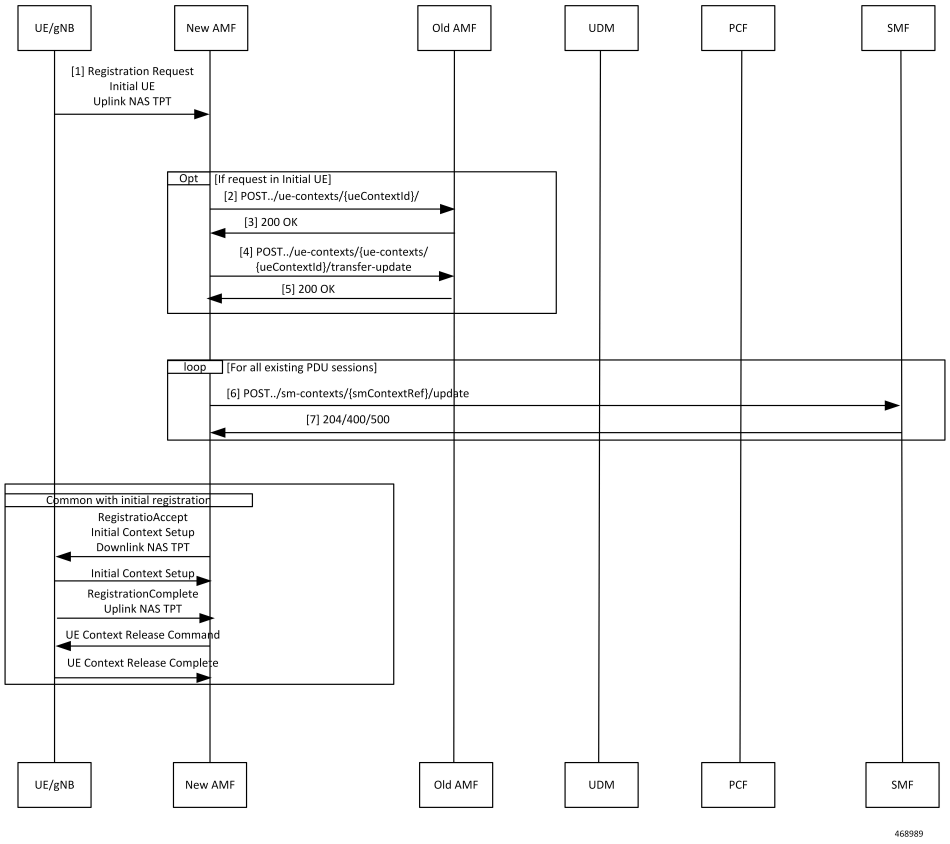


Table 210: Inter AMF (N2_Idle) Scenario Call Flow Description

Step	Description
1	The UE sends a Registration Request with the registration type set to initial or mobility.
2	The New AMF sends the Post../ue-contexts/{ueContextId}/ request to the Old AMF. When the New AMF gets the UE context from the Old AMF, the AMF derives the emergency registration which is based on the following parameters: • supiunauthInd is present • if only IMEI is present and the UE is in the same PLMN.
3	The Old AMF sends the 200 OK message to the New AMF.
4	The New AMF sends the Post../ue-contexts/{ueContexts}/{ueContextId}/transfer-update request to the Old AMF.
5	The Old AMF sends the 200 OK message to the New AMF.

Step	Description
6	The New AMF sends the POST../sm-contexts/{smContextRef}/update to the SMF.
7	The SMF sends the 204/400/500 to the New AMF. From the Registration Accept message onwards, the call flow is the same as Initial Registration Request except for UDM, PCF, and AUSF. For further information on Initial Registration Request, see *Registration with AMF Change Call Flow* in the chapter *Internode Registration Support* in this document.

AMF-MME (N26_Idle) Scenario Call Flow

This section describes the AMF-MME (N26_Idle) Scenario call flow.

Figure 90: AMF-MME (N26_Idle) Scenario Scenario Call Flow

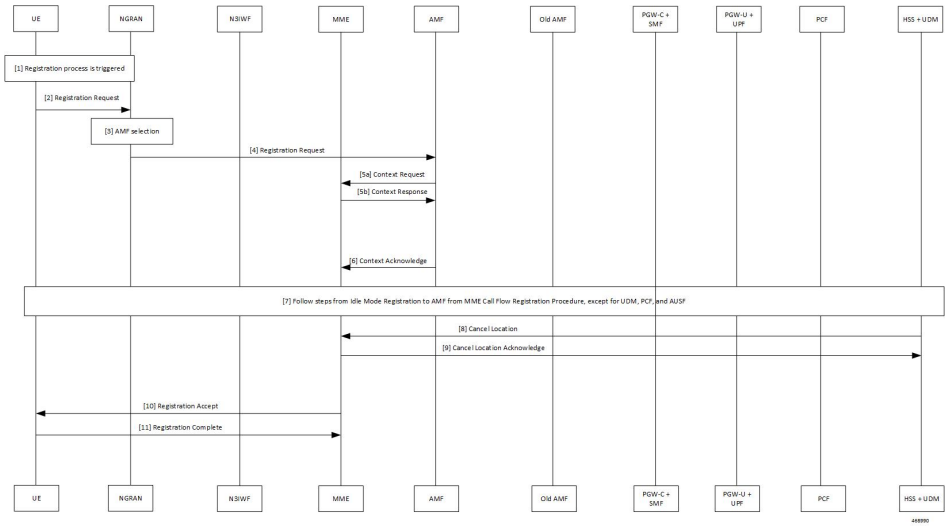


Table 211: AMF-MME (N26_Idle) Scenario Call Flow Description

Step	Description
1	The UE starts a registration procedure.
2	The UE sends a Registration Request to the NGRAN.
3	The NGRAN performs the AMF selection.
4	The NGRAN forwards the Registration Request to the AMF.
5a	The AMF sends the Context Request to the MME.
5b	The MME sends the Context Response to the AMF.
6	The AMF sends the Context Acknowledgment to the MME.

Step	Description
7	From the Context Acknowledgment message onwards, the call flow is the same as Idle Mode Registration to AMF from MME Call Flow except for UDM, PCF, and AUSF. For further information, see *Idle Mode Registration to AMF from MME Call Flow* in the chapter *Internode Registration Support* in this document.
8	The HSS+UDM sends the Cancel Location Request to the MME.
9	The MME sends the Cancel Location acknowledgment to the HSS+UDM.
10	The UE sends the Registration Accept message to the AMF.
11	The AMF sends the Registration Complete message to the UE.

Service Request Procedure Call Flow

This section describes the Service Request Procedure call flow.

Figure 91: Service Request Procedure Call Flow

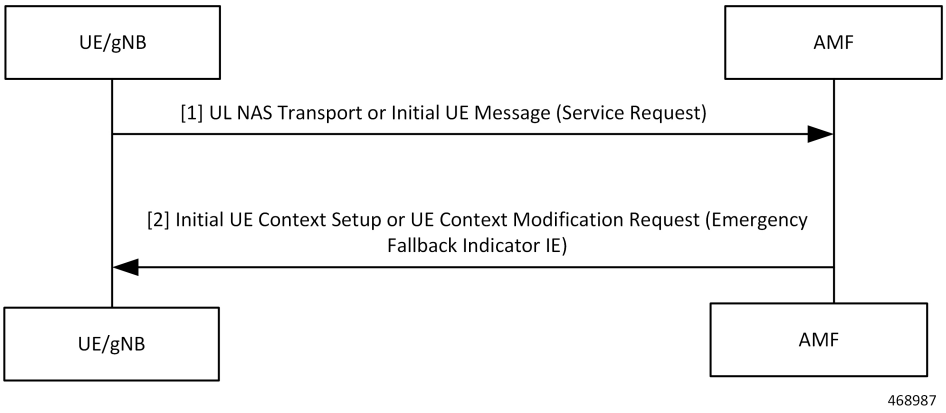


Table 212: Service Request Procedure Call Flow Description

Step	Description
1	The UE sends a Service Request with Service Type set to Emergency Services Fallback.
2	The AMF sends the Initial UE Context Setup request or the Modify UE Context request. If the Emergency Fallback feature support CLI is configured at AMF, AMF sets the Emergency Fallback Indication IE toward gNB in either Initial Context Setup Request or UE Context Modification Request along with Service Accept towards UE. The NGAP IE of the target CN is set optionally as EPC or 5GC, if configured; else CN type is not included. If Emergency Fallback feature support CLI is not configured, AMF sends Service Reject with cause NO SUITABLE CELLS IN TRACKING AREA.

Emergency Fallback Call Flow

This section describes the Emergency Fallback call flow.

Figure 92: Emergency Fallback Call Flow

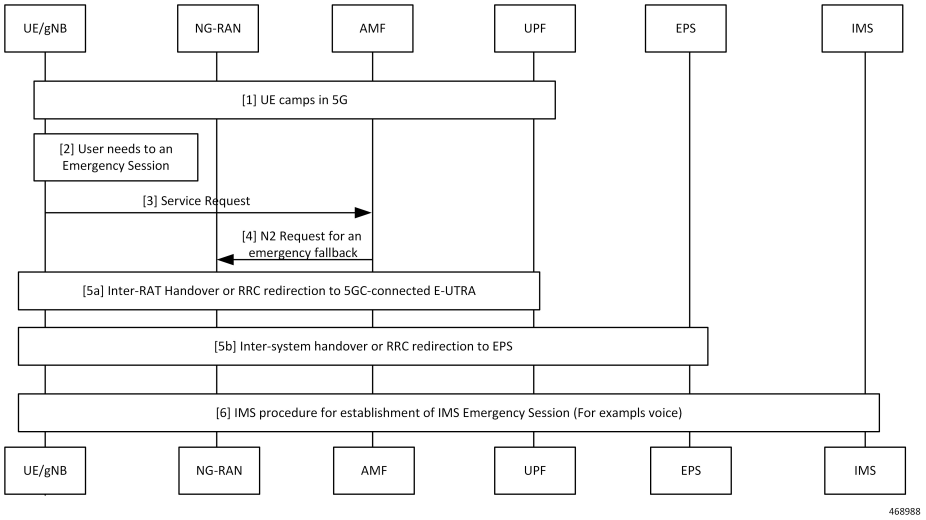


Table 213: Emergency Fallback Call Flow Description

Step	Description
1	The UE camps in the 5G network.
2	The UE starts an emergency session.
3	The UE sends a Service Request to the AMF. For more information, see *Service Request Procedure Call Flow* in this chapter.
4	The AMF sends a N2 Request for emergency fallback to the NG-RAN. For more information, see *Service Request Procedure Call Flow* in this chapter.
5a	The Inter-RAT handover or RRC is redirected to the 5GC-connected E-UTRA.
5b	The intersystem handover or RRC is redirect to EPS.
6	The IMS procedure is started to establish the IMS Emergency Session.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   amf-global
      call-control-policy ccp_name
         feature-support-ie
            emergency-fallback supported target-cn { EPC | 5GC }
            end
```

NOTES:

- **call-control-policy** *ccp_name*—Specify the Call Control Policy name.

- **feature-support-ie**—Enter the feature configuration mode that allows configuring the supported AMF or 5GC features.
- **emergency-fallback supported target-cn { EPC | 5GC }**—Configure AMF to enable UE to direct the emergency fallback to the 5GC or EPC network.

Configuration Example

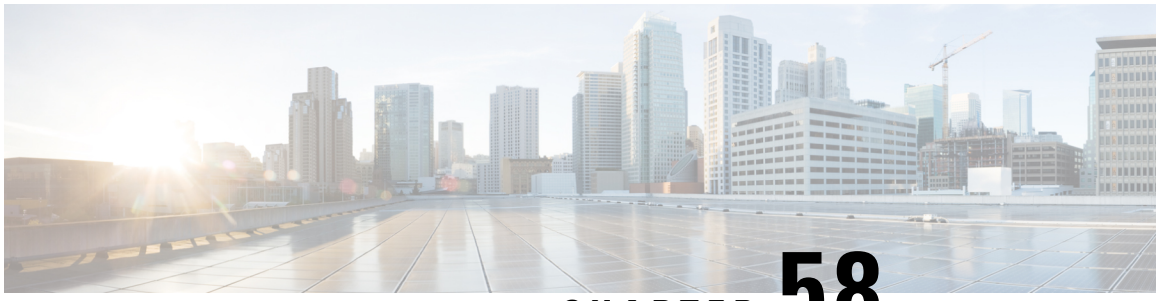
The following is an example configuration.

```
config
   amf-global
      call-control-policy ccp_name
         feature-support-ie
            emergency-fallback supported target-cn EPC
            end
```

Configuration Verification

To verify the configuration:

```
show full-configuration amf-global call-control-policy local feature-support-ie
emergency-fallback
amf-global
 call-control-policy local
  feature-support-ie emergency-fallback supported
  feature-support-ie emergency-fallback target-cn EPC
 exit
exit
```



CHAPTER 58

Xn Handover

Feature Summary and Revision History

Summary Data

Table 214: 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 215: 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 93: Xn Handover Call Flow

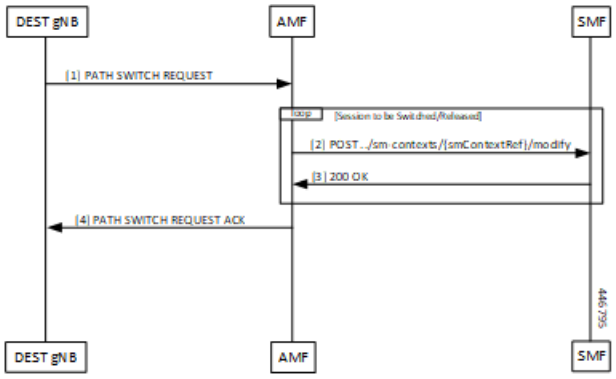


Table 216: Xn Handover Call Flow Description

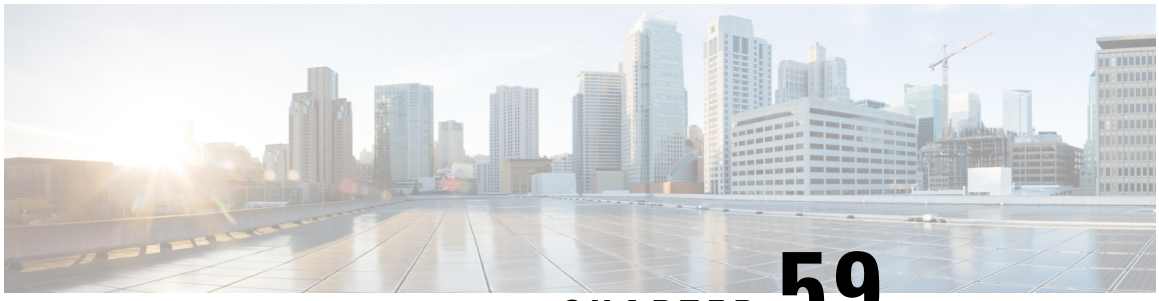
Step	Description
1	Once signaling that involves the UE, source and destination gNB have taken the decision to handover, the destination gNB constructs a PATH SWITCH REQUEST with the list of PDU sessions that have successfully switched and the list of PDU sessions that were not successful.
2	For each 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 59

Troubleshooting

Using CLI Data

This section describes the show and clear commands that are used for troubleshooting.

show subscriber

This section describes the **show subscriber** commands for the existing subscribers sessions.

Table 217: 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 218: clear subscriber Command Output Description

Field	Description
|	Output modifiers.
all	Clears all the subscriber sessions.

Field	Description
gnodeb-id	Clears the sessions that have the specified gnodeb-id.
supi	Clears the sessions based on the SUPI value.

Monitor Subscriber

Table 219: Feature History

Feature Name	Release Information	Description
Monitor Subscriber	2023.04	Cisco AMF supports the monsub to capture the N1/N2/N8/N11/N12/N15/N20/N22/N26 interface level messages. Default Setting: Disabled – Configuration Required

Feature Description

The "Monitor Subscriber" is a debugging and troubleshooting tool which captures the N1/N2/N8/N11/N12/N15/N20/N22/N26 interface level messages. The messages are logged only if SUPI is present or can be found from AMF database.

Configuring the Monitor Subscriber

Following are the various CLI options available for the monitor subscriber.

Option: 1

```
[amf-ops-center] amf# monitor subscriber supi imsi-123456789012345 capture-duration 200
internal-messages yes
```

With the preceding CLI option, both internal and external messages are logged for duration of 200 seconds. To explicitly record N1N2 messages, you must configure the 'internal-messages' option with the value "yes."

Option: 2

```
monitor subscriber supi imsi-123456789012345
```

With the preceding CLI option, only N26 and rest API messages are logged for a duration of 300 secs (default capture duration).

Option: 3

```
[amf-ops-center] amf# monitor subscriber supi imsi-123456789012345 capture-duration 50000
transaction-logs yes
logging transaction message enable.
```

With the preceding CLI option, transaction level messages are logged which are used for internal debugging.

Option: 4

```
[amf] amf# monitor subscriber supi imsi-123456789012345 capture-duration 3000
internal-messages yes file-name amf
```

With the preceding CLI option, MonSub file is generated with provided file-name in CLI.

Limitations

Following are the limitations for the monsub:

- If OAM pod restarts, the previously stored MonSub logs gets deleted.
- Enabling MonSub for a large number or all subscribers in a production environment impacts the system performance. So, it is recommended to enable the Monsub for few or specific subscribers.

Note The CLI option for enabling Monsub with imsi-* is not recommended in loaded system with bulk calls. As mentioned in the preceding section, specific SUPI (example - imsi-1234567890) should be used to capture the message logging with available options.

Not Supported

The MonSub doesn't support the following.

- Messages related to Non-UE
- Monsub CLI (Monitor Subscriber IMSI) and (Monitor Subscriber IMEI)
- Messages towards Lawful Intercept (LI) interface
- All the SBI messages towards NRF
- N2 interface messages like NGSETUP, NGAP_ERROR_INDICATION and NG_RESET

Logs

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 of the error messages:

- 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

Sample log:

```
[ERROR] [ApplicationContext.go:1820] [infra.dpd.core] Ping Unsuccessful for client Id 4
Name: amf-protocol-ep0 Setname: amf-protocol-ep Host: amf-protocol-ep Port: 9003 Url:  for
 [246]
```

Warn

These errors impact few specific call-flows majorly, but not blockers of functionality.

Example of the warning messages:

- 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

Sample log:

```
[WARN] [amf-service.amf-app.messageprocessor] No procedure defined for message type 763
```

Info

This log level purpose is to know information for cause.

Examples of the information messages:

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

Sample log:

```
[INFO] [amf-service.amf-app.auth] Sending N12 Authentication Request to Rest EP
```

Debug

This log level purpose is to get debug messages.

Example of the debug messages:

- All external exchanged messages
- Sending Registration accept to UE
- State machine changes
- Collision detailed logging

Sample log:

```
[DEBUG] [process.go:1606] [amf-service.amf-app.reg] [supi:123456789012345]
[supi:123456789012345] [1] Preparing registration accept to UE 123456789012345
```

Trace

This log level purpose is to get content of all external tracing messages.

Example of the trace messages:

- Registration request message
- N1N2 transfer message

Sample log:

```
[TRACE] [process.go:1627] [amf-service.amf-app.reg] [supi:123456789012345]
[supi:123456789012345]
[496] Sending RegistrationAccept:&MsgNas
{N1MsgType:154,N2MsgType:0,N1Msg:&MsgNas_MsgRegistrationAccept
{MsgRegistrationAccept:&ngn_nas.PBRegistrationAccept{ExtendedProtocolDiscriminator:126,SecurityHeaderType:
&SecurityHeaderType{HeaderType:PLAIN_5G_NAS,},MessageIdentity:&MessageType{MessageType:REGISTRATION_ACCEPT,}
,VgsRegistrationResult:&VgsRegistrationResult{EmergencyRegistered:false,NssaaPerformed:false,SmsAllowed:false,
VgsRegistrationResultValue:TGPP_ACCESS,}
```

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

Frequently Encountered Scenarious

Geo-Replication Pod in Pending State

This section describes how to correct geo-replication pod conflict if shared hardware setup.

Problem

After completing Day1 configuration on AMF, when you deploy AMF and SMF on the same mode, the geo-replication pod is in pending state.

The following table lists the ports configured use by a geo-replication pod. The port numbers are for reference purpose only.

Note The default base port is 15000. You can change the default base port.

Table 220: Ports Configured for Geo-replication Pod

15000	INFRA_PROMETHEUS_PORT
15001	PPROF_EP_PORT
15002	INFRA_ADMIN_PORT
15003	IPC_EP_PORT
15004	GEO_KEEPALIVED_PORT

15005	INFRA_DIAG_PORT

Resolution

1. Change the default base port for geo-pod from 15000 to other available port range.

   instance instance-id *<instance_id>* **endpoint geo internal base-port start** *<new_port>*

Note *<instance_id>* should match the *<local_instance_id>*.

Configure the relevant keepalive port in the SMI configuration (base_port + 4) .

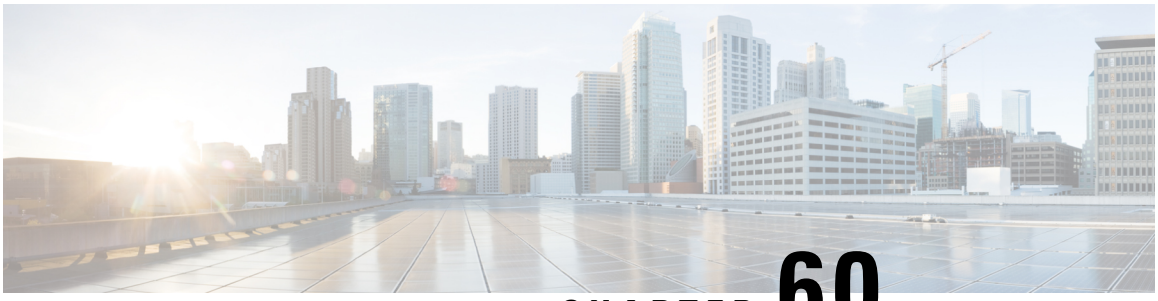
This configuration is required only for the GR setup.

2. To verify that the new port change configuration is reflecting, run the following command.

   ```
   kubectl describe pod georeplication-pod-0 -n cn | grep -i port
   ```

3. SSH to the server where geo-pod is running and run the following command.

   ```
   sudo netstat -plan | grep grpod | grep <port_range> | grep -v
   ```



CHAPTER 60

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 209.165.201.3
    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 209.165.201.3
    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 context-transfer-guard n14-interface value 5
 timers context-transfer-guard n26-interface value 5
 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 209.165.201.3
      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 209.165.201.3
      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 209.165.201.3
      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 209.165.201.3
      primary ip-address port 9082
     exit
     endpoint-name EP2
      priority 20
      primary ip-address ipv4 209.165.201.3
      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 209.165.201.3
      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 209.165.201.3
      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 209.165.201.4
 peer-mme gummei mcc 314 mnc 020 group-id 32777 mme-code 1 address 209.165.201.4
 peer-mme tai-match priority 1 mcc 311 mnc 480 tac 23 address 209.165.201.4
 peer-mme tai-match priority 1 mcc 314 mnc 020 tac 23 address 209.165.201.4
 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 209.165.201.5
  vip-ip 209.165.201.6
 exit
 endpoint sctp
  replicas 2
  nodes    2
  vip-ip 209.165.201.7 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 209.165.201.6
 exit
 endpoint service
  replicas 2
  nodes    2
 exit
 endpoint protocol
  replicas 2
  nodes    2
  vip-ip 209.165.201.6
 exit
 endpoint ngap
  replicas 2
 exit
 endpoint sbi
  replicas     2
  loopbackPort 8091
  instancetype IPv4
```

```
  vip-ip 209.165.201.9 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 209.165.201.8
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.209.165.201.10.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.209.165.201.10.nip.io/amf.2021.04.m0.i26
k8s single-node   false
k8s use-volume-claims true
k8s ingress-host-name 209.165.201.11.nip.io
k8s nodes amf-cndp-b19-3-main-1
 node-type   master
 worker-type master
exit
k8s nodes amf-cndp-b19-3-main-2
 node-type   master
 worker-type master
exit
k8s nodes amf-cndp-b19-3-main-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
```