5GC Product description

IPLOOK Technologies

www.iplook.com

IPLOOK 5GC Product description

IPLOOK Technologies / IPLOOK Technologies Co., Limited

Table of Contents

Revision history

Version	Usage State	Modification Summary	Reviser	Reviewer	Revision date
1.1	Initiation Version		Li	Steven	2019-10
1.2	Done	Add Open Interfaces	Li	Steven	2020-6
1.3	Done	Improve Flexible Network Architecture	Li	Steven	2020-10
1.4	Done	Support NF recursive queries	Mark	James	2021-5
1.5	Done	Enable more functional decoupling and interaction support	Mark	James	2021-11

1 Introduction

1.1 5GC overview

5GC refers to a core network architecture that supports 5G SA access networks. IPLOOK provides SA 5GC with most 4G/3G elements are integrated. It is able to interwork with 4G, 3G and 2G network. IPLOOK 5GC includes AMF, SMF, AUSF, UDM, UPF, PCF, NRF, NSSF and NEF. 5GC is service based which turns the P2P communication into communication among service modules. All the service modules(also called network functions) are able to deployed separately into different VMs or containers. And they are also able to be deployed together into one VM or container.

The diagram of 5GC is shown in Figure 1

Figure 1 5GC Diagram

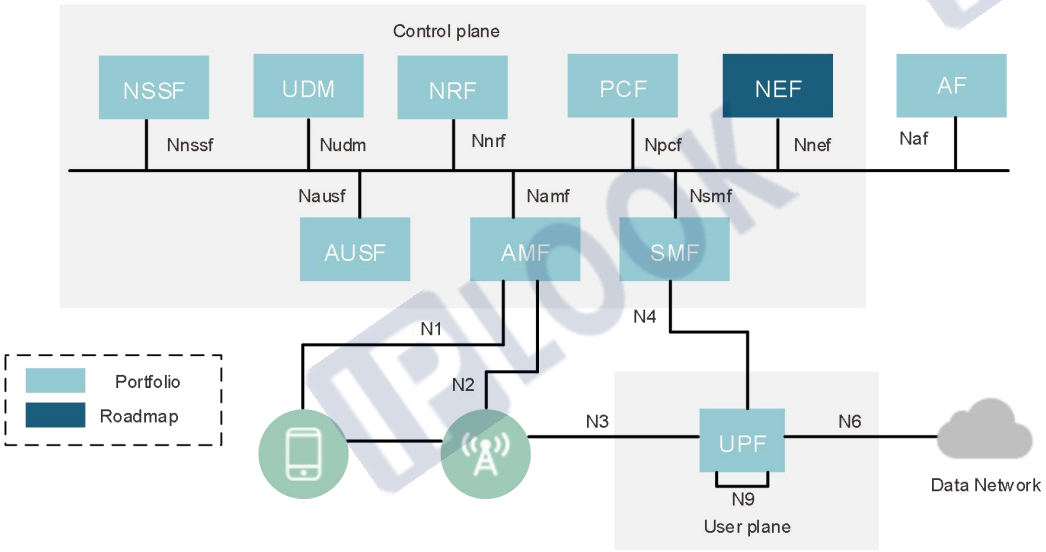


Table 1 Core network node description

Name	Function
NR	5G Radio Access Network.
AMF	Support authentication function, user equipment identification function, 5G-GUTI

Name	Function
	distribution function, NAS (N1 interface) signaling and its security, AS security context issuance function, registration area management, connection management function, registration and deregistration, service request, storage , Modify, delete user mobility context and bearer context information; The interface supports N1, N2, N8, N12, N11, N15; the service-oriented interface protocol supports NAS, NGAP
SMF	Supports PDU session establishment, PDU session modification, PDU session release, activation or deactivation of UP connections, service continuity (SSC), network element selection: UPF selection; PCF selection; UDM selection, business offloading: UL CL; Multi-homing; LADN, switching based on Xn interface, switching based on N2 interface, UE IP address management, CN tunnel management, flow detection, user plane forwarding control, UP path management, packet buffer management, charging policy control function, and associated flow of PDU session Policy, policy control request trigger, QoS Flow binding, policy control request event reporting function, 5GS and EPC policy integration control function, reflection QoS function, basic location management function; Interface support: N1, N2, N4, N7, N10, service-oriented interface protocol support: NAS, PFCP/GTP-U, Nudm.
AUSF	AUSF network elements support NF service authentication, 5G AKA authentication mechanism, and EAP-AKA authentication mechanism; AUSF network element interface supports N12 and N13.
UDM	Support the generation of 3GPP AKA authentication certificates, user identification processing, such as user SUPI storage and management, privacy protection identification (SUCI) de-hiding, subscription data-based access rights, such as roaming

Name	Function
	restrictions, UE service NF management, such as users Serving the storage of SMF information corresponding to AMF and PDN session, supporting service/session continuity, such as the SMF/DNN relationship corresponding to the session, legal monitoring function, user subscription management, short message SMS management, inheriting all functions of 4G HSS and 3G HLR; The interface supports N8, N10, N21, N13, N, 36, and the service-oriented interface protocol supports Nudm, Nudr
PCF	Support access to user information related to policy decisions in database storage (UDR), binding mechanism, flow monitoring and reporting mechanism, QoS control, gate control function, business monitoring and control function, flow-oriented control function; Interface supports Rx, N7, N15
UPF	Support PDU session management function, manage PDU session information, support multiple SMF control UPF, switch based on Xn interface, switch based on N2 interface, session level (APN-AMBR, TDF session UL and DL bit rate, or UL and PDN connection DL rate), bearer level (GBR, MBR carried by GBR), QoS Flow level (for 5GC), service data flow (SDF) or application, support upstream and downstream traffic classifiers and merge functions; The interface supports N3, N4, N9, N6, and the service-oriented interface protocol supports GTP-U, PFCP.
NRF	Supports service discovery function, maintains NF profile and available NF instances.
NSSF	The NSSF can be used by the AMF (Core Access and Mobility Management Function) to assist with the selection of the Network Slice instances that will serve a particular device.

Name	Function
NEF	NEF, located between the 5G core network and external third-party application functionaries (and possibly some internal AFs), is responsible for managing the external open network data, and all external applications that want to access the internal data of the 5G core must pass through the NEF

1.2 Highlight features

1.2.1 Virtualization

Software and hardware are decoupled through virtualization. The IPLOOK 5GC software can be deployed quickly and operate on universal hardware devices of the X86 COTS server or VM/container based virtual platform.

1.2.2 Carrier-grade High Availability

The IPLOOK 5GC hardware resources are virtualized to many VMs. When the IPLOOK 5GC needs to increase its processing capability, more VMs can be installed.
The IPLOOK 5GC supports redundancy and disaster recovery of components and NEs. NEs can be deployed in the entire resource pool through distributed deployment of VMs to enhance system reliability.
The IPLOOK 5GC supports smooth evolution and system migration through online patches and application updates.

1.2.3 Multi-NE Deployment

IPLOOK provides ALL-IN-ONE design compact 5GC solution, all NEs like AMF,SMF,AUSF,UDM,UPF, PCF and web management functions are in a single server. It also supports Nchf for external billing.
Compact 5GC specification:
5000 UEs, 50 eNBs, up to 6Gbps

1.2.4 Open Interfaces and Flexible Network Architecture

The 5GC system provides a series of products and open standard interfaces.

The IPLOOK 5GC supports multiple types of VIM/CMS cloud management systems, multiple types of Hypervisors, and multiple types of orchestrators. It can be configured flexibly based the network requirements.

1.2.5 Sophisticated Operation and Maintenance System

The IPLOOK 5GC performs daily maintenance and management through the unified EMS .
The IPLOOK 5GC functions can be maintained on the local O&M and in the upper-layer EMS.
The features are as follows:

- The O&M uses the B/S structure, and the EMS uses the C/S structure, ensuring a desirable networking capability and expansion of the operation and maintenance system.
- Provides remote and local access to the system so that both local and remote operation and maintenance can be implemented. Maintenance operations can be performed on the entire system and each specified NE.
- Multi-level permission mechanism to ensure system security.
- The IPLOOK 5GC has the dynamic management, preventive maintenance, MML navigation, tracing tool (including signaling tracing and failure observation), alarm management, and performance management functions. With these functions, the system provides multiple operation and maintenance methods precisely, reliably, practicably and conveniently. In addition, more functions can be added as needed.
- The EMS system provides friendly management interfaces, various functions and flexible networking. Multiple NEs can be managed in a centralized way.

1.2.6 NFV Performance Optimization Techniques

Network Function Virtualization (NFV) is a core structural change in the way telecommunication infrastructure gets deployed. This in turn will bring significant changes in the way that applications are delivered to service providers. NFV will bring cost efficiencies, time-to-market improvements and innovation to the telecommunication industry infrastructure and applications. NFV will achieve this through disaggregation of the traditional roles and technology involved in telecommunications applications.
Performance, especially the user plane performance using COTS has always been a concern for service providers and equipment vendors alike. IPLOOK's 5GC address the issue by applying the following performance optimization techniques to the user plane software processing module.
Combine the Single Root I/O Virtualization (SR-IOV) with Intel's Data Plane Development Kit (DPDK) techniques to enhance the performance.
Apply Open vSwitch (OVS) on enhanced Intel's DPDK (By IPLOOK) to further enhance the data processing performance.

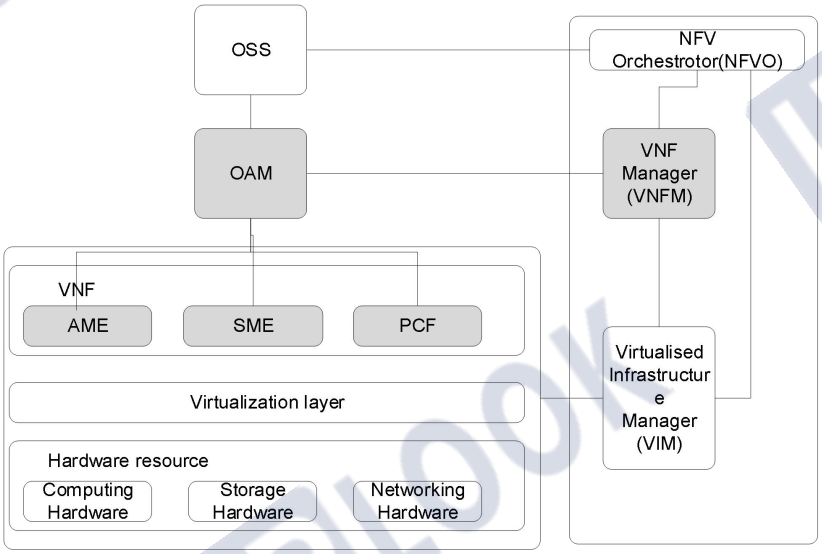
In addition, by using specific 10G, 40G or 100G NIC from Intel, the performance can be further enhanced.

2 System architecture

2.1 IPLOOK 5GC in the NFVI

IPLOOK 5GC is divided into three levels: HW level, virtualization level (cloud management platform and virtualization technology) and service level..

Figure 2 IPLOOK 5GC System Architecture



For a description of the architecture of the IPLOOK 5GC, refer to Table 2.

Table 2 IPLOOK 5GC System Architecture Descriptions

Node	**Description**
OAM	Comprehensive service operation and management platform, which provides various functions such as network management , system management and daily maintenance and management for MME.
NFVI	Network functions virtualization infrastructure, which refers to physical resources. The NFVI is provided and managed by the cloud platform.

Node	Description
Hypervisor	Arranges and manages NFV resources (infrastructure and applications) in the network, and deploys the NFV service on the NFVI.
Hardware	Includes computer hardware, storage hardware, and network hardware.
NFVO	Arranges and manages network services, virtualization resources, and physical resources in the network.
VNFM	Manages the MME lifecycle.
VIM/CMS	Management module of the NFVI, which is the VIM in the ETSI NFV and the CMS in the CCSA. • The VIM/CMS is a system managing virtual infrastructure, managing and monitoring infrastructure-layer hardware resources and virtualization resources, monitoring and reporting alarms, and providing virtual resource pools for upper-layer applications. • The VIM/CMS are operation interfaces providing virtual resources related to the VNF for the NFVO and VNFM. • The VIM/CMS is a cloud platform management function provided by the cloud platform. General applications include TECS, VmWare, and Openstack.

3 Functionality

3.1 AMF

3.1.1Basic function

3.1.1.1 Mobility management

3.1.1.1.1 Definition

The mobility management function controls the access of UE (User Equipment) in the 5G network and tracks the current location information of UE (TA/TA List, etc.) through the processes of registration, service request, switching, AN release, DE-registration, etc., and ensures the continuity of UE services.

3.1.1.1.2 Dependencies

UE	RAN	AMF	SMF	AUSF	UDM	PCF	NSSF	UPF
√	√	√	√	√	√	√	√	√

3.1.1.1.3 Descriptions of function parameters

Category	Parameters
Mobility Management Timer Parameters	T3550 = Register to accept timer(s)
	N3550=Register to accept time out retransmissions(times)

	T3560=Safety mode timer(s)
	N3560=safe mode timeout retransmission times(times)
	T3570=Authentication timer(s)
	N3570 = number of times the authentication timer retransmits (times)
	T3513 = Paging timer(s)
	N3513=Paging timeout retransmission times(times)
	T3522 = Network initiated de-registration timer(s)
	N3522=network initiated de-registration timeout retransmission times(times)
	T3555 = UE configuration update timer(s)
	N3555 = number of UE configuration update retransmissions (times)
	T3512 = Periodic registration update timer (min)
	MobileReachableTimer=UE Reachability Timer(min)
	ImplicitDeregistrationTimer=implicit de-registration timer (min)
Tracking area list parameters	TALISTID=tracking area list label
	TAI = Tracking Area Identification

3.1.1.1.4 Principle

The mobility management function is mainly implemented through processes such as registration, service request, switching, AN release, and de-registration. These processes ensure the timely update of UE location information in the relevant network entities when the UE is mobile.To obtain 5G network services, the UE first needs to initiate a registration process with the network side, which can save the UE's contextual information, location information and some network protocol parameters. After the registration process is completed, the UE can carry out other business processes. Initiated to release the RRC connection on the wireless side and the UE turns to idle state, which saves the network signaling and wireless side resources. If the UE has data to send to the network side or the network side has data to send downward, the service request process shall be initiated to restore the connection between the UE and the network side before the data transmission service. If the UE moves its position from one (R)AN to another (R)AN, the (R)AN will trigger the Handover process to switch the UE to the (R)AN with strong signal to continue the service according to the signal strength. If the UE wants to log off from a network and no longer receive services from this network, it can initiate a de-registration process to stop its services in this network. The following describes the main application scenarios of mobility management related processes.

• Registration process: When the UE needs to access the network to receive the service, the UE performs the initial registration process; when the UE moves out of the originally registered area, it performs the mobility registration update; when the periodic registration update of the idle state UE times out, the UE initiates the periodic registration update process.

• De-registration process: The de-registration process occurs when the UE does not need to continue accessing the network to receive services, or when the UE does not have permission to continue accessing the network.

• AN Release Process: When the UE is inactive for a long time, the (R)AN initiates the AN Rlease process to save network resources after the UE inactivity timer on the (R)AN times out.

• Service request process: The service request process is used to establish a signaling connection between the idle state UE and the AMF, and can also be used for the idle state or connected state UE to activate the user-plane connection of an established PDU session.

• Switching process: The switching process of the connected UE from a source (R)AN node to a target (R)AN node occurs in the 5GS systems, which is divided into Xn-based switching and N2-based switching process according to the existence of Xn interfaces at the source and target (R)AN nodes.

• UE configuration update process: The UE configuration can be updated at any time by the network side by initiating the UE configuration update process.

3.1.1.2 Authentication function

3.1.1.2.1 Definition

5G supports a two-way authentication mechanism between the network and the user. The network side determines the validity of user identity through authentication, enabling legitimate users to use the services provided by the network; the user side ensures the security of access to the network through authentication.

3.1.1.2.2 Dependencies

UE	AMF	AUSF	UDM
√	√	√	√

3.1.1.2.3 Description of function parameters

Category	Parameters
Authentication Quaternion Parameters	RAND
	AUTN
	XRES*
	KAUSF

3.1.1.2.4 Principles

The UE first accesses to the network, data encryption and integrity check failure, etc. The UE and the network side carry out two-way authentication to verify whether each other is safe and legal. 5G authentication function is done by UE, AMF, AUSF and UDM interaction. The authentication is divided into two ways EAP-AKA' and 5G AKA, currently the main way is 5G AKA, the following mainly introduces the principle of 5G AKA authentication.

5G AKA is a variant of EPS AKA, which adds an attribution network authentication process to EPS AKA to prevent fraudulent attacks. Compared with EPS AKA where MME performs the

authentication function, 5G AKA where AMF and AUSF jointly perform the authentication function, AMF is responsible for service network authentication and AUSF is responsible for attribution network authentication. 5G AKA authentication can be divided into three sub-processes: acquiring authentication data, bi-directional authentication of UE and service network, and attribution network authentication.

• Acquisition of forensic data:

The AMF initiates an initial authentication request to the AUSF, and the AUSF determines that the service network is authorized to be used and requests authentication data from the UDM, which decrypts the SUCI to SUPI, selects the authentication method based on the user's contract information, and generates the corresponding authentication vector. 5G AKA authentication can only obtain one authentication vector at a time, and the AUSF will do a derivative transformation and send it to the AMF.

• Two-way authentication of UE and service network:

a. The AMF initiates an authentication request to the UE, carrying authentication parameters such as AUTN, RAND, etc.

b. The UE authenticates the network according to the AUTN, and after the authentication is successful, the authentication response RES* is calculated by RAND and sent to the AMF.

c. The AMF verifies the authentication response returned by the UE to determine whether the service network authentication is passed.

• Attribution Network Forensics:

The AMF sends the authentication response RES* from the UE to the AUSF, which verifies RES* to give the attribution network authentication confirmation result and notifies the AMF. If the authentication is successful, the AUSF sends KSEAF to the AMF so that the AMF can derive subsequent keys.

3.1.1.3 Network user identity confidentiality

3.1.1.3.1 Definition

The user identity confidentiality function means that the AMF assigns a temporary identity 5G-GUTI (5G Globally Unique Temporary UE Identity) to the UE to avoid disclosure of the user's permanent identity.

3.1.1.3.2 Dependencies

UE	AMF
√	√

3.1.1.3.3 Principles

5G-GUTI (5G Globally Unique Temporary UE Identity) is a temporary identity assigned by the AMF to the UE to prevent disclosure of the user's permanent identity SUPI.

5G-GUTI structure

<5G-GUTI>= <GUAMI> <5G-TMSI> where:

• <GUAMI> = <MCC> <MNC> <AMF Region ID> <AMF Set ID> <AMF Pointer> which is a globally unique identifier for AMF.

• <5G-TMSI> is unique in the AMF range.

5G-GUTI allocation process

AMF supports sending 5G-GUTI to UE through registration process, 5G-GUTI redistribution process.

• Registration process: See 5G Network Mobility Management.

• 5G-GUTI redistribution process:

• After the Service Request process is triggered on the network side, the AMF re-assigns the 5G-GUTI to the UE.

• The AMF provides the GUTI reassignment timer function, which is started after the UE enters the connected state. After the timer timeout, if the UE is in the connected state, the AMF redistributes the 5G-GUTI for the UE.

3.1.1.4 NAS signaling encryption and integrity protection

3.1.1.4.1 Definition

The AMF and UE use consensus encryption and integrity protection algorithms to protect the NAS signaling and improve the security of the network.

3.1.1.4.2 Dependencies

UE	AMF
√	√

3.1.1.4.3 Principles

AMF supports three encryption and integrity protection algorithms: AES algorithm, SNOW 3G algorithm and ZUC algorithm.

- AES algorithm: AES is currently the most widely used encryption and integrity algorithm in the world, corresponding algorithms include EEA2 (EPS Encryption)
Algorithm2) and EIA2 (EPS Integrity Algorithm2) with a key length of 128 bits.
- SNOW 3G algorithm: SNOW 3G is a basic 3GPP encryption algorithm and integrity algorithm, the corresponding algorithms include EEA1 (EPS Encryption Algorithm1) and EIA1 (EPS Integrity Algorithm1) with a key length of 128 bits.
- ZUC algorithm: The ZUC algorithm (also known as Zuchon's algorithm) is a sequential cryptographic algorithm designed for hardware. The algorithm outputs a 32-bit sequence of keys for encryption and integrity protection of data based on an initial key of 128 bits and an initial vector of 128 bits.

3.1.1.5 Identification function

3.1.1.5.1 Definition

Identification function means that the network side requests the user to provide an identity (SUCI, PEI, etc.) to identify the real identity of the user.

3.1.1.5.2 Dependencies

UE	AMF
√	√

3.1.1.5.3 Principles

In 5G networks, the user identity includes SUPI, SUCI, 5G-GUTI, and PEI.

• SUPI (Subscription Permanent Identifier): the permanent identity of the UE in the 5G network.

• SUCI (Subscription Concealed Identifier): The UE encrypts the SUPI to generate SUCI. when the UE has no valid 5G-GUTI, it uses SUCI to identify itself.

• 5G-GUTI (5G Globally Unique Temporary UE Identity): the temporary identity assigned to the UE by the AMF.

• PEI (Permanent Equipment Identifier): Permanent equipment identifier of UE in 5G network.

When a UE registers to the network with a 5G-GUTI, the AMF sends an identification request to the UE to obtain the SUCI or PEI of the UE if the first authentication fails, or if the AMF cannot recognize the 5G-GUTI, or if the AMF needs to obtain the PEI of the UE for device identification.

3.1.1.6 User data management

3.1.1.6.1 Definition

User data management refers to the process of inserting, modifying and deleting user data in AMF.

Subscriber data includes subscriber sign-up data in UDM and data dynamically generated during the subscriber's access to the 5GC network.

3.1.1.6.2 Dependencies

UE	AMF	UDM

√	√	

3.1.1.6.3 Principles

This section includes the following:

• User Data

• User data management functions

• User Data Management Process

User Data

• The information that mobile subscribers sign up for in UDM, including subscriber identification SUPI, slice information, etc.

• The data dynamically generated during the process of user access to the 5G network, including the user's current location information, UE security capabilities, etc.

User data management functions

AMF's user data management functions include the following:

1. When a user registers for the first time or when the tracking area is updated to a new AMF, the AMF actively requests the contracted data of the user from the UDM; when the contracted data of the user in the UDM (such as NSSAI) is changed, the UDM will actively insert the updated user data to the AMF to realize the modification of the contracted data on the AMF.

2. When the AMF receives mobile subscriber data, it checks the subscriber's contracted features (service features, etc.), and if some of these features are not supported, it notifies the UDM, which stores the information locally and decides whether to allow the subscriber to access the AMF based on this information.

3. When a user is active in the AMF service area, AMFF keeps the data of that user to reduce the interactive signaling with the UDM. When a user does not register again for a period of time after separation, AMF actively clears the user's data and releases the occupied resources.

User Data Management Process

The processes related to the user data management function are as follows:

• User Data Management

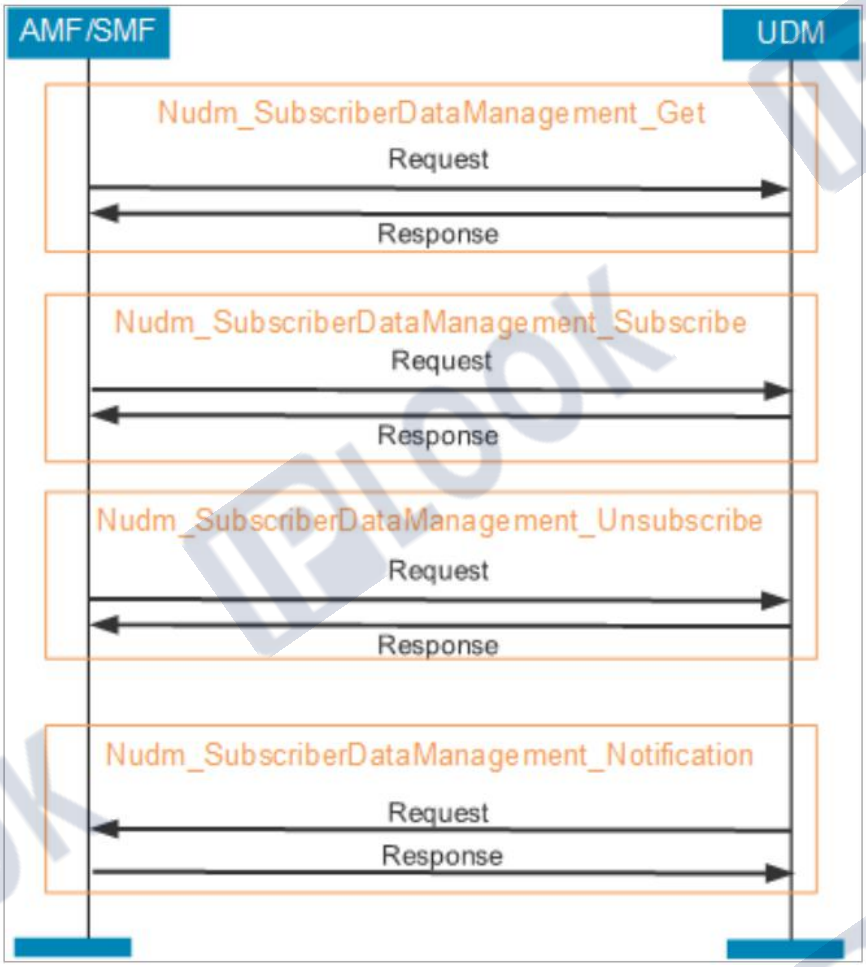


Figure 1 User data management process

As shown in Figure 1-6:

▪ The Nudm_SubscriberDataManagement_Get process between AMF and UDM is mainly used for AMF to obtain user data, such as NSSAI for UE.

▪ The Nudm_SubscriberDataManagement_Subscribe process between AMF and UDM is mainly used for AMF to subscribe to the changes of user data in UDM.

▪ The Nudm_SubscriberDataManagement_Unsubscribe process between AMF and UDM is mainly used for AMF to unsubscribe the user's data changes in UDM.

▪ The Nudm_SubscriberDataManagement_Notification process between AMF and UDM is mainly used for UDM to notify AMF related user data changes that have subscribed to data change notifications.

▪ UE Context Management

Figure 2UE Context Management Flow

As shown in Figure 2:

▪ The Nudm_UEContextManagement_Get process between AMFF and UDM is mainly used for AMF to obtain the registration information of the corresponding AMF of UE from UDM.

▪ The Nudm_UEContextManagement_Update process between AMF and UDM is mainly used to update the registration information of AMF in AMF to UDM.

▪ The Nudm_UEContextManagement_Registration process between AMF and UDM is mainly used for AMF to register its own information to UDM for the presence of UE context related data in UDM.

▪ The Nudm_UEContextManagement_Deregistration process between AMF and UDM is mainly used for AMF to de-register with UDM.

▪ The Nudm_UEContextManagement_DeregistrationNotification process between AMF and UDM is mainly used for UDM to send the result of deregistration to the AMF that initiated the deregistration process.

3.1.1.7 N2 interface

3.1.1.7.1 Definition

The N2 interface is the control plane interface between the (R)AN and AMF in 5G systems. The signaling connection function of the N2 interface provides reliable transmission of wireless network signaling.

3.1.1.7.2 Dependencies

RAN	AMF

√	√

3.1.1.7.3 Principles

N2 interface protocol stack:

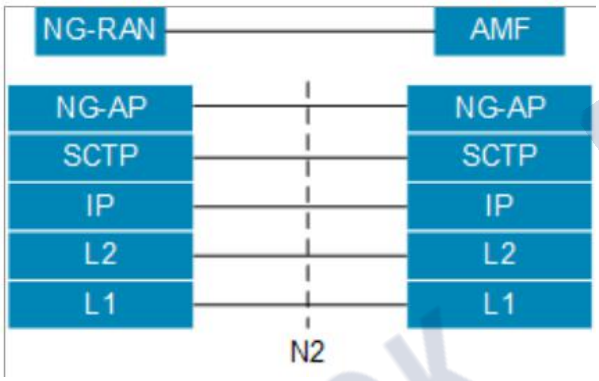


Figure 3N2 interface protocol stack

NG-AP Introduction

The NG-AP consists of several Elementary Procedure EPs, one for each interaction between NG-RAN and AMF, and one initialization message and one response message.

▪ There are response messages that indicate the success or failure of the EP. The following types of responses are returned.

▪ Success

A signaling message explicitly indicates the success of the EP process.

▪ Failure

A signaling message explicitly indicates that the EP process has failed.

The timer timed out and no response message was received.

▪ Success and failure

A single signaling message indicates the success and failure results of several different requests at the same time.

▪ No response message, considered successful by default.

3.1.1.8 Service-oriented interfaces

3.1.1.8.1 Definition

The 5G system architecture is a service-oriented architecture, where functions are provided by different NFs (Network Function), which are independent of each other and can be deployed on demand. The same service of the NF can be invoked by other NFs through the service-based interface of the NF, and the NFs achieve the corresponding functions by invoking each other's service-based interfaces.

3.1.1.8.2 Dependencies

AMF	SMF	AUSF	UDM	PCF	NSSF	NRF
√	√	√	√	√	√	√

3.1.1.8.3 Principles

Serviced interface stack:

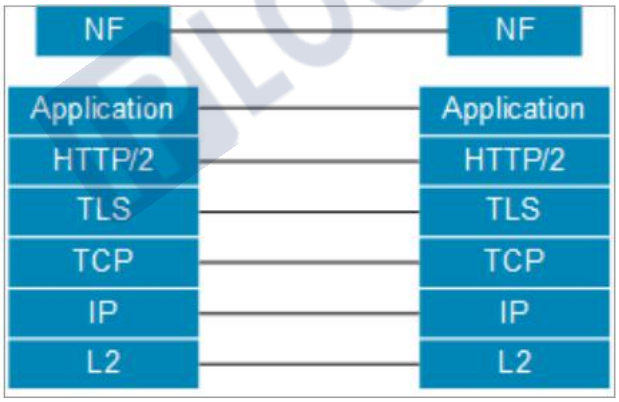


Figure 4 Service-oriented interface protocol stack

The same protocol stack is used between servitized interfaces, the transport layer is unified with HTTP/2 protocol, and the application layer carries different service messages. Because the underlying transport is the same, all servitized interfaces can then be transported on the same bus, supporting the flexibility to bring the business online.

Serviced Interface Interaction Example

The interaction between all NFs in the control plane of 5G core network adopts service-oriented interface, each NF can provide different services, and multiple Service Operations are defined in each service, and the same Service Operation of NF can be invoked by multiple other NFs through service-oriented interface to achieve specific functions. Taking the interaction between AMF and SMF in the PDU session establishment process as an example, we introduce the process of Service Operation of NFs among NFs being invoked by other NFs through the service-oriented interface.

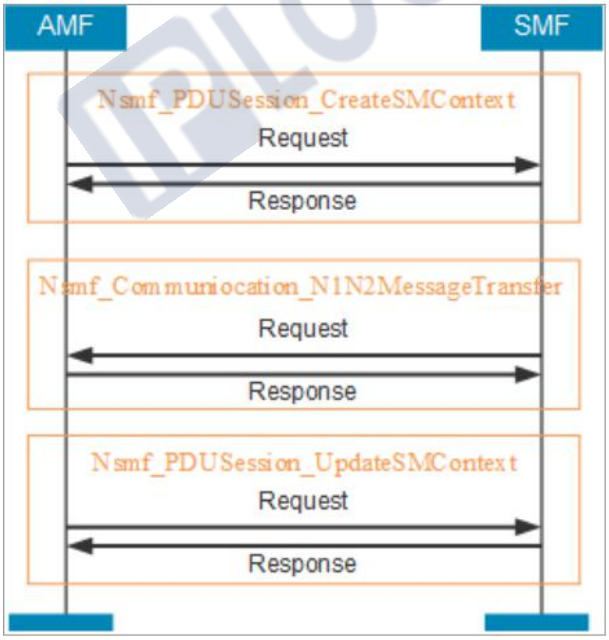


Figure 5 Interaction between AMF and SMF in the PDU session establishment process

Description of the Service Operation during the interaction:

The AMF creates the context by calling the CreateSMContext Service Operation request in the SMF's Nsmf_PDUSession service.

The SMF sends the messages to be transmitted to the RAN and the UE to the AMF by calling the UE Specific N1N2 Message Service Operation (N1N2MessageTransfer) in the Namf_Communication service of the AMF.

The AMF forwards the N2 information received from the RAN to the SMF by calling the Update SM Context Service Operation in the Nsmf_PDUSession service of the SMF.

NFs service the available functions and encapsulate them as Service Operation for other NFs to invoke and achieve the corresponding functions. The servitized interface protocol stack is consistent, and the invocation of Service Operation between NFs uses the servitized interface to send Reqeust, Response, as shown in Figure 5.

AMF and SMF do not need to care about the internal implementation of each other's NFs, nor do they need to make corresponding adaptations due to the internal structure of each other's NFs changing, but only need to call the corresponding Service Operation through the service-oriented interface to achieve the specified functions between NFs. the interface coupling between NFs is low, the definition is flexible, and NFs can be combined on demand according to the functions of the whole network.

3.1.1.9 N26 interface

3.1.1.9.1 Definition

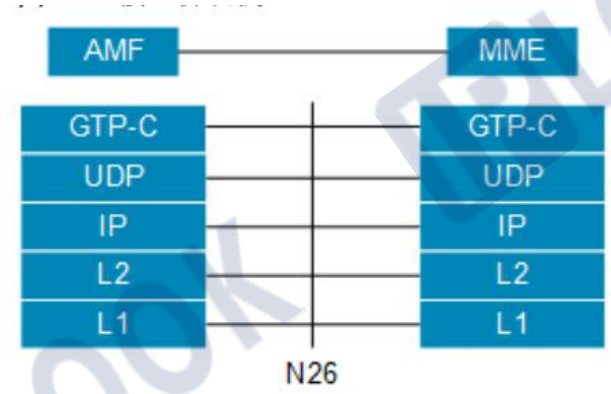
The N26 interface is the interface between the AMF and the MME, providing a signaling message tunnel between the AMF and the MME, and is used to assist in the interoperability between the 5G network and the LTE network.

3.1.1.9.2 Dependencies

AMF	MME
√	√

3.1.1.9.3 Principles

N26 interface protocol stack



3.1.1.10 EPS Fallback

3.1.1.10.1 Definition

This feature means that VoNR (Voice over NR, NR network voice service) is not deployed in the wireless network, and when the UE accesses from the 5G network, it is allowed to register in the IMS domain, but when the UE wants to make a call, it will fall back to the 4G network to make a call via VoLTE. Provides a voice solution for 5G networks without deploying VoNR.

3.1.1.10.2 Dependencies

AMF	SMF	RAN	UE	MME	PGW-U/ UPF	E-UTRAN	PCF
√	√	√	√	√	√	√	√

3.1.1.10.3 Principles

The EPS Fallback process is shown in Figure 6.

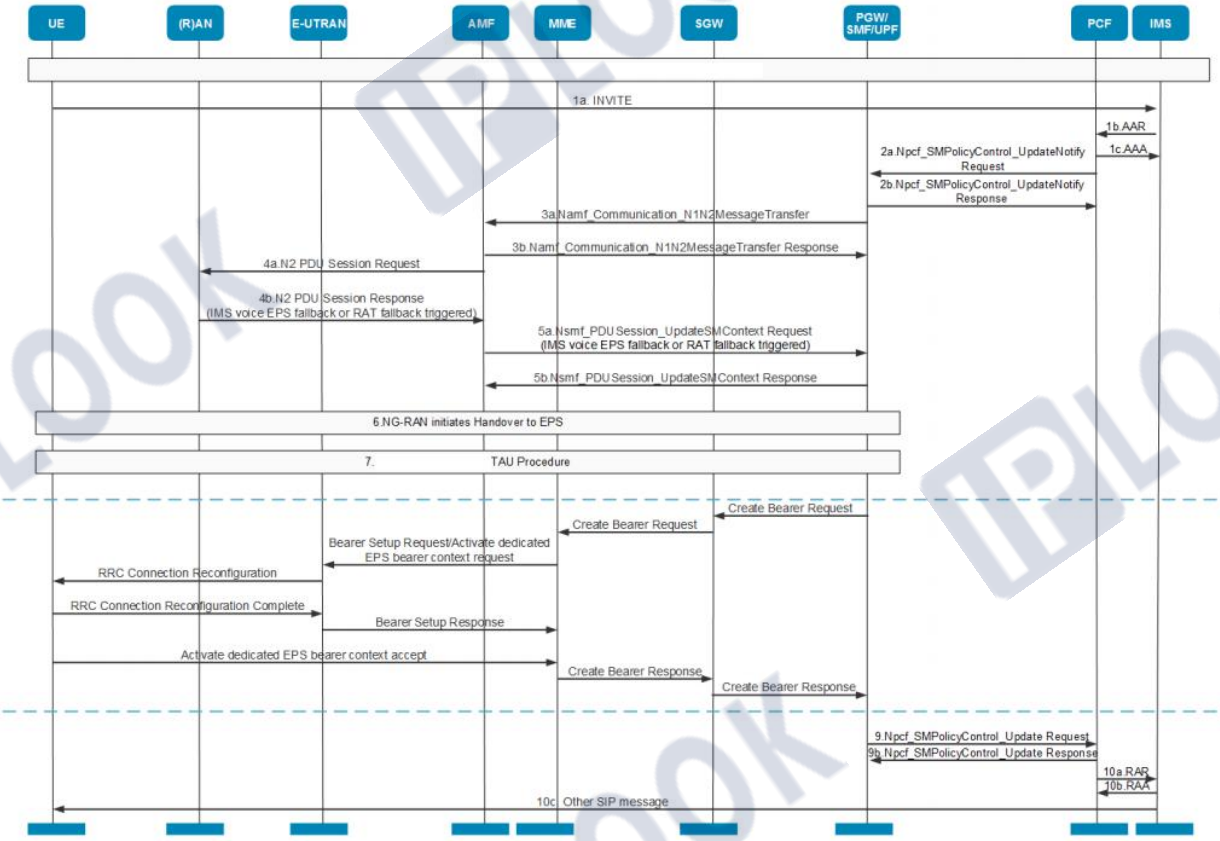


Figure 6EPS Fallback Process

The UE has established an IMS PDU session after attaching to the 5G network and has been successfully registered on the IMS network.

1. the UE initiates the IMS voice service. the UE sends a SIP invite message to the IMS. the IMS sends an AAR message to the PCF. the PCF responds to the AAA message to trigger the process of creating a dedicated QoS Flow.

2. the PCF sends an Npcf_SMPolicyControl_UpdateNotify Request message to the SMF to notify the SMF of the creation of a voice proprietary QoS Flow. the SMF responds with an Npcf_SMPolicyControl_UpdateNotify Response message.

3. the SMF sends Namf_Communication_N1N2MessageTransfer to the AMF, carrying SM-related information in the message. the AMF responds with the Namf_Communication_N1N2MessageTransfer Response message.

4. The AMF sends an N2 Session Request message to the NG-RAN to notify the NG-RAN of the establishment of the voice QoS Flow resource, and the NG-RAN rejects the voice QoS Flow in response to the N2 Session Response message and carries the IMS Voice EPS Fallback or RAT Fallback Triggered reason value.

5. the AMF sends an Nsmf_PDUSession_UpdateSMContext Request to the SMF carrying the IMS Voice EPS Fallback or RAT Fallback Triggered cause value. the SMF responds with the Nsmf_PDUSession_ UpdateSMContext Response message.

6. (R)AN initiates the 5GS to EPS Handover process.

7. the TAU process after Handover.

8. The PGW creates the request based on the cached QoS Flow with QCI=1 and then initiates the IMS voice proprietary bearer creation process after the user has fallen back to the EPS network.

9. PGW sends Npcf_SMPolicyControl_update request message to PCRF/PCF, the message carries IP-CAN-Type, RAT-Type and other information, which are all letter elements in 4G network.

10. the PCF then sends a RAR message to IMS and IMS responds to the RAA message. the IMS network sends a SIP message to the UE and the voice call is normal.

3.1.1.11 IPV4V6 dual stack access

3.1.1.11.1 Definition

This feature supports assigning both IPv4 and IPv6 types of addresses to the UE in the PDU session establishment process, so that the UE can subsequently use IPv4v6 addresses for data transmission and provide IPv4v6 dual-stack access services to users.

3.1.1.11.2 Dependencies

AMF	SMF	RAN	UE	UPF	UDM	PCF
√	√	√	√	√	√	√

3.1.1.11.3 Principles

Dual stack address allocation method

Dual-stack technology is an effective technology for the transition from IPv4 to IPv6. Dual-stack means that the nodes in the network support both IPv4 and IPv6 protocol stacks, and the source node selects different protocol stacks according to the destination node, while the network device selects different protocol stacks for processing and forwarding according to the protocol type of the message. The dual-stack nodes use IPv4 protocol stack when communicating with IPv4 nodes and IPv6 protocol stack when communicating with IPv6 nodes. SMF assigns an IP address to a PDU session when the user establishes that PDU session. For terminals that support IPv4v6 dual-stack, UNC supports assigning IPv4v6 dual-stack addresses to them. Depending on whether the assigned address is a static address obtained from the

UDM or an address dynamically assigned by the SMF, the way the SMF assigns IPv4v6 dual-stack addresses can be divided into

The three types of static allocation, dynamic allocation and mixed allocation are as follows.

▪ Static distribution method

The user signs up for a static IPv4v6 dual-stack IP address, and the SMF obtains this signing information from the UDM to pass to the UE and UPF.

▪ Dynamic allocation method

The SMF assigns IPv4v6 dual-stack IP addresses to subscribers from the locally configured IP address pool based on the PDU session type carried by the subscriber and the signed or PDU session type obtained from the UDM.

▪ mixed distribution method, as shown in Table 1.

User signed up for a static IPV4 address	User signed up for a static IPV6 address	Mixed IPV4V6 dual-stack IP addresses assigned by SMF
Yes	No	Static IPV4+Dynamic IPV6
No	Yes	Dynamic IPV4 + Static IPV6

Table 1 Hybrid IPv4v6 dual-stack IP address allocation method

3.1.1.12 AMF Pool

3.1.1.12.1 Definition

AMF Pool refers to multiple AMFs serving the same wireless area at the same time, and the AMFs in the Pool are connected to all gNodeBs in the corresponding area. gNodeBs detect the

device status (availability) of AMFs and obtain the load weight of AMFs, and adjust the load balancing policy of the Pool in time according to the device status and load weight. The load balancing policy of the pool is adjusted in time according to the device status and load weight.

3.1.1.12.2 Dependencies

AMF
√

3.1.1.12.3 Principles

AMF Pool As shown in Figure 1, a group of AMFs (AMF1~AMF3) can form an AMF Pool. when a subscriber moves within an AMF Pool area, it can be continuously served by a specific AMF, and as long as the subscriber is active within the Pool area, inter-AMF re-registration and switching within the area will not occur. This results in a significant reduction in Inter AMF Registration and Handover processes generated when a user is active, thereby reducing signaling between AMFs and AMFs, and between AMFs and UDMs, and reducing network load. The MCC, MNC, AMF Region ID and AMF Set ID in GUAMI uniquely identify an AMF Set, so when deploying an AMF Pool, the same PLMN, AMF Region ID and AMF Set ID should be configured for all AMFs in the Pool. Therefore, when deploying an AMF Pool, the same PLMN, AMF Region ID and AMF Set ID should be configured for the AMFs in the Pool.

3.1.1.13 DNN correction

3.1.1.13.1 Definition

During the PDU session establishment, the AMF selects the SMF and the AMF compares the network slice and DNN requested by the user with the contracted data. If the UE carries a DNN in the request message, the AMF compares the requested DNN with the contracted data, and if the DNN requested by the user and the contracted DNN under the selected network slice do not match, the AMF rejects the user's activation request. If the UE does not carry a DNN in the request message and there is no default DNN under the selected network slice, the AMF rejects the user's activation request. Therefore, UNC provides the function of DNN correction to correct the DNN requested by the user to the DNN locally configured by the AMF that matches the contracted data, thus reducing the occurrence of PDU session establishment failure.

3.1.1.13.2 Dependencies

UE	AMF	UDM
√	√	√

3.1.1.13.3 Principles

In 5G networks, UDM stores the latest subscriber signup data, and when a PDU session is established, AMF and SMF need to perform signup data matching to determine the legitimacy of access to the network. signup data matching on the AMF side includes AMF matching the

subscriber requested network slice with the signed network slice, and matching the subscriber requested DNN information with the signed DNN in the selected network slice The AMF side of the AMF matches the user-requested network slices with the contracted network slices. In actual network operation, the DNN information carried by the subscriber may not match the contracted DNN data due to factors such as incorrect subscriber settings, resulting in DNN matching failure and rejection of the subscriber request, which affects the end customer experience. To reduce the occurrence of such problems, UNC introduces the DNN correction feature, which can correct the DNN in the user request information after the contracted DNN matching failure, so as to improve the success rate of PDU session establishment, reduce the configuration requirements of the user's cell phone and enhance the end-customer experience.

3.1.1.14 NSSAI slice selection based on

3.1.1.14.1 Definition

When the UE initiates registration, the AMF determines that if it cannot provide slicing service for the UE, it queries the NSSF to obtain information about the AMF that can provide slicing service, and the NSSF returns the slicing configuration information assigned to the UE at the same time.

3.1.1.14.2 Dependencies

UE	AMF	UDM	NSSF

√	√	√	√

3.1.1.14.3 Description of function parameters

Category	Parameters
Slicing type parameters	S-NSSAI
	NSSAI
	Subscribed S-NSSAI
	Configured NSSAI
	Allowed NSSAI
	Requested NSSAI

3.1.1.14.4 Principles

In the registration process, when the initial AMF cannot provide slicing service for the UE, it is necessary to use the requested NSSAI and contracted S-NSSAI information to query the NSSF to obtain an AMF that can provide service for the UE, and the NSSF supports the completion of the slicing selection function based on the slicing information requested and contracted by the user.

▪ The AMF locally configures the network element information of the NSSF, including the priority (priority), weight (capacity), IP, Port, and protocol version of each service provided by the NSSF.

▪ The NSSF needs to pre-configure the list of slices supported by each TAI of the managed AMF and the slice configuration information supported by the PLMN of this network for slice selection query, and the NSSF returns the AMF SET or candidate AMF that can provide the service and the slice configuration information issued to the UE for decision.

▪ When the UE initiates registration, the AMF judges that if slicing service is provided for the UE, it queries the NSSF to obtain the AMF that can provide slicing service, and the NSSF returns the slicing configuration information assigned for the UE at the same time.

3.1.2 Optional Functionalities

3.1.2.1 Support NRF basic functions

3.1.2.1.1 Definition

The 5GC network adopts a service-oriented architecture, abstracting the control plane functions into multiple independent Network Functions (hereinafter referred to as NFs), each of which supports multiple services (hereinafter referred to as NFSs). AMF supports initiating registration, de-registration, NF status subscription, and receiving status notifications from NRF.

3.1.2.1.2 Dependencies

AMF	NRF
√	√

3.1.2.1.3 Principles

AMF registration process to NRF

Figure 7 AMF registration process to NRF

1. The AMF sends Nnrf_NFManagement_NFRegister_Request message to the NRF requesting registration, carrying the NF/NFS Profile information associated with this AMF (nfInstanceID, nfType, nfStatus, nfServices, heartBeatTimer, plmnList, sNssais, etc., where nfInstanceID uniquely identifies the NF).

2. The NRF processes the registration request from AMF and performs the corresponding checks, and saves the NF/NFS Profile record after passing.

3. The NRF returns the Nnrf_NFManagement_NFRegister_Response message to the AMF.

NF/NFS access authorization control

- NF/NFS can have a corresponding access authorization policy for authorization judgment and control during NF/NFS discovery. When the NF/NFS adopts access authorization control, access to NF/NFS within the authorization range is allowed; if access authorization control is not adopted, the NF/NFS can be accessed by any registered NF/NFS.
- The access authorization control policy can be carried during NF registration or NF/NFS update, and the access authorization control policy can be configured on the NRF.

AMF to NRF to go to the registration process

Figure 8 AMF to NRF de-registration process

1. AMF sends Nnrf_NFManagement_NFDeregister_Request message to NRF to request to register, only need to carry this AMF has generated nfInstanceID, do not need to carry NF/NFS Profile.

2. The NRF receives the de-registration request and finds the record corresponding to the nfInstanceID and deletes the AMF and all associated NFS profiles.

3. The NRF returns the Nnrf_NFManagement_NFDeregister_Response response to this AMF.

AMF Update Process

In 5GC networks, NRF is responsible for the automated management of all NF/NFS, which includes NF/NFS updates, served by Nnrf_NFManagement.

▪ When the used NF/NFS information changes (such as services or capabilities, etc.), it needs to be updated to the NRF. The NRF update includes a full update and partial updates in both ways.

▪ NF full volume update process

The NF full update process is different from the NF registration process. The difference between the NF full update process and the NF registration process is that NRF first recognizes that

nfInstanceID already exists in NRF, considers it to be a full update of NF, and replaces all the attributes of nfInstanceID with all the attribute information of NF.

- NF section update process

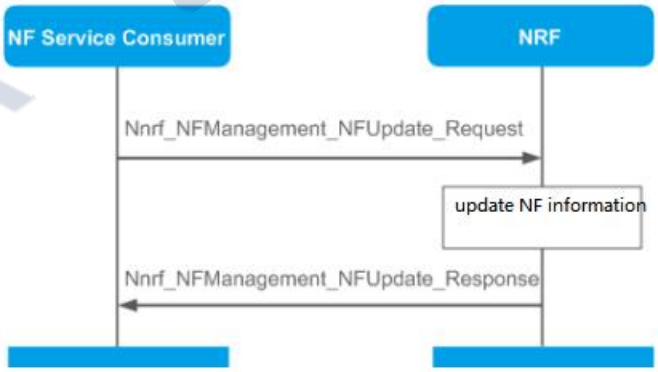


Figure 9 AMF section update process

1. The registered AMF sends the Nnrf_NFManagement_NFUpdate_Request message to the NRF requesting update information, and the request message carries only the NF/NFS Profile to be updated and the update operation (add/remove/replace) for these attribute information.

2. NRF handles AMF update requests.

3. the NRF sends the Nnrf_NFManagement_NFUpdate_Response message to the AMF.

- AMFs that have been registered with the NRF send messages to the NRF periodically through the NF update process to inform the AMF of its valid status (later called heartbeat). The heartbeat period can be set by command and returned to the AMF by the NRF upon successful registration of the AMF. when the NRF detects that the AMF has not sent a heartbeat message within a number of heartbeat periods (configurable), the NRF sets the AMF status to SUSPENDED and this AMF and the corresponding NFS are no longer discovered by other NFs.

NF Heartbeat Process

The NRF updates the heartbeat cycle of the registered NF by carrying the new heartbeat cycle (configured by command) in the heartbeat response message of the NF, the process is the same as the NF part update process.

1. The registered NF sends the Nnrf_NFManagement_NFUpdate_Request message to the NRF, the request message contains the NF status and the corresponding replacement operation.
2. NRF handles NF update requests (heartbeat messages).
3. the NRF sends the Nnrf_NFManagement_NFUpdate_Response message to the NF.

AMF Status Subscription Process

Figure 10 AMF initiates status subscription process to NRF

1. AMF sends Nnrf_NFManagement_NFStatusSubscribe_Request message to NRF to request subscription to status information of other NF/NFS instances, and the request message carries information such as subscription conditions, subscription events, subscription duration, and subscription notification conditions.
2. The NRF sends the Nnrf_NFManagement_NFStatusSubscribe_Response response to the AMF, carrying the subscription ID that uniquely identifies this subscription created by the NRF.

3.1.2.2 NF Certification

3.1.2.2.1 Definition

For security reasons, NFs need to obtain authorization when requesting a certain service to prevent and reduce the risk of elevation of authority. 5GC network adopts Oauth2.0 dynamic Token authorization for the service-based interface between NFs (Token can be understood as a short-term token used by NFs to request access to a service, and the required service can be obtained when and only when the token is in hand), and the authorization method is After the NF first applies for service discovery, it applies for Access Token to the NRF, and then carries this Access Token for subsequent corresponding service requests, and the NF service provider first authenticates the NF service consumer to ensure the integrity and legality of the Access Token before providing the service. When the Access Token expires or the requested service changes, the NF requestor will apply for a new Access Token.

3.1.2.2.2 Dependencies

AMF	NRF	SMF	UDM	AUSF	NSSF	PCF
√	√	√	√	√	√	√

3.1.2.2.3 Principles

In the Token authorization mechanism, the NF service consumer is the client, the NF service provider is the resource server, and the NRF is the NF authorization server, which serves as the

centralized control point for the authority management of Token and provides Access Token Nnrf_AccessToken provision service to the NF service consumer.

Access Token Application Process

When NF service consumers request a service, they first request an Access Token from the NRF.

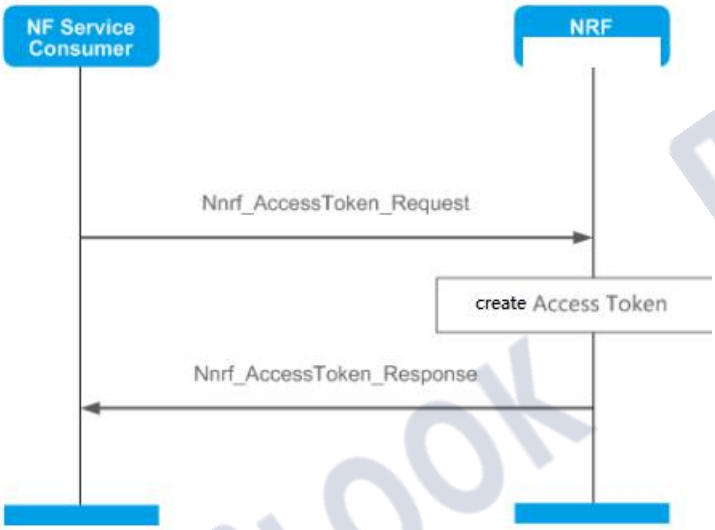


Figure 11Access Token application process

1. The NF service consumer initiates a Nnrf_AccessToken_Request request to the NRF with attributes such as grant_type, nfInstanceId and scope.

2. NRF generates Access Token based on the nfInstanceId of NF service consumer and NF service provider's NF/NFS access authorization control, etc. The Access Token contains AccessTokenClaims InstanceID of NF service consumer, NF service provider and NRF, the name of NFS that can be Access Token contains AccessTokenClaims (InstanceID of NF service consumer, NF service provider and NRF, NFS name that can be accessed, etc.), Access Token expiration time and NFS name that can be accessed by NF service consumer, etc.

3. The NRF returns the generated Access Token to the NF service consumer via the Nnrf_AccessToken_Response message.

3.1.2.3 Selection of SMF based on contract information

3.1.2.3.1 Definition

UE requests for PDU Session establishment, etc. involve the selection of SMFs. When operators deploy different network grouping scenarios, they can flexibly select the SMF under the corresponding network based on the signing information (snssaisdnn attribute).

3.1.2.3.2 Dependencies

UE	AMF	UDM	NRF	SMF
√	√	√	√	√

3.1.2.3.3 Principles

When establishing a PDU session, the AMF first selects the most suitable SNSSAI and DNN for the UE based on the SNSSAI and DNN that the UE may carry and the Smf Selection Data contracted by the UDM, and then sends a Nnrf_Discovery_Request to the NRF based on the selected SNSSAI and DNN The NRF returns the corresponding SMFs to the AMF through the Nnrf_Discovery'_Response message, and the AMF selects the best SMF from the returned SMF list to serve the UE based on load balancing, etc.

3.1.2.4 AMF redirection

3.1.2.4.1 Definition

The initial registered AMF selected by the base station for the UE is changed from the final registered AMF.

3.1.2.4.2 Dependencies

AMF	NSSF	NRF
√	√	√

3.1.2.4.3 Principles

The UE is registered on power on, the base station selects the initial AMF for the UE, the registration request message carries the Requested NSSAI which is not supported by the AMF, the initial AMF sends Nnssf_NSSelection_Get request to the NSSF, the NSSF receives the request and selects the Allowed NSSAI and Configured NSSAI for the UE, and returns an AMF collection or the NF InstanceID of the AMF. According to the returned AMF collection or NF InstanceID, there are two types of redirection, i.e., direct redirection between AMFs and redirection via AN.

1. Direct redirection between AMFs

The NSSF returns the NF InstanceID of the target AMF to the initial AMF, and the initial AMF initiates a Nnrf_Discovery_Request to the NRF to request the AMF instance corresponding to the NF InstanceID, and the initial AMF forwards the Registration Request message carried by

the UE to the target AMF through the Namf_Communication_N1MessageNotify service. After forwarding the Registration Request message carried by the UE to the target AMF, the registration of the UE is completed by the target AMF.

2. Redirected by AN

The NSSF returns the target AMF set containing AMF RegionID and AMF SetID to the initial AMF, and the initial AMF forwards the Registration Request message through the N2 Reroute NAS Message carrying the AMF RegionID and AMF SetID to the RAN node to reroute to the The initial AMF carries the AMF RegionID and AMF SetID through the N2 Reroute NAS Message and forwards the Registration Request message to the RAN node for rerouting to the target AMF, which completes the registration of the UE.

3.1.2.5 SBI interface encryption

3.1.2.5.1 Definition

The SBI secure transport layer uses TLS (Transport Layer Security) protocol to provide data encryption and integrity protection.

3.1.2.5.2 Dependencies

AMF	UDM	AUSF	SMF	PCF	NSSF	NRF
√	√	√	√	√	√	√

3.1.2.5.3 Principles

The encryption method and key used for SBI interface encryption is negotiated through the TLS handshake process, as shown in Figure 12.

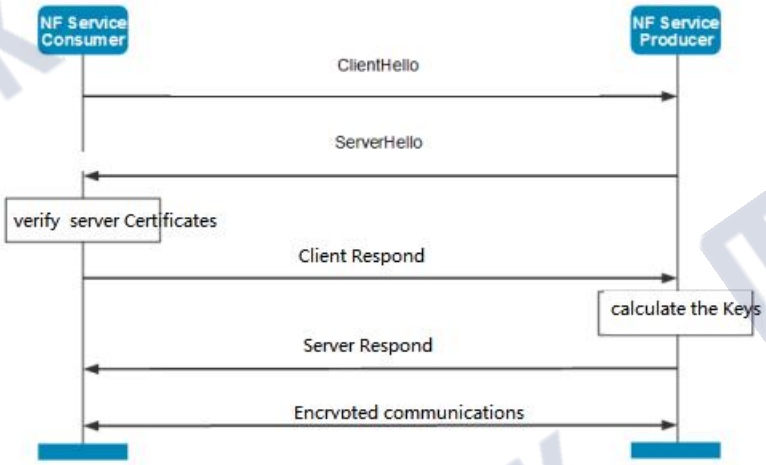


Figure 12 TLS handshake flow

The NF Service consumer acts as the client and the NF Service producer acts as the server.

1. The client sends a ClientHello message to the server, i.e., an encrypted communication request, and enters the TLS handshake process. The ClientHello message contains the TLS protocol version supported by the client, the encryption method, the compression method, and the random number generated by the client.

2. The server receives the request and returns a ServerHello message containing confirmation of the TLS protocol version and encryption method used, a random number generated by the server, and the server certificate. If the server needs to confirm the identity of the client, it will also include a client certificate request. If the client does not match the version of the TLS protocol supported by the server, the server rejects the communication.

3. After the client receives the server response, it verifies the server certificate. If the server certificate is not issued by a trusted authority, or if the certificate has expired, the client rejects

the communication. If the server certificate is validated, the client obtains the server's public key from the server certificate and generates a random number. The random number is encrypted by the server's public key to prevent eavesdropping. Thereafter, the client calculates the "session key" for subsequent communication based on the three random numbers in the above step and the consensus encryption method.

4. The client sends a random number, an encoding change notification, and a client handshake end notification to the server. The encoding change notification indicates that all subsequent messages will be sent encrypted with the mutually agreed encryption method and key. If the server requests a client certificate, then the client also sends information about the certificate. 5. After the server receives the response from the client, it calculates the encryption method used for subsequent communications based on the three random numbers and the consensus encryption method in the above steps.

3.1.2.6 IMEI check

3.1.2.6.1 Definition

IMEI check feature refers to the service that AMF obtains IMEI information of UE during UE registration process and sends it to 5G-EIR for legality check. After receiving the check result returned by the 5G-EIR, it decides whether to allow UE access based on the result returned by the EIR. The IMEI check confirms the legality of the terminal, thus prohibiting illegal terminals from entering the network.

3.1.2.6.2 Dependencies

UE	AMF	5G-EIR

√	√	√

3.1.2.6.3 Principles

IMEI (International Mobile Equipment Identity) is used to uniquely identify a user's terminal. IMEI legality information is stored in the 5G-EIR, which has three lists: white list, grey list and black list. list).

The AMF obtains IMEI information of the terminal by sending Identity Request or Security Mode Command message to the terminal and confirms the legitimacy of the terminal to the 5G-EIR through Check IMEI process. When the 5G-EIR rejects the user's access, the AMF will deny the user's access to the network.

3.2 SMF

3.2.1 Basic functionalities

3.2.1.1 PDU session establishment

3.2.1.1 .1 Description

The SMF session management function provides the UE with the ability to access the packet data network over the 5G network and enjoy the data services provided by the Internet or enterprise network. Session management includes business processes such as the creation, update and deletion of PDU Sessions.

A PDU session is the process of communication between a user terminal UE and a data network DN. a PDU session is established and a data transmission channel from the UE to the DN is established.

3.2.1.1 .2 service scenarios

- UE needs to interact with external networks for business
- UE switching between 3GPP and non-3GPP access methods
- UE switches from 4G PDN link to 5G PDU session
- Network-side initiated PDU session creation (triggered when the terminal is in paging)

3.2.1.1 .3 PDU session processing

1．SMF receives and processes AMF PDU session creation requests

Main fields for establishing a session request.

- PDU Session ID
- PDU Session Type
- Session Access Type
- DNN
- Location information
- Slicing information
- SSC mode requested

- 5G SM Capability
- UE maximum data rate

2．SMF checks the UE's request and the UE's contracted data in the UDM

The main contracting data related to SMF in the UDM are.

- Allowed PDU session types & default PDU sessions
- Allowed SSC modes and default SSC modes
- QoS information, signed Session-AMBR, default 5QI and default ARP
- Static IP address/prefix
- Contracted User Side Security Policy
- Billing attributes associated with a PDU session
- SMF supports the type of PDU sessions sent by the UE

3．**SMF gets dynamic or local PCC rules**

As long as it includes triggers information, Qos information, billing, triage etc.

4. SMF establishes N4 sessions

SMF selects UPF by UE location, DNN,S-NSSAI, UPF load etc.

Establish connection to UPF, provide data monitoring for this PDU session, reporting rules, CN tunnel information

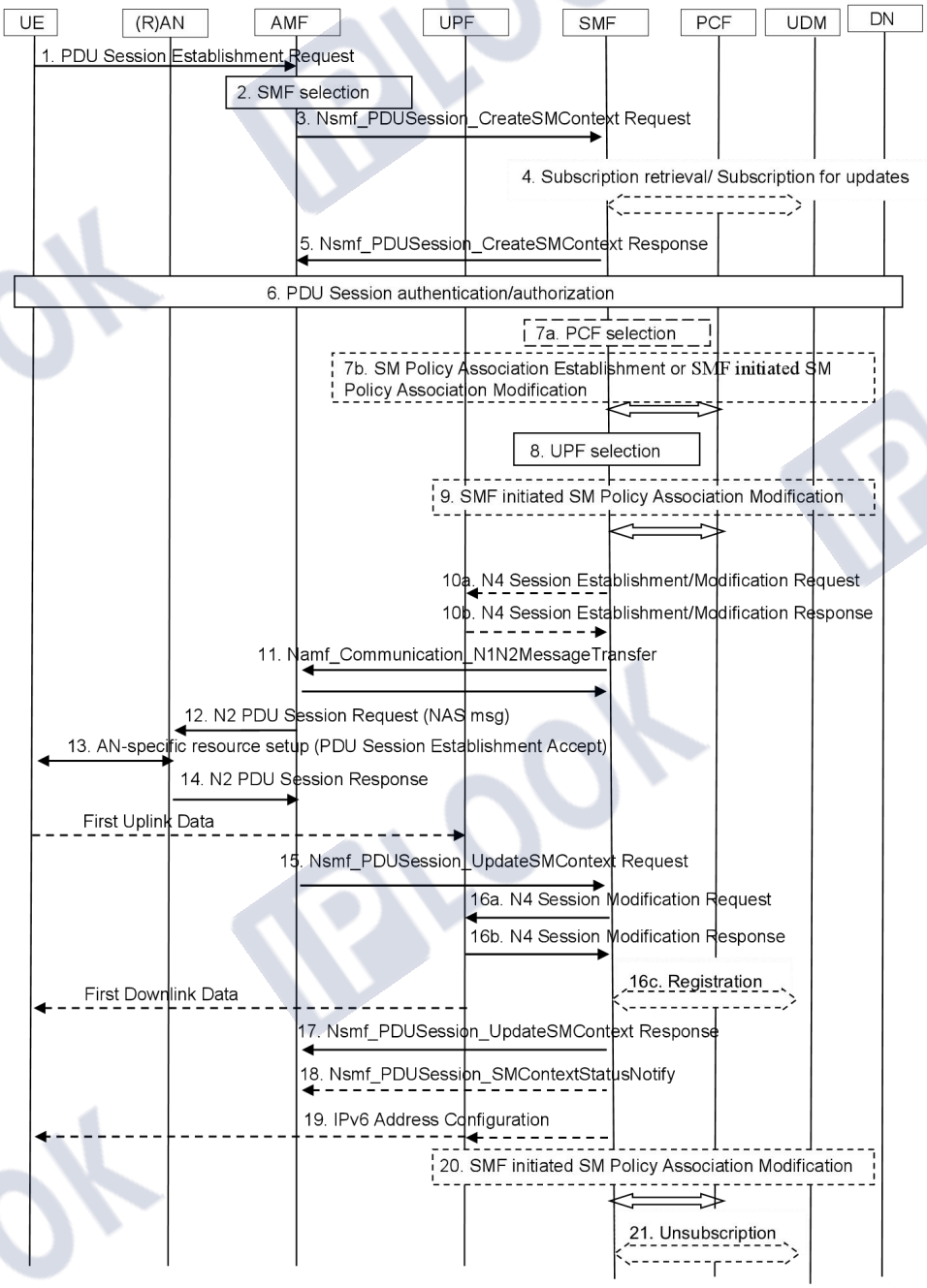
5. SMF transmits N2,N1 information back to the base station and terminal via AMF

- N2 messages contain mainly information about QFI, QosProfile, CN Tunnel, etc.

- N1 Includes Accept responses created by PDU sessions Assigned IP information, etc.

Note: Due to the different terminal behaviour and configuration services, the information included above may vary slightly.

The session creation signalling flow chart is as follows.



PDU creation process description Refer to 3GPP

Note: The service request initiated by the UE is used to establish a signalling link between the idle state UE and the AMF.

3.2.1.2 Session changes

3.2.1.2.1 Description

In scenarios such as changes in UE capacity and changes in QoS parameters, both the UE and the network side can initiate PDU session modification requests.

The following can trigger a PDU session to modify signalling.

- UE initiates a PDU session modification request
- SMF initiates PDU session modification request
- AN initiates a PDU session modification request

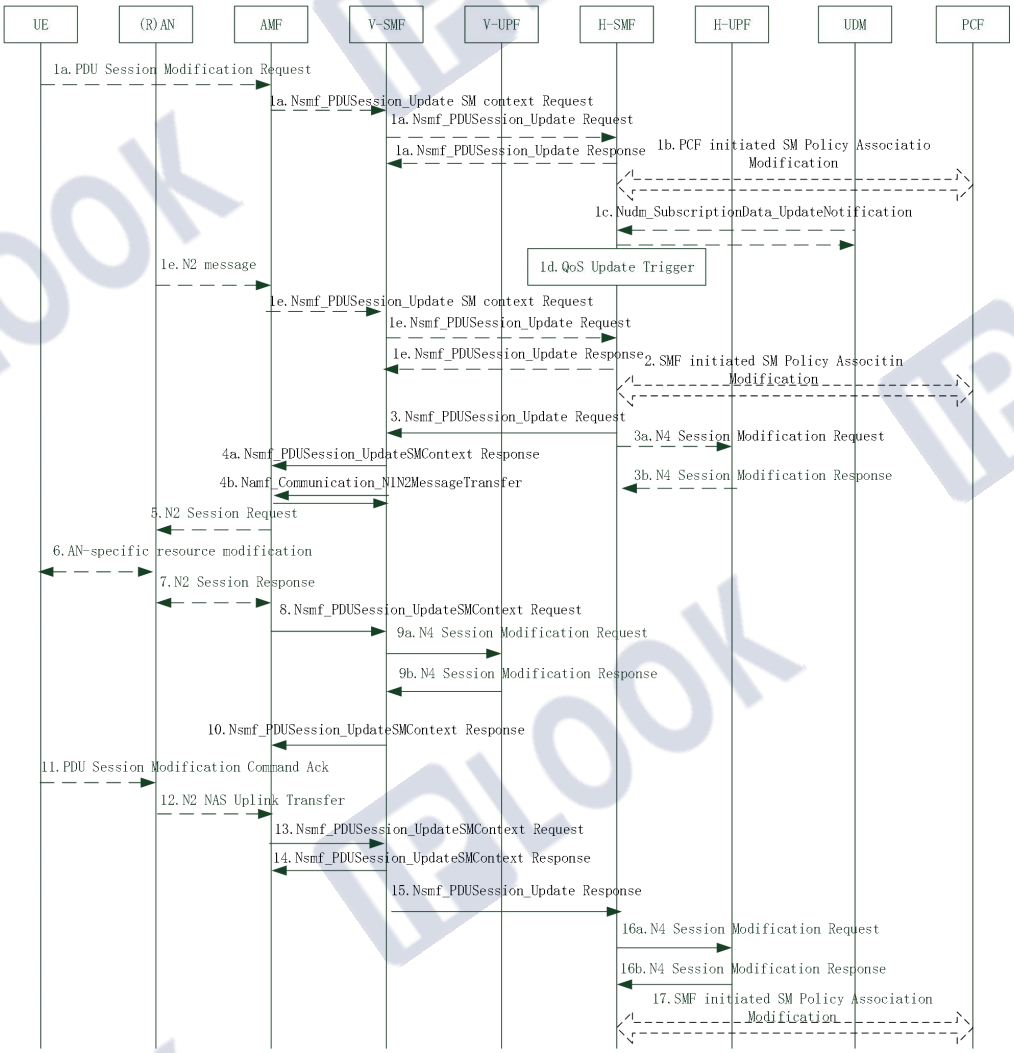
Among the network elements that allow the SMF to initiate PDU session modification requests are.

- UDM SM contracted data generation change triggers SMF to initiate PDU session modification
- PCF policy change triggers SMF to initiate PDU session modification

Related IE:

- nGSM-capability UE-capability
- qos-rules carrier rules
- pdu-session-ID Session ID
- modification Command request command
- Far Action is popular for
- AN TUNNEL
- CN TUNNEL

3.2.1.2.2 PDU session change process.



A description of the process can be found in 3GPP-23502 4.3.3.2

3.2.1.3 Session release

3.2.1.3.1 Description

PDU session release is essentially the release of all resources related to the session.

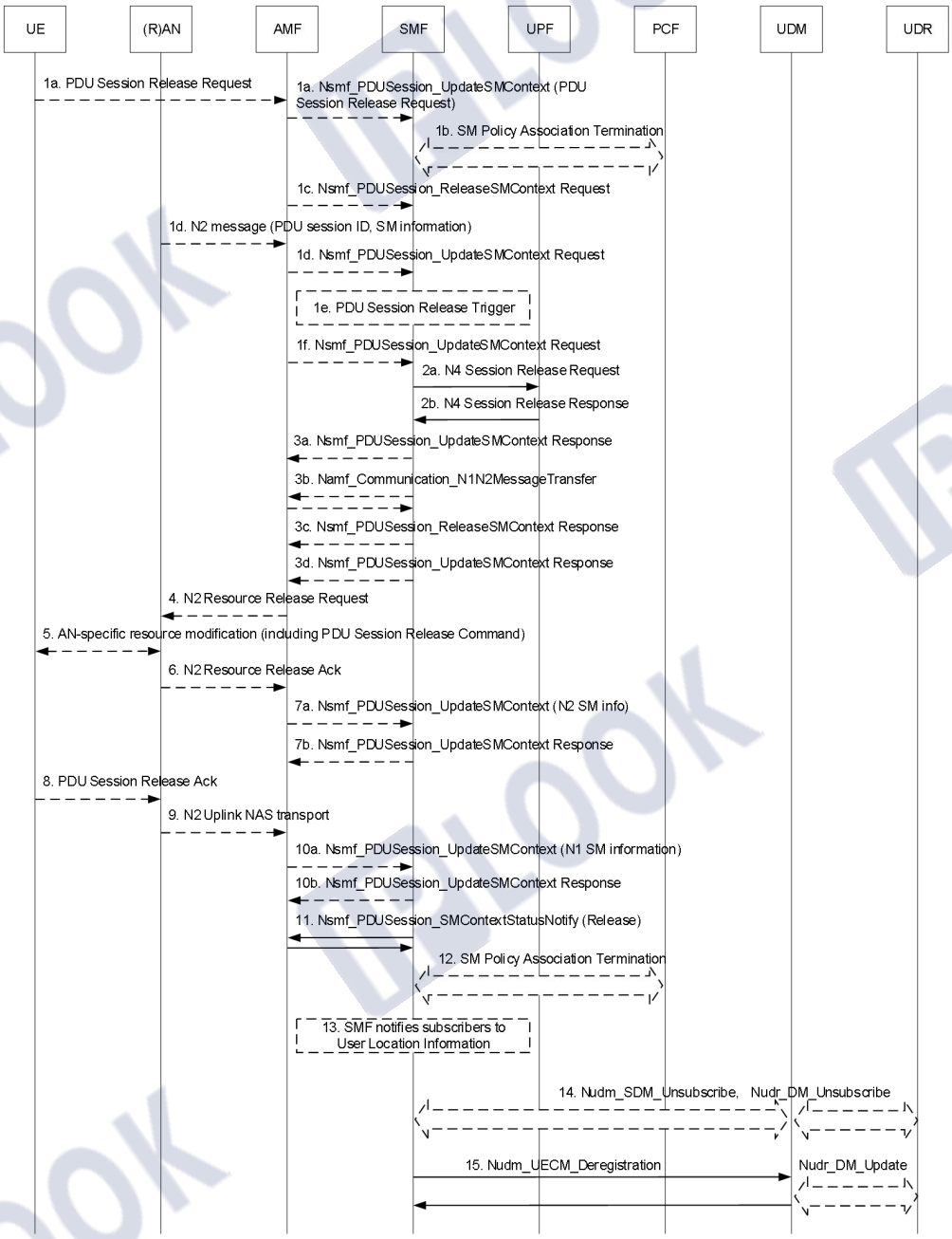
Key resources released by the session.

- IP address and prefix assigned to the PDU
- UPF resources for PDU sessions (N3 N9 N19)
- Access resources used by PDU sessions

The following can trigger a PDU session release request.

- UE initiates a PDU session release request
- SMF initiates PDU session release request
- AMF initiates PDU session release request

The release process is shown in the diagram.



Refer to section 3GPP-23502 4.3.4.2 for process description

3.2.1.3.1 Service scenario

- When the UE no longer needs the business in question
- When the session status of the UE and AMF do not match, or when the UE's network slice is not available
- PCF, SMF local configuration release policy
- Changes to UDM subscription data
- The DN needs to remove the access rights of the UE.
- UE is not in the LADN service area
- UE removes session anchor service scope area (no suitable IUPF exists)
- QoS Flow has been released for all PDU sessions

Situations where the SMF local configuration initiates PDU release include.

- Configuration changes

  Delete address pools that are already in use by terminals

  Delete a UPF node that already has a PDU session
- Restarting the process to recover stock data that cannot be recovered
- UPF is registered with the NRF

3.2.1.4 Session type support

Only one of these session types can be selected per PDU in the 5GC

Current PDU session types are.

- IPV4
- IPV6
- IPV4V6

- Ethernet
- Unstructured

The Unstructured type of PDU is generally used in applications where data is delivered to the destination via the N6 interface via peer-to-peer tunneling technology, which is not supported in the current IPLOOK SMF version.

3.2.1.5 Access type support

5GC access types are

Enumeration value	Description
NR	New Radio
EUTRA	(WB) Evolved Universal Terrestrial Radio Access
WLAN	Untrusted Wireless LAN (IEEE 802.11) access
VIRTUAL	Virtual (see NOTE 1)
NBIOT	NB IoT
WIRELINE	Wireline access
WIRELINE_CABLE	Wireline Cable access
WIRELINE_DSL	Wireline DSL access
WIRELINE_PON	Wireline PON access
LTE-M	LTE-M (see NOTE 2)
NR_U	New Radio in unlicensed bands
EUTRA_U	(WB) Evolved Universal Terrestrial Radio Access in unlicensed bands
TRUSTED_N3GA	Trusted Non-3GPP access
TRUSTED_WLAN	Trusted Wireless LAN (IEEE 802.11) access
UTRA	UMTS Terrestrial Radio Access
GERA	GSM EDGE Radio Access Network

Note If n3iwf does not know what access type to use to access the non 3GPP type, it can use the virtual

The current version of IPLOOK SMF supports the following access types.

- NR
- EUTRA

- VIRTUAL
- WLAN

3.2.1.6 Session Mode

Unlike I-UPF changes in some cases, changes in PDU session anchor points will affect one of the important user experiences, business continuity. To ensure different business continuity requirements, 5GC has defined three business continuity modes: SSC Mode 1, SSC Mode 2, and SSC Mode 3.

Session mode features

The SSC Mode of a PDU session remains the same for the lifetime of the session

The UE creates a new PDU session for the application when the SSC Mode of the existing PDU session does not meet the application requirements

IPLOOK SMF supports the following three session modes.

一、SSC Mode 1

For PDU sessions in SSC Mode 1, the IP address provided by the network to the UE remains the same as the UPF selected for the UE.

Features.

- Provide IP continuity
- PDU session anchors are not allowed to change
- The IP provided by the network to the UE remains the same
- Suitable for any PDU session type and access type

Application scenario.

Suitable for applications with high business continuity requirements such as IMS voice

二、SSC Mode 2

For a pdu session with SSC mode 2 already established in the network and only one pdu session anchor, the network may trigger the release of the pdu session and instruct ue to immediately establish a new pdu session to the same DN.

Features.

- No IP continuity available
- Disconnect first Release the old session to select another anchor point to rebuild a new PDU session to the same DN
- Suitable for any PDU session type and access type
- PDU session anchor point can be changed, when changing, you need to delete the old PDU session and create a new PDU session

Application scenario.

- Suitable for caching applications that do not require high business continuity and allow for short interruptions
- When the UPF needs to be changed or when the user surface path is not optimal

Note: In ULCL mode, ue does not participate in the reallocation of session anchors for pdu sessions.

三、SSC Mode 3

For pdu sessions in ssc mode 3, the network allows the ue connection to be established via a new pdu session anchor to the same data network and then releases the connection between the previous pdu session anchor and the ue.

Features.

- For sessions with any access type and IP PDU session type
- Provides short-lived IP continuity
- Changing PDU session anchor points
- Connect first, then disconnect PDU session, the anchor point can be changed, when changing, you can create a new PDU session first, and then delete the old PDU session sometime after the new PDU session has been created.

Note: (SSC Mode3 IPV6 Multihoming is not supported in the commercial version at this time)

Application scenario.

Suitable for applications such as MPTCP that support multi-path transmission.

3.2.1.7 De-activation

De-activation is actually a mechanism to notify the base station to release radio resources and to notify the UPF to change the downlink to BUFFER state to avoid wasting resources for a long time. The NOCP flag needs to be set when activation from the data plane is required, while some can only be activated from the access side without setting the NOCP flag, such as the de-activation initiated by the LADN service removing the service area.

Application Scenarios

SMF supports de-activation for the following scenarios.

- Handover switchover process in which all QoS flows are rejected by the RAN
- No data during UPF detection cycle

- AMF notifies UEs to move out of permitted operational areas

Related IE

- The SMF implements packet handling by setting the appropriate flags in the Apply Action IE in the FAR.
- Set the DROP flag to discard packets
- Set the FORW flag and provide instructions on packet forwarding with the forwarding parameters provided
- Set the BUFF flag to warm up the downlink packet and provide instructions on how to buffer the packet
- Set the NOCP flag to set the SMF to be notified when the first DL packet about buffering arrives
- Set DUPL flag to handle duplicate packets

Restrictions

Not available for permanently online PDU sessions, an always-on PDU session activates the user plane capital during each transition from idle to connected state, VoNR then uses the always-on PDU session, in this scenario the SMF cannot deactivate the UP connection for that PDU.

3.2.1.8 Session activation

Session activation means: restoring a terminal in the IDLE state to the ACTIVE state so that it can exchange data and signalling with the network normally.

The terminal UE has three basic operational states: DETACHED, IDLE and ACTIVE:

- DETACHED: When the UE is switched on, the UE first enters the DETACHED state, at which point the UE is not registered to the network, possibly because it is not registered or has failed to register under an unsuitable available network.
- IDLE: The state in which the UE is registered to the network but not activated and is in low power mode is called the IDLE state. The group core domain is already aware of the location of the UE and if a service is established, the UE is able to switch to ACTIVE mode in a very short time to continue the previously activated data session. In the IDLE state, the network side is able to know exactly where the UE is located in terms of TA (Tracking Area) and when the UE is called, the network is able to paging within the user's latest TA.
- ACTIVE: The state in which the UE is in the process of receiving and sending data is called the ACTIVE state, which is the only active state in which the UE and the network actually exchange data and signalling.

Trigger conditions.

- Terminals in IDLE status will initiate a report notification to the SMF when the UPF receives a downlink packet and the SMF will initiate the activation process

- When the terminal moves into the service area, the terminal initiates an activation request
- PDUs are also triggered when data comes in from a UE in CM-IDLE state, transforming the idle UE into a connected state in response to a paging message and activating the user-plane link

Session activation process.

UE with CM-IDLE status: UE or network side Request for activation

When the UPF in BUFFER state receives a downlink packet, it will initiate a downlink data notification to the session with the FLOW message set with the NOCP flag, and the SMF will trigger the activation process after receiving the report information from the UPF. See below for UE activation

UE with CM-CONNECTED status: UE requested activation via service request

When the terminal enters the service area, it initiates an activation request to the SMF, which receives the request from the AMF and clears the FAR of the BUFFER state.

3.2.1.9 LADN (Local Data Network) sessions

A LADN session means that the UE can only access the local data network via a PDU session connected to the local data network in the service area of the local data network.

Characterisation

The services of LAND are provided by the service PLMN, where the LADN data network area is a TA set, where whether a DNN corresponds to a LADN service is a property of the DNN.

The LADN service has the following features.

- LADN information is provided to the UE by the AMF on the registration process and the UE configuration update process
- LADN service area and LADN DNN configured on the AMF to allow different UEs to access the same LADN
- If a LADN is not available under all TAs in an AMF service area, then this AMF should not configure LADN information for this network

Functional operations.

- PDU session creation: If the configuration of the LADN related DNN is configured on the SMF, the SMF will check the status value of the presenceInLadn sent from the AMF of the corresponding DNN, and if the status value is not in the area, the session will be rejected directly.
- PDU Session Modification : If the configuration of the LADN related DNN is configured on the SMF, the SMF will check the status value of the presenceInLadn sent from the AMF of the corresponding DNN, and if the status value is not in the area, the session will be released or the session will be de-activated.
- AMF subscribes to LADN notifications: the SMF behavior is determined by the value of the presenceState field, and the SMF triggers a session release or triggers a PDU session deletion when not in the ladn area, depending on the local LADN configuration.

Main interfaces.

N11

During the creation of a LADN session, the AMF communicates with the SMF through the N11 interface with the LADN logo, and the SMF checks and verifies the LADN logo carried by the AMF.

Restrictions.

- Permanent sessions are not supported
- Only available in 3GPP access mode and not available for Home Routed roaming scenarios

Service configuration.

Local data network In /opt/IPLOOK/smf/config/ladn.json, start the ladn service by changing the value of enableLadn to yes and turn off the ladn service by assigning the value of no. where ladn is the dnn value and ladnType is the behaviour of the UE after it has left the ladn area, which can be different depending on the value

as follows.

- If ladnType is deactivateUp: the deactivation is initiated and the session is released if it is not returned to the zone within the system specified time (15s).
- If ladnType is empty or other value: the pdu session will be released directly.

3.2.1.10 Area of interest tracking

Area of Interest (AOI): is a geographical area within the designated 3GPP system.

Area of interest tracking refers to the tracking of end devices that have initiated location area subscription tracking to the AMF in a geographical area within the 3GPP system designation.

For 3GPP access, the area of interest includes the following.

- TA List
- Cell ID
- RAN ID
- PRA ID(s)
- LADN DNN

Process for subscribing to the Zone of Interest.

- SMF subscribes to the "UE Mobility Time Notification" service from AMF
- UE enters or leaves area of interest, SMF receives notification from AMF
- SMF determines how to handle PDU sessions based on the UE's location information

SMF treatment of areas of interest.

When the area of interest is a LADN the SMF provides the DNN information of the LADN to the AMF and subscribes to the "UE Mobility Time Notification" service

Characterisation

Terminal movements and status in the area are sent down to the SMF via AMF notifications

Main interfaces.

N11 The AMF pushes the status of the terminal in the area to the SMF by subscribing to notification messages

Associated business.

- PDU session creation: sending a subscription to the AMF for the terminal's area of interest
- PDU session modification: de-activation of subscription notifications sent by the end zone behaviour
- PDU session release: release processing of subscription notifications sent by the end zone behaviour
- AMF subscription notifications: subscription notification processing for endpoint areas of interest

Restrictions.

- Permanent sessions are not supported
- For 3GPP access mode only

Configure/stop up service.

Local data network In /opt/IPLOOK/smf/config/ladn.json, set the value of enableLadn to no to turn off the ladn service.

The parameters in the trackingAreaList field are configured to include the area to be tracked, and the AMF receives the subscribed tracking area based on the terminal's

3.2.1.11 Base station switching services Support

XN switching (Handover process)

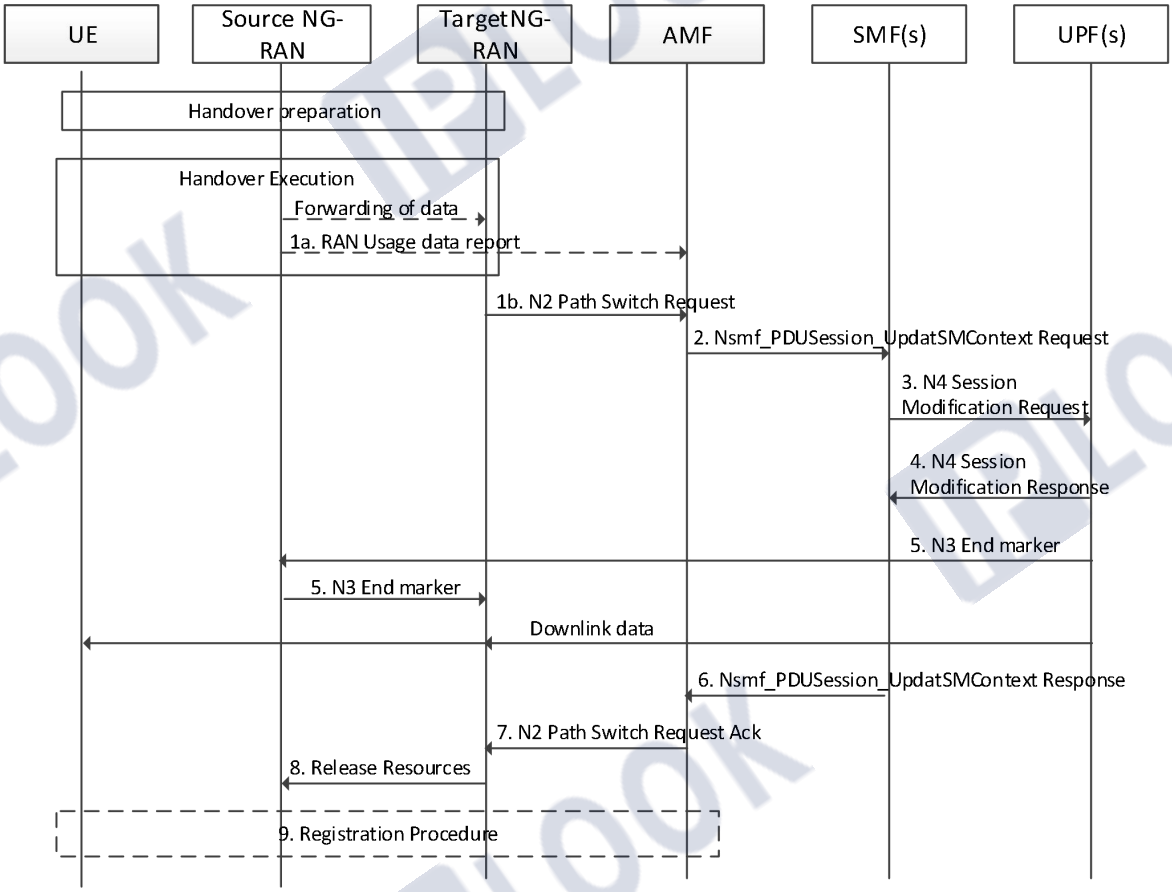
The Handover process is used to switch the UE from a source NG-RAN node to a target NG-RAN node, using the Xn interface during the switchover. The switchover process can be triggered due to new wireless conditions, load balancing or specific services.

In order to ensure that the order of the target NG-RAN packets is not confused, immediately after the path switch, the UPF sends one or more "end marker" packets to the source NG-RAN via the old path and the source NG-RAN forwards the packets to the target NG-RAN. Downstream packets can be sent directly to the UE via the new NG-RAN.

Key IE

- Tunnel ID information for N3 port downlink data
- UE Security Capability
- Location information for UE
- End marker logo

Reference flow chart.



A description of the process can be found in: 3GPP 23502-4.9.1.2.2

Note: During the switchover process, if the terminal is located in an area outside the service area of the anchor PSA, an intermediate IUPF is inserted, or if the area activates certain separation policies, the corresponding ULCL or BP is created in the middle.

N2 switching (Handover process)

Access and mobility capabilities in 5G networks, and business continuity capabilities for UEs during mobility. Mobility management includes business processes such as user state management, registration, service requests, switching and logging off.

Characterisation

User terminals are always in a state of constant movement and the core network needs to handle the terminal's services according to the user's service performance. The network continuity is ensured by ensuring that the UE is not interrupted while it is on the move.

Features

Xn switching

1 Based on switching between NG-RAs on the N2 interface.

2 Switching between NG-RANs based on XN interfaces

3 Regional mobile update of ULCL/BP/I-UPF shunt support

4 Activation and de-activation of the terminal IDLE status

3.2.1.12 Strategic Control

SMF policy control is done through PCF to control the QoS and billing policies of the UE based on the subscriber's contract information, etc. It can be divided into PCC policy and billing policy control.

The PCC rules are embodied in two ways.

Dynamic PCC rules.

The SMF dynamic PCC rules are simply obtained through the N7 interface with the PCF. This rule can either be pre-defined by the PCF or generated dynamically by the PCF. defined rules or dynamically generated by the PCF. Dynamic PCC rules can be replaced, modified, deleted

Predefined PCC rules.

Predefined PCC rules are configured on the SMF, flow filters are provided to the UPF as flow filter rules and can be configured either on the SMF or on the UPF, but if configured on the UPF then the relevant application identifier needs to be configured on both the SMF and the UPF.

Note (in addition to the above two rules there is also an ADC application detection and control rule as detailed in the following predefined rule processing)

PCC rules key messages include.

- Rule name
- Service marks
- Data flow filters
- Priority
- Door status
- Qos parameters
- Rate Groups
- Other billing parameters
- Monitoring Team
- Initiatorship
- Application service provider identification
- Traffic-oriented policy identifier

Purpose of PCC Rules.

- Detection of packets belonging to the service data stream.
- The service data flow template in the rule is used to select the downlink IP CAN bearer.

- The service flow filter in the rule is used to enforce that the uplink IP flow is transmitted correctly in the IP CAN bearer.
- Identify the services provided by the service data stream.
- Provide applicable charging parameters for the service data stream.
- Provides policy control for service data flows.

Application scenario.

- PDU session creation, modification and release
- Policy Control Issuance
- Diversion control
- Billing

Billing Strategy

See Convergent Billing for details

3.2.1.13 Convergent billing

Billing is a costing system set up by the operator to measure the usage of network resources by the subscriber and to charge the subscriber according to certain tariff policies.

In 2/3/4G networks, billing is divided into online billing and offline billing, and in 5G networks, convergent billing is introduced. Convergent billing uses a service-oriented interface to support

convergent online and offline billing, thereby simplifying the network and flexibly supporting different business scenarios and needs.

The role of the SMF in billing is as follows.

- As a service user, the billing session process for the Nchf interface is supported.
- Support the selection of CHF.
- Request and receive quotas from CHF.
- Supports PDR, URR rule issuance and billing usage collection for the N4 interface with the UPF.
- Supports billing policy control of the N7 interface with the PCF.
- Report quota usage, operational usage reports to CHF.
- Handling of quota reauthorisation trigger conditions.

Billing process.

1. Terminal initiates a PDU session
2. SMF requests PCC rules and billing rules
3. SMF applies to CHF for quota
4. SMF issues quotas and PCC rules to UPF
5. UPF reporting of billing reports
6. SMF reports billing information to CHF

Current SMF version supports both online and offline billing

The billing is measured whenever there is.

- Measurement by flow rate usage

- Measurement by time
- Event-based measurement methods (not supported in current version)

Billing related processes.

- Reported usage
- Stop sending traffic data when traffic is exhausted

Billing is important in relation to URR IE.

- Type of billing (online, offline)
- Billing method (usage, time)
- Key value (billing identification)
- Dosage
- Usage thresholds (reported when traffic arrives)
- Time spent
- Time Threshold
- Reset time
- Call sheets

Billing configuration

Configure the relevant CHF server information in SMF Network Management Interface Property-->Peer-->N40 Profile

Locally configured billing.

Configure the relevant service information associated with the CHF server on the Service Profile in SMF Network Manager and select Offline Billing. Add Static PCC Rules to configure billing-related information in the corresponding CHG Action.

Configuration of billing on PCF.

Configure the appropriate Quate information on the PCF network manager and associate the configured Quate information with the Charging Data in the corresponding service.

3.2.1.14 Flow management monitoring

Traffic management offers the possibility of billing and some traffic restrictions for terminals and other network elements

The traffic monitoring process is performed at the UPF, mainly to determine which session or which service data flow the packet belongs to. The whole monitoring process is not performed by the UPF independently, but requires the SMF to guide the UPF, telling the UPF through the PDR how to detect to whom the packets belong and how to manage the statistics.

The SMF binds the data flows to be managed and monitored to the URR when creating a PDU session or modifying a PDU session and sends them to the UPF, and activates the UPF traffic usage report distribution function to the SMF.

One of the UPF traffic usage reports is as follows

- Request UP Success Usage Report when traffic reaches threshold
- Generate a report to inform the SMF when the flow is exhausted
- Flow measurement methods are
- Time measurement
- Measurement by volume
- Traffic Package Changes

When the SMF provides an inactivity check time, the UPF will suspend the time measurement on this time. Current version does not support

3.2.1.15 Diversion strategy control

SMF split control refers to the ability of the SMF to route uplink services for the same PDU session to two or more PDU session anchor points through policy control signalling, and the ability to route the downlink tunnel link of these PDU session aiming points towards the UE.

In the edge computing scenario, the PDU session will divert the uplink data traffic to multiple PSAs (PDU session anchor) of the UPF, and the N9 tunnel will be established between the UL CL and each PSA, and the UL CL will forward different traffic to different PSAs according to the PDR, FAR and other rules issued by the SMF, and then the PSAs will forward to the DN.

Upstream splitting and downstream convergence. Different services can be associated with different QOS FLOWs, and different QOS FLOWs are going to different PDU session anchor points, which can flexibly implement various services in 5GC that require complex multi-anchor support.

The SMF distinguishes traffic going to the remote DN exit from the local DN exit by issuing multiple PDRs and FARs to the UL CL so that traffic going to the local exit is forwarded by the UL CL to the local DN exit (i.e. the local PSA, PDU session anchor 2 in the diagram), while traffic going to the remote end is forwarded to the remote DN exit.

Characteristic features.

- Each PDU session can only have one DN

- The function of the UL CL includes, in addition to diverting upstream traffic, aggregating downstream traffic from multiple DN outlets to the UE
- PSA and UL CL can be combined on the same UPF;
- The SMF may insert the UL CL as soon as the session is established, or it may insert it sometime after the PDU session has been established

ULCL (Uplink Classifier) Upstream Classifier

The uplink splitter can be used for IPV4,IPV6, IPV4V6 or Ethernet PDU sessions. The shunting principle is based on the prefix of the destination IP address or uplink packet as a condition for shunting the data to the corresponding anchor point.

BP (Branching Point)

For multi-homed PDU sessions of type IPV6, uplink services are routed to different PDU session anchors based on the source IP prefix. Requires endpoint support for multi-homing

How to use.

- The current IPLOOK -PCF service templates that can be supported are (silent load, Volte load, time-of-use load, carrier load, user load, usage load, unlimited traffic load, slice load). The SMF will find a suitable anchor point for the splitting according to the policy rules and trigger the splitting policy.
- Mobility changes anchor points or triggers/deletes diversion policies, triggering different anchor policies as the UE moves into different areas. Diversion policies can be created/deleted on the move depending on the zone
- Network side trigger, add a new diversion policy to the PCF network management corresponding to the SMF to trigger the diversion, either by adding a new service with

diversion or by adding a diversion to the original service to trigger the diversion policy. (PCF access required)

The UL CL can usually be applied in scenarios where user traffic needs to be directed to the local DN outlet.

Restrictions.

Locally configured diversion policies do not support zone changes, i.e. if you move out of the zone supported by the UPF that acts as the diversion anchor, the diversion policy will be abnormal. Some services will be affected.

Configure/stop up service.

Main interfaces.

- N9 Communication interface between UPF and UPF for direct data transfer from UPF

Relevant configurations and conditions.

The PCF/local needs to be configured with diversion rules that must include the following items.

- Qos Flow .
- TraffContDecs .

  UPF-related configurations.
- Dnai.
- N9 tunnel.
- For IPV6 sessions you need to configure N4u.
- If you need to switch the diversion on or off according to the zone plan, you need to configure and plan the corresponding UPF Tac

- Terminal-related configuration.
- In the case of IPV6 multi-homed PDU sessions, support is required at the endpoint capability level

Flow billing and traffic management statistics. See above

Key interfaces:

Inter UPF shunt function N9 interface

3.2.1.16 SMF and UPF interoperability

Associated with.

- PFCP Association Set up
- Association Update (PFCP Association Updata)
- Associated Release (PFCP Association Release)

Characteristics.

Two-way operation, i.e. both SMF/UPF can initiate or receive requests

Related IE:

- Node identification
- Start-up timestamp
- UP function
- CP Function
- User plane IP resource information (eg: resource type, FTEID range)

- UE IP address pool identifier (can be present when the UP is sent and is used to specify information about the address pool currently available to the UPF in relation to the assigned UE IP)

PFCP session related.

During the process of establishing a PDU session by the user, an N4 session, also known as a PFCP session, is established simultaneously, using PFCP (Packet Forwarding Control Protocol), a protocol used to define a series of UPF actions on PDUs actions include.

- PFCP session establishment
- PFCP Session Modification
- PFC session release

Among the relevant IEs are:

- Identification: PDRs (Packet Detection Rules).
- Forwarding: FARs (Forwarding Action Rules)
- Caching: BARs (Buffering Action Rules)
- Marking: QERs (Qos Implementation Rules)
- Reporting: URRs (Usage Reporting Rules)
- Multiple Access: MAR (Multiple Access Rules) (not supported)

PFCP Session Report

See UPF report section

3.2.1.17 Vo5G support

The 5G network architecture is inherited from 4G, which has no core network to support voice services and must rely on the IMS system.

Characterisation

Vo5G is a generic term for 5G voice solutions, which includes VoNR, EPS FB, VoeLTE, RAT FB. current IPLOOK Vo5G supports deployments in the form of SA Option2 mode as shown in Figure 2.7-1. current Vo5G can be broadly divided into processing based on NR support for voice, and processing with NR not supporting voice sinking to EPC+.

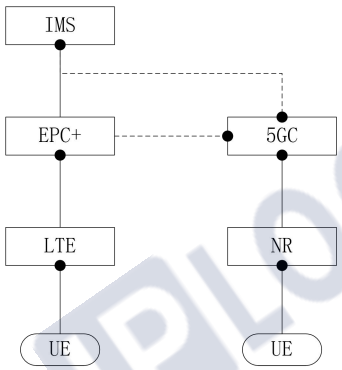


Figure 2.7-1 SA Option2

Features

VoNR

VoNR means that the voice service terminal resides in the NR network through the gNB bearer and goes for different voice services according to different network environment architectures.

For example:

- Voice services are carried via gNB and 5GC, signalling services go QOS FLOW

- Voice services are carried by gNB and EPC Signalling and services are carried by EPS bearer
- UE resides on NR network, when NR signal becomes poor, voice will switch to 4G VoLTE

Application conditions.

Terminals

- NR voice support required
- No need for 4G network coverage including 5G network
- Calls in NR coverage can be handled directly by NR base stations

Base stations

- NR base stations need to be voice enabled
- VoNR required

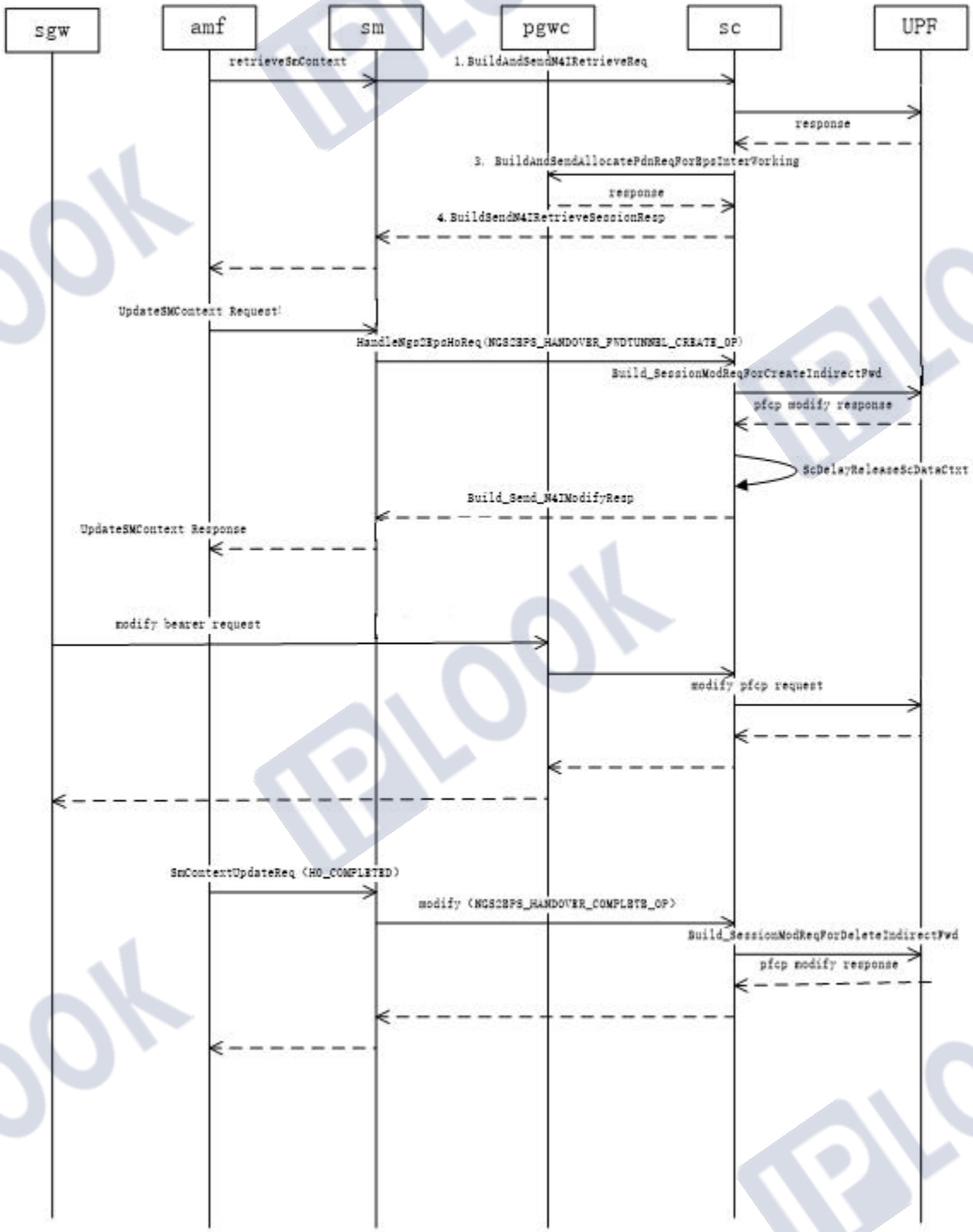
Core Network

- EPC and 5GC support the N26 interface
- IMS supports access to 5GC

EPS FB

This approach is used in the initial phase of 5G deployment, i.e. the UE resides on the NR side and registers in the IMS domain, when a voice service is initiated, will be redirected to switch to the 4G network for voice over VoLTE.

The EPS to 5GS switchover occurs when the UE moves to the 5GC network while in the E CM-CONNECTED state in the EPC. The schematic flow is as follows.



Application conditions.

Terminals

- Calls in NR coverage can be handled directly by NR base stations
- Requires VoLTE as base network, 4G network coverage including 5G network

Base stations

- NR voice is not supported or not required
- Weak 5G signal
- The base station supports IMS voice EPS fallback or RAT fall back triggered request initiation, and can fall back to 4G LTE to provide voice based on VoLTE
- Supports 4G/5G interoperability

Core Network

- IMS supports access to 5GC
- 5GC requires EPS FB to be opened
- EPC and 5GC support N26 interface and network support for 4G/5G interoperability

VoeLTE

Voelte refers to the voice bearing in ng-eNB, this solution UE is stationed in ng-eNB, to the poor coverage of the base station The UE will continue to carry voice through VoLTE or VoNR on 4G or 5G networks in areas with poor coverage.

RAT FB

This means that the UE resides in the NR test and is registered in the IMS domain, and when redirected or switched to the ng-eNB, the voice is carried out via Voelte voice. This scheme is similar to EPS FB, with the difference that RAT FB is done within 5G.

Main interfaces.

S5-C

- This interface is used for SGW and PGWC signalling interactions during the 4G/5G switchover

Application use.

Depending on the current network environment or state, the client can request different bearer services as follows.

- If the current network environment NR supports voice services and the UE resides in the NR network, the VoNR solution is used
- If the current primary network environment is VoLTE and the 4G network coverage includes a 5G network, the EPS FB solution is used
- If the current UE voice is carried on the ng-eNB, and the UE moves to some areas with poor coverage, the UE will switch to a 4G or 5G network and continue to carry voice via Volte or VoNR.
- If the current eLTE network coverage environment is larger than the coverage of NR, then use the RAT FB solution

Associated business.

- XN Switching

- N2 switch
- Core network side to be replenished

Restrictions.

None

Configure/stop up service.

Find Interface Property-->Local-->S5 Profile on the IPLOOK Large Network Manager SMF branch and configure the corresponding service restart PGWC process. The Deactive Flag is false to enable the service and true to disable it.

3.2.1.18 NRF Dynamic Selection Discovery Functionality

The 5GC network adopts a service-oriented architecture, abstracting the control plane functions into multiple independent Network Functions (NF), such as AMF, SMF, NRF, NSSF, etc. IPLOOK SMF can achieve diverse network adjustments through the NRF function, allowing other network element devices to discover or find other network element devices, giving users the choice of The corresponding available service network elements, including UDM, AMF, UPF, etc. provide more flexible and convenient services for users.

Where IPLOOK SMF supports the NRF by providing.

1. NF Registration Management (Nnrf_NFManagement)

Registration management between SMF and NRF.

- Service Registration
- Service Updates
- Services to register

2. NF Discovery Service (Nnrf_NFDiscovery)

SMF through the NRF to NF service.

- NF Discovery
- NF Status Subscription
- NF Status Notification

Current IPLOOK SMF support for NRF discovery network elements include.

- Support SMF to discover AMF
- Support SMF to discover UDM
- Support SMF to discover UPF
- Support for NRF discovery SMF

3. NF Token authentication service (Nnrf_AccessToken)

When Token information is configured, the SMF finds that access to the relevant network element will take the relevant Token information with it, and only when the Token information is verified can the corresponding network element be accessed.

Service configuration.

When the NRF service needs to be turned on, in order not to affect the NRF service can be deleted on the SMF unnecessary UDM, AMF, UPF configuration to avoid interference, add Nnrf Profile configuration, restart the service

Note: NFs can only register with the NRF to which they belong, no cross-PLMN registrations, no same-tier cross-region registrations

3.2.1.19 CallTrace support

Call Trace is a very important analysis method in the system and can collect a wide range of trace information including single or multiple network elements, single or multiple handsets. The traces collected can be analysed using packet capture tools, which can quickly locate the point of occurrence of errors and provide a complete message flow.

The call trace options currently supported by SMF

By business interface there are.

- N4
- N7
- N10
- N11
- S5-C

By session interface there are.

- PDU session creation
- PDU Session Modification
- PDU session release
- 4/5G interoperability
- Standard and non-standard 3GPP operation

Performance features.

- You can filter specified information based on SUPI
- Information can be filtered based on a specified service or session interface

- Each network element controls its own Trace function independently (similar to SMF control of UPF Trace status via signalling is not supported)

Support operations.

All access-side initiated services and activation and de-activation services currently supported by the SMF

Operating configuration.

See webmaster operations manual

3.2.1.20 PCF service subscriptions and deletions

The current SMF supported PCF service subscriptions are as long as

- Silent load
- Volte Special
- Time dedicated to
- Carrier-specific load
- User-specific load
- Usage
- Unlimited traffic dedicated load
- Slices exclusively

Service configuration and description.

See PCF webmaster manual

3.2.1.21 Local policy control

Local policy control, without access to the PCF, can be configured according to the SMF local configuration to limit Qos parameters, billing information, traffic splitting and other services

3.2.1.22 IUPF Support

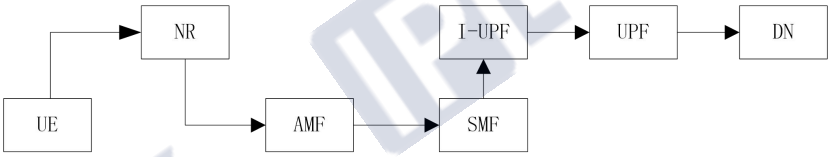
Characterisation

Each PDU has a user-plane path, which contains at least one UPF and may contain multiple I-UPFs. for an established PDU session, its user-plane path is not static, UE movement or policy changes may cause the SMF decision to change the user-plane path, when the terminal moves to an area that cannot be supported by the current session anchor point, in order to ensure the service continuity, when a qualified IUPF exists in the absence of other specific services, the IUPF will be inserted as a transit between signalling and data plane to preserve the continuity of services.

IUPF insertion conditions.

- Presence of UPF with N9 opened (IUPF)
- This IUPF area covers the current area of the terminal and the PDU session anchor PSA area
- The session anchor PSA service area is not in the current area

After insertion of the IUPF the 5GC Simplex architecture is as follows.



Note: Inserting an IUPF when creating a PDU session is not supported

Application Scenarios

When the terminal moves to an area that cannot be supported by the current session anchor, the IUPF is inserted to ensure continuity of service.

Interfaces involved

N9: User-plane interface between UPF and UPF for passing upstream and downstream user data flows between UPFs

3.2.1.23 Secondary Authentication

SMF secondary authentication is the process by which the SMF initiates a secondary authentication to AAA (RADIUS) before establishing a data channel for its end users

The following information is required to check whether secondary authentication is initiated:

- Contract information
- Does the terminal support
- Local configuration of Access Mode information

Time of secondary authentication authorisation: when the PDU session is established

Secondary certification process.

SMF issues authentication to the AAA service and establishes an authentication channel and completes the authentication request with AAA through message interaction. After secondary authentication, SMF will establish a connection to the data network for the terminal.

Deployment

SMF deployed with AAA

Configuration.

SMF Network Manager --->Subscriber Profile Information --->Access Mode Select TRANS_AUTH Other options are not supported in the current version. Not supported in previous versions, CHAP,PAP is currently supported (EAP is not supported).

3.2.1.24 UE IP allocation management

IPLOOK 5GC currently supports the assignment of UE IPs to terminals in the following ways.

1. **UDM Static IP Configuration**

The SMF resolves the static IP field staticIpAddress issued by the UDM when it acquires subscription data on the UDM, and uses the acquired IP as the endpoint IP address. The obtained IP address is used as the endpoint IP address and no new IP address is dynamically assigned.

2. **SMF assigns dynamic IPs**

When no static IP is configured on the UDM and the UP feature UeIp is not set, the SMF assigns an IP address dynamically for the terminal.

3. UPF Assignment of dynamic IP

When there is no static IP configured on the UDM and the UPF feature UeIp is set, the UPF will respond to the N4 PDU session when it is created by sending the to the IP address of the SMF UE.

Where the SMF configuration file needs to be modified smfProcess.json

3.2.1.25 Fteid allocation

The F-TEID shall be assigned by the SMF or the UPF, where the assignment of the F-TEID by the SMF is mandatory and the UPF is optional.

The UPF can implement the assignment of F-TEIDs by the UPF by setting the FTUP function flag on the UP function. the same F-TEID assignment option should be used for all CP functions controlling a specific UP function.

SMF allocation F-TEID

When performing F-TEID assignment on the SMF, the SMF shall take the local F-TEID IE on the PDR IE and provide the assigned F-TEID value to the UP function.

UPF allocation F-TEID

When performing F-TEID assignment on the UPF, the SMF requests the UP to assign an F-TEID by setting the F-TEID IE in the PDR IE that needs to request the F-TEID to the CHOOSE flag when requesting the UPF. when the PDR is successfully created, the UPF will bring the assigned F-TEID with it when it answers.

Fteid release

For F-TEIDs assigned by SMF/UPF, the assigned F-TEID is released when an operation such as deleting a PFCP session or removing a PDR is received F-TEID resources

3.2.1.26 UP IP RESOURCE processing

User plane IP resource information

UP IP RESOURCE is obtained by.

- SMF local configuration
- UPF is distributed to SMF via PFCP Association Setup or update
- Discover UPF down to SMF via NRF

UP IP RESOURCE As long as the content.

- Provides access information for the N3 interface and the TEID range for the associated FTEID
- Provide N9 interface access information with the TEID range of the associated FTEID
- Provides access information for the GTP-U interface and the TEID range for the associated FTEID

3.2.1.27 SMF user surface management functions

The SMF user interface management functions simply include the following:

1. UE IP address management

See section 2.16 for more information

2. CN tunnel management including N3,N9

The CN tunnel is the core network address of the N3/N9 tunnel corresponding to the PDU session, which includes the TEID and IP address, and is provided by the UPF.

Among these are the management of CN tunnels as long as there are.

- When new CN tunnel information is required, the SMF will request the UPF to allocate CN tunnel information to it via PFCP
- The SMF will notify the UPF to release CN tunnel information when it needs to be released or when the user plane path is abnormal

3. Stream detection

SMF controls traffic detection in the UPF function by providing detection information for each PDR for IPV4,IPV6 or IPV4V6 session types.

The information tested contains.

- CN Tunnel
- Web examples (eg:dnn)
- QFI
- IP PFS
- Application Identifier APP ID

For a session type of Ethernet, the detection message contains.

- CN Tunnel
- Web examples

- QFI
- Ethemet PFS

With this detection information above the SMF is responsible for guiding the UPF on how to detect that user data traffic matches the rule parameters provided in the PDR.

4. User-facing forwarding control and data caching management

Transfer of user plane data forwarding functions from the UPF to the SMF (not supported in current version)

5. Send End Mark

To ensure that the order of packets from the target base station is not confused, the UPF sends one or more End Marker packets to the source base station after the base station path switch, which in turn forwards the packets to the target base station.

The construction of End Marker messages can be done either in the SMF function or in the UPF function, and support for End Marker in the UP function is optional.

When it is necessary to construct an End Marker on a UPF the following conditions need to be met.

- UPF attribute value Empu must be set
- The SMF needs to bring the new downstream F-TEID with SNDEM identification on the PFCP session modification request.
-

Note: (currently not supported by IPLOOK 5GC, current programmes End Marker are initiated by SMF, regardless of UPF support)

Application scenario.

- Xn switching
- N2 switch
- 4G HANDOVER 5G

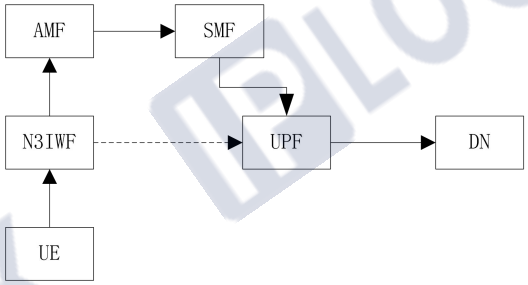
6. UP tunnel management (AN side)

When the PDU session uplink connection is deactivated, the SMF may release the link on the N3 terminal, at which point the UPF is in the uplink BUFFER state.

3.2.1.28 Non 3GPP access

The 5G core network supports access through 3GPP access networks (e.g. gNB, eNB) and also through Non 3GPP networks. non 3GPP networks access the 5G network through the N3IWF (Non-3GPP InterWorking Function) and the N3IWF accesses the 5G network through the N2 and N3 interfaces.

The N3IWF creates a permanent session identifier on the N2 message band during PDU session creation, and the SMF checks the legitimacy of the PDU session creation requests coming from the N3IWF network and creates a permanent PDU session for those requests that pass the check. For non-3GPP access as per the N3IWF example, the access framework diagram is as follows.



Access features

- The user plane data must be activated each time the terminal cuts back from the CM-IDLE state to the CM-CONNECTED state.
- If the UE is connected to a 5G core network by both 3GPP and non-3GPP means, then for this terminal there will be two N1 entities at the same time, one corresponding to 3GPP access and the other to non-3GPP access; if the N3IWF and the 3GPP access network are also part of the same network (same PLMN), then these two N1 instances should be in the the same AMF.

Operational configuration.

None

Operational restrictions.

None

3.2.1.29 Predefined rules processing (PCC/ADC)

Predefined PCC rules are pre-configured in the SMF, either locally or on the PCF, if the PCF is connected then the rule entity is configured on the SMF and the PCF sends down static rule service names to match the static rules configured on the SMF. If the PCF is not connected, the SMF can configure static rules on the network management and do not configure the associated QosFlow. The matched rule will be created or modified via a PFCP session and sent to the UPF (see Policy Management section for PCC rule details).

Predefined ADC rules are supported. ADC rules are pre-configured on the TDF and the SMF brings the corresponding APP ID entry on the PDI in the PDR when creating or modifying a PFCP session, and the UPF matches the corresponding ADC rules based on the APP ID in the PDI.

Characteristics.

- Can be activated or deactivated at any time
- PCC rules configured on SMF
- ADC rules are then configured on the UPF (normatively referred to as stored in the TDF)

Configuration.

- SMF local predefined PCC rule configuration: SMF network management configuration Add Service Profile configuration where Flow Information is not configured
- Service name of the predefined rule issued on the PCF: Qos Action configured on the PCF webmaster in the corresponding rule
- Configuring ADC predefined rules on the UPF: Configuring the APP ID on the corresponding service Qos Action on the PCF network manager

The configuration on the UPF is described in the UPF network management manual.

Note: See UPF detailed functional documentation for ADC details

3.2.1.30 UPF Framed Routing Processing

The Framed Routing feature allows the IP network behind the UE to make ranges of IP addresses or IPv6 prefixes reachable on a single PDU session, for example for enterprise connectivity.

The UPF may indicate support for the frame routing feature by setting the FRRT flag in the UP Feature IE. The UPF advertises the relevant IP routes to receive packets destined for these destination IP addresses or IPV6 prefixes and forwards these packets via PDU sessions. FrameRouting support in IPLOOK 5GC requires the following configuration of network elements.

- Configure relevant forwarding route addresses such as IPV4 and IPV6 prefixes on the UDM
- UPF function feature IE requires the FRRT flag to be set
- SMF includes Framed-Route IEs in PDRs sent to UPF

Restrictions.

Framed routing is only available for IP type PDN connections and PDU sessions

3.2.1.31 Session data change notification SMF

Business scenarios

When the endpoint session data changes, the UDM sends it to the SMF via a subscription notification. Currently, the SMF only processes changes to the session data upstream and downstream AMBR and default Qos change information, but not other data changes.

SMF's handling of subscription notifications.

- When the AMBR or default Qos changes, the SMF initiates a PFCP session change to the UPF and notifies the base station and terminal to update the new AMBR or default Qos information via N1N2 messages
- When a session information Dnn is deleted, the SMF will directly release all current sessions that use this Dnn

Webmaster configuration.

See UDM network management configuration

3.2.1.32 Reflective Qos

In the absence of QoS rules provided by the SMF via signalling, the UE can map uplink user-plane data to QoS flows by reflecting QoS.

Reflective Qos characteristics.

- For IP and ethenet type PDU sessions only
- QoS rules derived by the UE based on received downlink data
- Reflected QoS and non-reflected QoS can co-exist for the same PDU session
- The default QOS does not support reflective Qos attributes

Business Processes.

- (a) When the 5GC determines that it wants to use reflected QoS, the SMF sends a message with an RQI signalling indication to the UPF via the N4 interface.
- (b) Upon receipt of this indication, the UPF sets the RQI parameter in the N3 packet header when packing each downlink packet corresponding to this SDF.
- When the base station receives an N3 downlink packet and finds that the RQI field is set, it sets the QFI and RQI parameters (i.e. the QFI and RQI fields in the downlink SDAP header field) when it is sent to the UE.

SMF Business Support.

- By bringing its ability to reflect Qos when creating a PDU session, the SMF decides according to its policy (configuration) whether to bind the reflected RQI identity to the QER of the uplink signalling UPF versus making the QoS-configured RQA identity of this QoS flow available to the NG-RAN via an N2 message.
- When a PDU session is already in place, the terminal can initiate a PDU session change to support or cancel the Reflected QOS capability, and the SMF will follow the request to the UPF and NG-RAN to cancel or support the Reflected QOS capability.
- If RQA is already provided to the NG-RAN and the 5GC determines that it no longer uses reflected QoS for a QoS flow, the SMF has to notify the NG-RAN via N2 port signalling to remove RQA for this flow.(5GC active trigger not supported)
- When the 5GC determines that it no longer uses reflected QoS for a particular SDF, the SMF is to notify the UPF via the N4 interface that reflected QoS is cancelled; (5GC active trigger not supported)

Operational configuration.

- SMF local configuration on Network Manager Service Profile-->Services-->QosAction, select true (effective) or false (disabled) for Reflective Qos
- PCF network management configuration, see PCF network management instructions for details

Operational restrictions.

Currently only 3GPP access is supported, non-3GPP is not supported at this time

Note: For non-3GPP access networks N2 signalling is not required to enable reflective QoS, the QFI and RQI will be transmitted directly to the UE in the non-3GPP access network. (subsequent enhancement)

3.2.1.33 UPF Report

1. Node level (not supported in current version)

2. Session level,Report Types and Operations

Session level report types :

1. **DLDR (Downlink Data Reporting)**

DLDR report to the SMF when a PDU session UPF in the idle state receives downlink data

Trigger scenes

The terminal is in the Paging state and the UPF receives the packet from the DN

When the SMF receives a UPF DLDR report request, it sends an N2 message to reactivate the base station to resume the PDU session

Business scenarios

Downlink data activation for PDU sessions that are idle

2. USAR Usage Report

Traffic Usage Report

Trigger scenes

The UPF reports the traffic usage to the SMF based on the ticket information and the endpoint traffic usage.

Business scenarios

- Flow management (e.g. matching different policies to different QosFlow for different traffic classes)
- Traffic statistics
- Billing

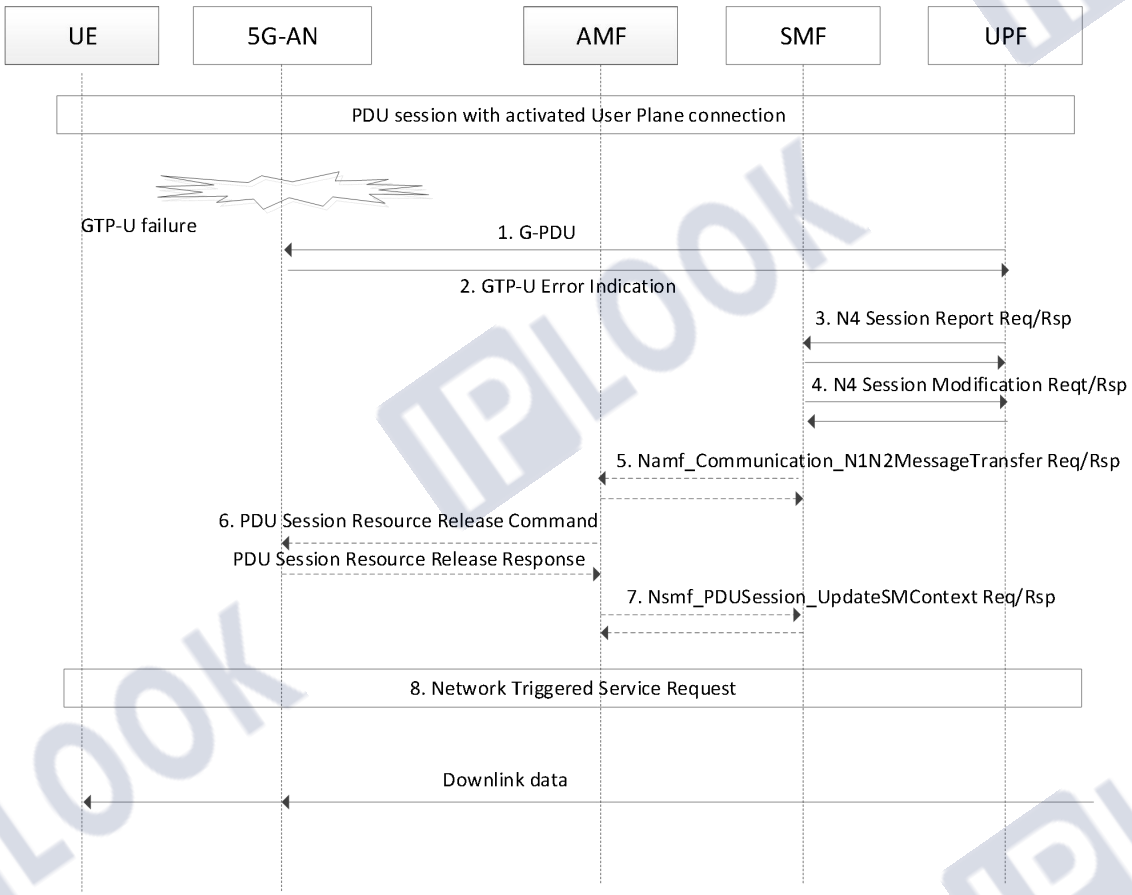
3. ERIR Error Indication Report

Trigger scenes

After receiving the GTP-U error indication message, the UPF initiates an ERIR-type report to the SMF that created the PDU session

Business Processes

As shown below The SMF receives the ERIR report and initiates a PFCP change session request to the UPF based on this PDU, leaving the UPF in in the downlink packet cache state. At the same time, if the base station is still connected, the SMF will release the AN resources of this PDU via N2 message.



4. UPIR User Plane Inactivity Report

Trigger scenes

If a PFCP session is created with an inactivity duration value and no upstream or downstream data passes through the UPF for a given period of time after the session has been successfully created, the UPF will report this event to the SMF

Business scenarios

The SMF creates the PFCP session with the session inactivity duration i.e. when no downstream data passes through the UPF during the inactivity time, the UPF has to initiate an inactivity report to the SMF for the SMF to activate this user plane.

Key fields and configuration

Modify the upInactiveTime value in the smfProcess.json file to the time in seconds that needs to be configured, and restart smfScProcess after the change. (Subsequent versions may consider incorporating the configuration of the Network Manager UP Node Profile)

When the upInactiveTime value is configured, the UpInactiveTime field can be seen on the message when the PFCP session is created.

Note: (Refer to section above for SMF de-activation details)

3.2.1.34 Webmaster support

See webmaster operations documentation

3.2.1.35 Support for OAM management

See OAM design document

3.2.1.36 Security Management

The IPLOOK SMF acts as the network element that controls the management session and can effectively control whether a user is a legitimate user, whether they can access the network and whether they can use network specific resources. the access control functions of the IPLOOK SMF mainly include security and permission control.

The main security features supported by SMF are.

- Secondary authentication function (CHAP, PAP) EAP (not supported): Secondary authentication is performed on requests initiated by the terminal, and the corresponding service is processed only if the authentication is passed, otherwise the request is rejected. (See Secondary authentication for details)
- Overload control function: rejects new session establishment requests when the system throughput reaches a certain on-line level, ensuring system security.
- State control function: filtering and discarding of illegal or abnormal event requests on the system state machine.

3.2.1.37 License Support

The IPLOOK SMF system supports License authorisation management, providing appropriate authority control for interfaces, services and system access.

License Maintenance Interface.

- Get License (GET)
- Update License (POST)
- Webmaster query interface

Minimal operational support for devices with no license or expired license

Minimalist operations include.

- Basic PDU session creation limit
- Only single NRF registration and single pass type NF acquisition are supported
- Only single UPF connections are supported

Note: No License devices are not supported for services other than minimisation

After authorization of License.

- Number of UPF connections, limited by License service
- Maximum number of PDU sessions, limited by License service
- NRF registered connections control, limited by License service
- Support for all operations on SMF business documents

3.3 UPF

3.3.1 Basic functionalities

3.3.1 .1 Interface Features

3.3.1 .1.1 N3 Interface

The N3 interface mainly interacts with the 5G-AN, which is responsible for the transmission of upstream and downstream user-plane data streams, using the GTPv1 protocol, and the interface protocol stack is shown in the following figure.

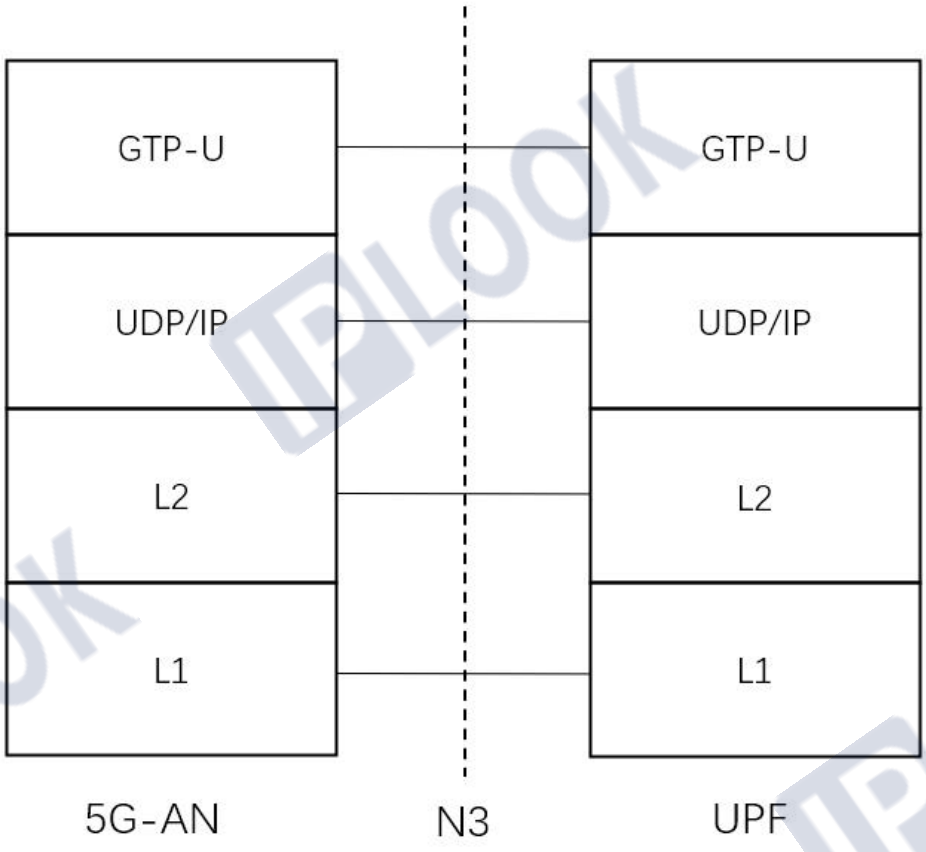


Figure 2.1.1-1 N3 Interface Protocol Stack

The reference standards for N3 interface characteristics are shown below

- 3GPP TS 23.501 System architecture for the 5G System （5GS）
- 3GPP TS 29.281 General Packet Radio System （GPRS） Tunnelling Protocol User Plane （GTPv1-U）
- 3GPP TS 38.415 NG -RAN;PDU Session User Plane Protocol

3.3.1 .1.2 N9 Interface

The N9 interface mainly interacts with the UPF at the opposite end, which is responsible for the transmission of upstream and downstream user-plane data, using the GTPv1 protocol, and the interface protocol stack is shown in the following figure

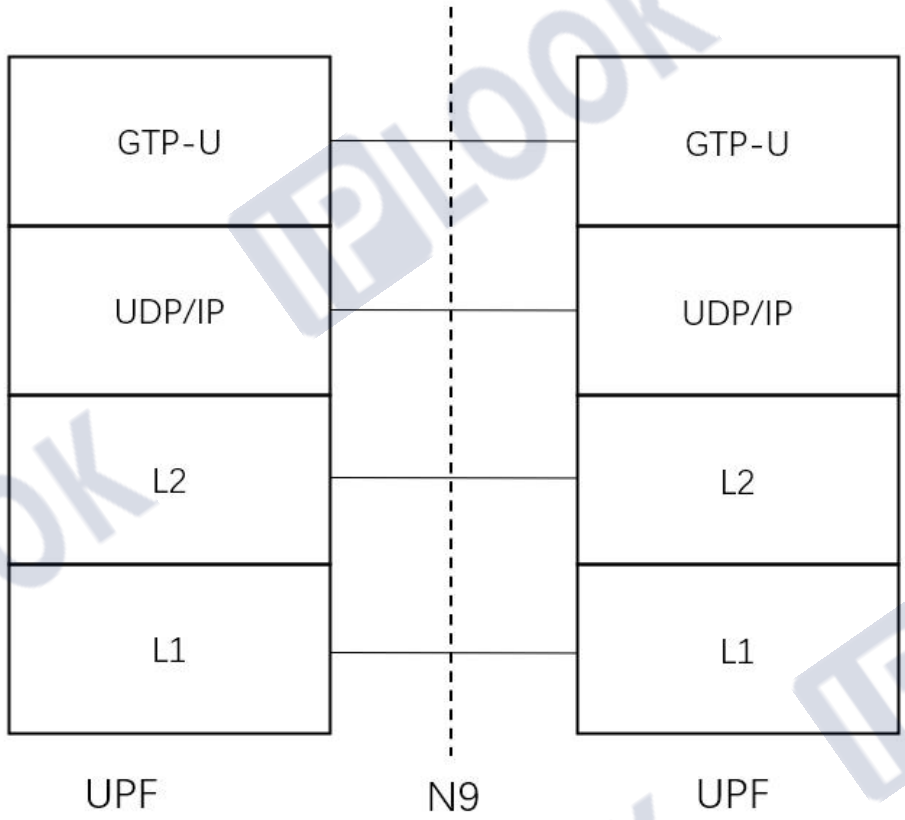


Figure 2.1.1-1 N9 Interface Protocol Stack

The reference standards for the N9 interface characteristics are shown below.

- 3GPP TS 23.501 System architecture for the 5G System （5GS）
- 3GPP TS 29.281 General Packet Radio System （GPRS） Tunnelling Protocol User Plane （GTPv1-U）
- 3GPP TS 38.415 NG-RAN;PDU Session User Plane Protocol

3.3.1 .1.3 N6 Interface

N6 interface mainly interacts with DN, which is responsible for the transmission of upstream and downstream user-plane data, currently only based on the exchange of IP data, and the interface protocol stack is shown in the following figure,

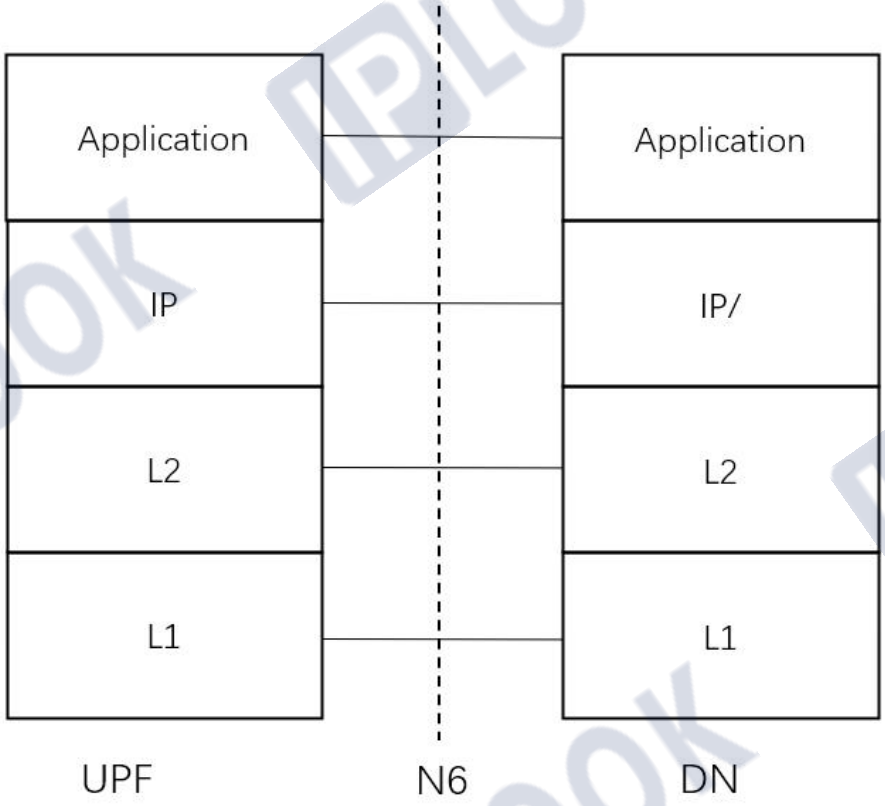


Figure2.1.

1-1 N6 Interface Protocol Stack

The reference standards for the N6 interface characteristics are shown below

- 3GPP TS 23.501 System architecture for the 5G System （5GS）

3.3.1 .1.4 N4 Interface

The N4 interface mainly interacts with CPs that support PFCP entities such as SGW-C, PGW-C, TDF-C and SMF, using the PFCP protocol stack, and the interface protocol stack is shown in the following figure.

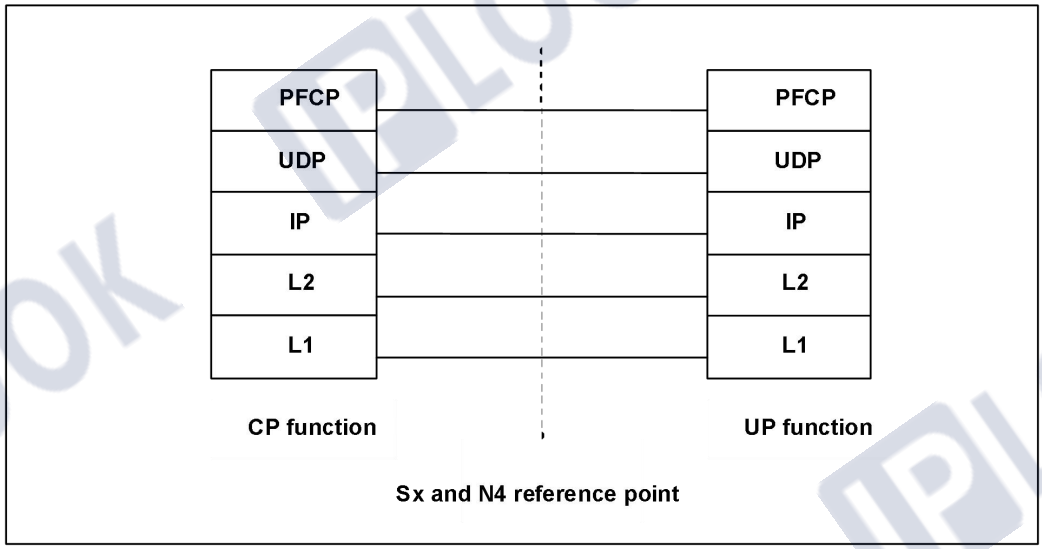


Figure2.1.4-1 N4 Interface Protocol Stack

Reference Standards

3GPP TS 23.501 System architecture for the 5G System （5GS）

3GPP TS 29.244 Interface between the Control Plane and the User Plane Nodes

3GPP TS 23.527 5G System; Restoration Procedures

3.3.1 .1.5 N4u Interface

The N4u interface mainly interacts with CPs supporting PFCP entities such as SGW-C, PGW-C, TDF-C and SMF, and is the user-plane interface between them, using the GTPv1 protocol stack, and the interface protocol stack is shown in the following figure.

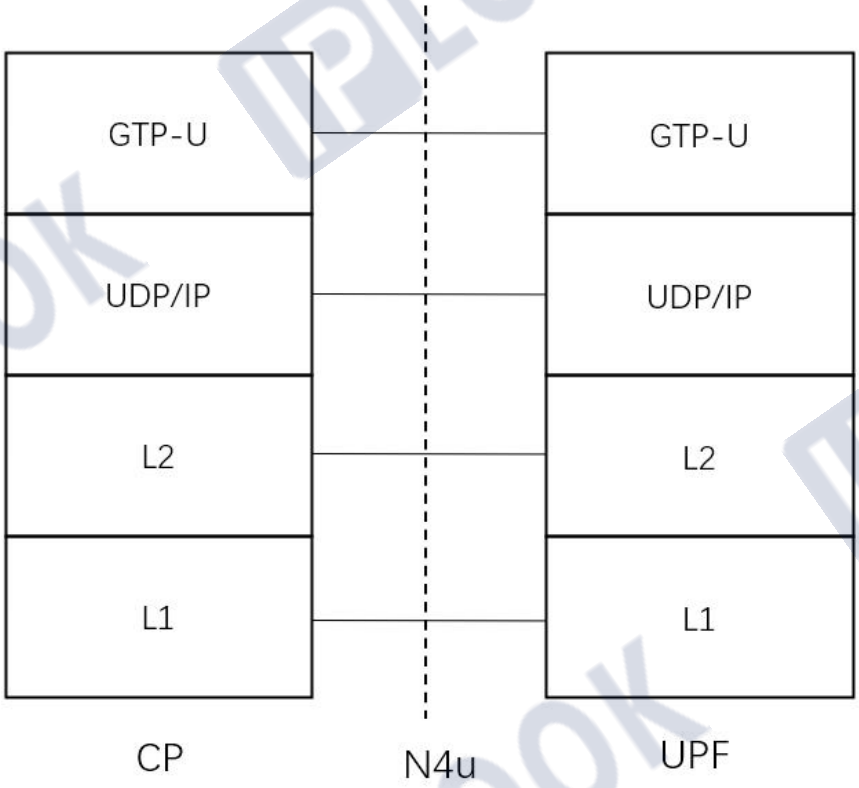


Figure2.1.4-1 N4u Interface Protocol Stack

The reference standards for the N4u interface characteristics are shown below,

3GPP TS 23.501 System architecture for the 5G System （5GS）

3GPP TS 29.281 General Packet Radio System （GPRS） Tunnelling Protocol User Plane （GTPv1-U）

3GPP TS 38.415 NG-RAN;PDU Session User Plane Protocol

3.3.1 .2 User group forwarding

In 5GC, the CP controls the processing of user data packets by providing or activating/deactivating the corresponding rules while creating, modifying or deleting each

session context in the UPF, corresponding to PDR, FAR, QER, URR and BAR, etc. These rules instruct the UPF to adopt certain processing behavior for the user group data of each PFCP session context.

The user data grouping process for each PFCP session context is shown in the following diagram.

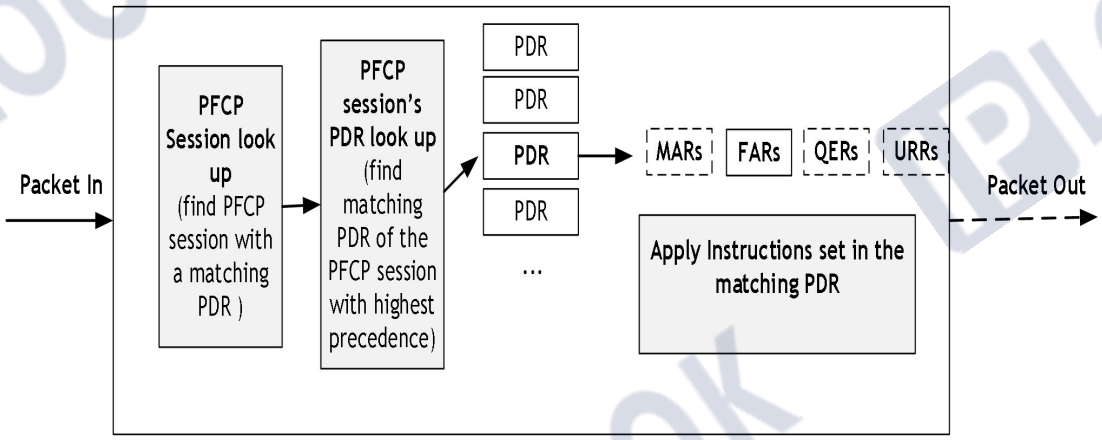


Figure2.2-1 Message flow in UP function

When each user data packet is received, the UPF will first look for the PFCP session context corresponding to the packet, and when it finds it, it will further match the PDR provided by the CP to the UPF in this session context or the PDR predefined by the UPF activated by the CP, otherwise it will be discarded. Accordingly, each PDR has a priority, then UPF will match according to the priority, the matching criterion is the combination of parameters carried by the PDI in the PDR, the parameters are as follows.

- UE IP address
- Local F-TEID
- Network Instance
- SDF filter
- Application ID
- QFI
- Framed Route Information

If neither the PDR nor the predefined PDR can match this user data packet, it will be discarded. When the highest priority PDR is matched, the UPF will further search for the corresponding rule it identifies based on the rule ID of FAR, URR or QER it carries, and then perform usage billing, QoS policy implementation or forwarding behavior control, etc. At this point, the service processing flow of a user data grouping is completed.

3.3.1 .3 Data forwarding between CP and UP

The scenarios applied for user-plane data forwarding between CP and UP are shown in the following table.

	Scenario description	Data forwarding direction	For EPC applicable to	For 5GC applicable to
1	Forwarding of user-plane packets between the UE and the CP function.	UP to CP function CP to UP function	PGW	UPF to SMF SMF to UPF
2	Forwarding of packets between the CP function and the external PDN （over SGi） / DN （over N6）.	UP to CP function CP to UP function	PGW	UPF to SMF SMF to UPF
3	Forwarding of packets subject to buffering in the CP function.	UP to CP function CP to UP function	SGW	UPF to SMF SMF to UPF
4	Forwarding of End Marker Packets constructed by the CP function to a downstream node.	CP to UP function	SGW, PGW	SMF to UPF
5	Forwarding of user data using Control Plane CIoT 5GS Optimisation	UP to CP function CP to UP function	-	UPF to SMF SMF to UPF

Figure2.3-1 Data forwarding between CP and UP

User-plane data forwarding between CP and UP is accompanied by GTP-U encapsulating user data, taking the N4u interface between the two. The current application scenarios supported by UPF are 1, 2, and 4.

3.3.1 .4 Service detection and bearer/QoS flow binding

Service Detection refers to the process by which a PFCP session context allows the UPF to identify the intended user data grouping through a Service Data Flow Filter or Application Detection Filter provided by the SMF. The specific service data flow filter or application detection filter is provided to the UPF by the SMF in the PDI of the PDR rule. currently only IP data grouping filters are supported, each IP data grouping filter consists of a series of parameters in any combination, containing the following parameters.

- IPv4 source or destination address/IPv6 source prefix or destination prefix
- Source or target port (port can be a range, e.g. 20000-21000)
- The upper layer protocol number identified by the IPv4/ IPv6 message header
- Service type of IPv4 message header / Class of service of IPv6 message header
- IPv6 Streaming Tags
- IPv6 Security Parameters Index

- Data grouping filtering direction, upstream, downstream or up/downstream

  For 4/5G converged UPF and SMF, bearer binding is the process of realizing 5G service data streams associated with 4G IP-CAN bearers, in which the service data streams are transmitted on the IP-CAN bearer.

  For the uplink user data packets in the EPC system, the UPF will use the uplink service data flow template provided by the SMF to match these data packets, and discard them if the match fails. The combination of matching parameters configured by the uplink PDR at this time is as follows.

- Local F-TEID
- UE IP address that matches the source address of the IP message
- SDF filter or Application ID

The SMF provides the UPF with a downstream PDR to match the service data mapped to the IP-CAN bearer, and a FAR with a forwarding destination of the downstream bearer (S5/S8 or S1/S12/S4/Iu) is associated to this PDR.

QoS flow binding in 5GC is to associate a service data flow to a QoS flow, in which the service data flow is transmitted on the QoS flow.

For the incoming uplink user data packet, it will go to match the QoS flow corresponding to the uplink direction, when the parameters carried by the uplink PDR provided by SMF are as follows.

- Local F-TEID
- UE IP address that matches the source address of the IP message
- QFI for QoS streams
- SDF filter or Application ID

If this uplink user data grouping fails to match, i.e., it does not match the SDF filter (or Application ID) and the QFI corresponding to the QoS flow, it is discarded.

The downstream user data packet mapped to a QoS flow is matched with a corresponding downstream PDR, which is associated with a QER carrying a QFI identifying the corresponding downstream QoS flow and a FAR whose forwarding destination is the downstream GTP-U endpoint (N9 or N3).

3.3.1 .5 Gating

Gating is the process of turning on or off the forwarding of IP packets belonging to service data streams or inspected application traffic in user-plane functions (PGW-U and TDF-U for EPC, UPF for 5GC) to pass through in order to reach the destination endpoint.

Gating can be applied to either upstream or downstream, and the specific behavior depends on the value in the Gate Status IE in the QER issued.

3.3.1 .6 QoS Control

QoS control refers to the authorization and enforcement of the maximum QoS that is authorized.

For EPC, the main applications are in the following scenarios.

- Session level (APN-AMBR, TDF Session uplink and downlink bit rates or uplink and downlink data packet rates for PDN connections)
- Carrier stage (GBR, MBR for GBR carrier)
- Service data flow level or application level

For 5GC, the main applications are in the following scenarios.

- Session level (uplink and downlink data packet rates for Session-AMBR or PDU sessions)
- QoS Flow Level
- Service data flow level or application level

For SMF instructions to UP to perform QoS control, the relevant instructions are as follows.

- Create PDRs for associated service streams, applications, 5GC QoS streams, bearers or sessions
- Create session-level, service-data flow, or application-level QERs
- Create QER for QoS implementation of aggregated service streams with the same GBR QFI
- Associating session-level QERs to all PDRs in the context of each PFCP session
- Associating the corresponding service-stream-level or application-level QER to a PDR associated to a service data stream or application
- QERs for service data streams associated with shared QERs or PDRs for applications associated with the corresponding aggregated service data streams

3.3.1 .7 Usage monitoring

Usage monitoring and control is the process of monitoring the user plane traffic in PGW-U, TDF-U or UPF to understand the cumulative usage of network resources for each user, with the main monitoring directions

- Single or group of service data streams
- Single or group of applications
- 5GC PDU sessions, but may not include service data streams

- EPC IP-CAN session, may not include service data streams
- EPC TDF sessions, which may not include service data streams

The SMF activates and controls the reporting of UPF usage through the following instructions

- Create a PDR and associate it with the service data stream, application or session to be monitored
- Create an URR and specify the method to be monitored, such as capacity or time
- Associates URR to all PDRs in the PFCP session context for usage monitoring in IP-CAN sessions or TDF sessions, but may not include PDRs for matching service data streams or applications
- Associated URR to PDRs in the context of PFCP sessions for monitoring at the service data flow level or at the application level

3.3.1 .8 Predefined PCC/ADC rules

The SMF can enforce activated predefined PCC or ADC rules in the UPF via PCRF/PCF by

- Determine the service data filter or application ID referenced by the activated predefined PCC or ADC rule and the corresponding QoS and billing control information, respectively;
- Create the necessary PDRs to identify the service data streams and applications covered by the predefined PCC or ADC rules if they do not previously exist
- Create the necessary QERs to implement QoS at the service data stream or application level respectively

- If new FARs need to be created due to bearer binding (for EPC) or QoS flow binding (for 5GC) and QoS control for forwarding detected service data flows or application services, create the necessary FARs or redirect or apply flow control (if included in predefined PCC/ADC rules)
- Create the necessary URRs for each combination of monitoring object, billing object, billing object and service ID or combination of billing object, sponsor ID and application service provider ID (if included in a predefined PCC or ADC rule)
- Then associate URR to the newly created PDR

Associate an existing FAR or a new FAR to a newly created PDR

Optionally, a common service processing policy for multiple PFCP sessions may be configured on the UPF, i.e. predefined rules such as PDR/QER/FAR/URR. The SMF may be activated by a Create PDR IE in a PFCP Session Establishment Request message or an Update PDR IE in a PFCP Session The SMF can activate these traffic processing by including the Activate Predefined Rules IE in the Create PDR IE in the PFCP Session Establishment Request message or the Update PDR IE in the Modification Request message or by including a predefined FAR/URR/QER ID (where the highest valid bit is set to "1"). policy.

If the SMF activates a service processing policy by containing predefined FAR/URR/QER IDs, i.e., the eighth bit of the above ID value is set to "1", and subsequent SMFs containing Create/Update FAR/URR/QER IEs should no longer use these IDs.

If the received Create/Update PDR IE contains both the Activate Predefined Rules IE and the predefined FAR/URR/QER ID (the eighth bit is set to "1"), how the UPF processes the message depends on the specific implementation. For the above case, the UPF either overrides the FAR/URR/QER rule associated by the Activate Predefined Rules IE with the FAR/URR/QER rule identified by the received FAR/URR/QER ID, or it rejects the message and responds with a

Cause IE value of " Rule creation/modification Failure" while carrying the Failed Rule ID IE to indicate the rule that caused the error.

If the PDR used for service matching is associated with activated predefined rules, the UPF shall implement these rules. If the URR rule, the UPF will still generate the corresponding Usage Report information and report it to the SMF according to the measurement method indicated by this rule.

For predefined rules that have been activated on the UPF, the SMF can include the Deactivate Predefined Rules IE in the Update PDR IE of the PFCP Session Modification Request message to inform the UPF to activate the predefined rules for the relevant PDR.

To de-activate a predefined FAR/URR/QER rule previously activated on the UPF by a Create PDR IE or Update PDR IE containing a predefined FAR/URR/QER ID, the SMF can include the Remove FAR IE, Remove URR IE and/or Remove QER IE in the PFCP Session Modification Request message. Remove URR IE and/or Remove QER IE to remove the corresponding predefined FAR/URR/QER IDs.

3.3.1 .9 Billing

In the following scenarios, SMF supports billing behavior by activating the measurement and reporting of cumulative network resource usage in the UPF

- For EPC，
  - IP-CAN Bearer on SGW
  - IP-CAN bearer on PGW, IP-CAN session and/or single or group of service data streams
  - TDFsessions and/or individual or groups of applications on TDF
- For 5GC，

- PDU sessions and/or single or group service data streams on SMF
- QoS flow on SMF

The SMF will control the UPF for dosage measurement and reporting through the following instructions.

- Create PDRs for associated service data streams, applications, bearers or sessions
- Create URR for specified measurement methods
- Associate the URR to the relevant PDR defined in the PFCP session context for use in IP-CAN bearers, IP-CAN sessions, TDF sessions, service data streams or application level usage escalation

For online billing, the SMF provides a capacity (or time) quota to the URR, if a quota threshold is received from the OCS.

3.3.1 .10 Requested/unsolicited application uploads

In EPC, the requested/unsolicited application upload is the process of TDF or PCEF uploading the application to start the service or stop the service.

In 5GC, the requested application upload is the process of SMF to PCF to upload the application to start the service or stop the service.

For the above scenario, the UPF will detect and report the behavior of the application through the following instructions.

- Create the PDR associated with the application to be detected
- Create URR and instruct Repotrting Trigger IE to monitor the start or stop of business data

- Also this URR may contain a zero quota and a Quota Action IE, where the Quota Action IE specifies a FAR to instruct the UP function to drop or buffer packets associated with detected application traffic before the quota is granted in subsequent PFCP session modification request messages.

- Associate this URR to PDR

When the application is detected to be in service or out of service, the UPF will initiate a PFCP Session Report request to the SMF and specify the type of report as Usage Report, and set the Usage Report Trigger to the corresponding 'Start of Traffic' or 'Stop of Traffic'. ' or 'Stop of Traffic'.

In the process of initiating a PFCP Session Report request, the UPF also carries the following information to the SMF in the Usage Report.

- When the application is detected to start using the service, it carries the following information
  - Match the application ID of this user data group
  - Stream information, including the direction of the stream, source IP, destination IP and port, etc.
  - Application Example Identification
  - Multiple PDN overlapping IP addresses and Network Instance when the UE IP address is not provided to the UPF
- When the application is detected to stop using the service, it carries the following message
  - Match the application ID of this user data group
  - The application instance identifier when the reporting application starts using the service

- Multiple PDN overlapping IP addresses and Network Instance when the UE IP address is not provided to the UPF

3.3.1 .11 F-TEID allocation and release

When the UPF establishes a PFCP Association with the SMF, the FTUP flag in the UP Function Features IE is set to "1" to tell the SMF that it supports the assignment of F-TEIDs. Subsequently, in the PFCP Session Establishment Request or PFCP Session Modification Request message, the SMF can request the UPF to assign the F-TEID, as follows.

- Set the CHOOSE flag position of the Local F-TEID IE in the PDR rule to "1"
- If multiple PDR requests in the same PFCP session context are assigned the same F-TEID, the CHOOSE ID flag position of the Local F-TEID IE is set to "1" and carries the same CHOOSE ID value at the same time.

When the F-TEID is successfully assigned by the UPF and this PDR is successfully created, the requested assigned F-TEID will be present in the PFCP Session Establishment Response or PFCP Session Modification Response message, which is responded to the SMF by the UPF.

3.3.1 .12 PFCP Session Management

The SEID is used by the same PFCP entity to uniquely identify a PFCP session, and the SEID provided by the other party is required to interact with PFCP session-related messages between PFCP entities. the specific interaction process between SMF and UPF is as follows.

- The SMF initiates a PFCP Session Establishment Request message, which contains the SEID value of the SMF side and its IP address in the F-SEID IE

- UP responds to SMF through PFCP Session Establishment Response message and carries its own SEID in this message, similarly, UPF's SEID is also included in F-SEID IE
- For subsequent PFCP session-related messages, the SMF and UPF each interact using the SEID previously provided by the other and transmit it in the message
- When the PFCP session is released, the SMF and UPF will each release the SEID corresponding to the session

When the PFCP session context needs to be modified, the SMF will provide the UPF with the appropriate instructions to request it to create a new IE, modify or remove an existing IE.

3.3.1 .13 PFCP association management

When establishing a PFCP session context through UPF, a PFCP association needs to be established between SMF and UPF first, and for a given SMF and UPF, only one PFCP association can be established between them. the PFCP association initiator can be either SMF or UPF, depending on the actual deployment for the specific application.

Each SMF can establish a PFCP association with multiple UPFs, and similarly, a UPF can establish a PFCP association with multiple SMFs. After this, the SMF or UPF can identify itself to the peer by a unique Node ID, which can be either an IP address or an FQDN; FQDN is not currently supported by the UPF.

3.3.1 .14 Error Indication Handling

For UPF forwarding downlink user data packets to the 5G-AN, the GTP-U Error Indication message is triggered, as shown in the following figure.

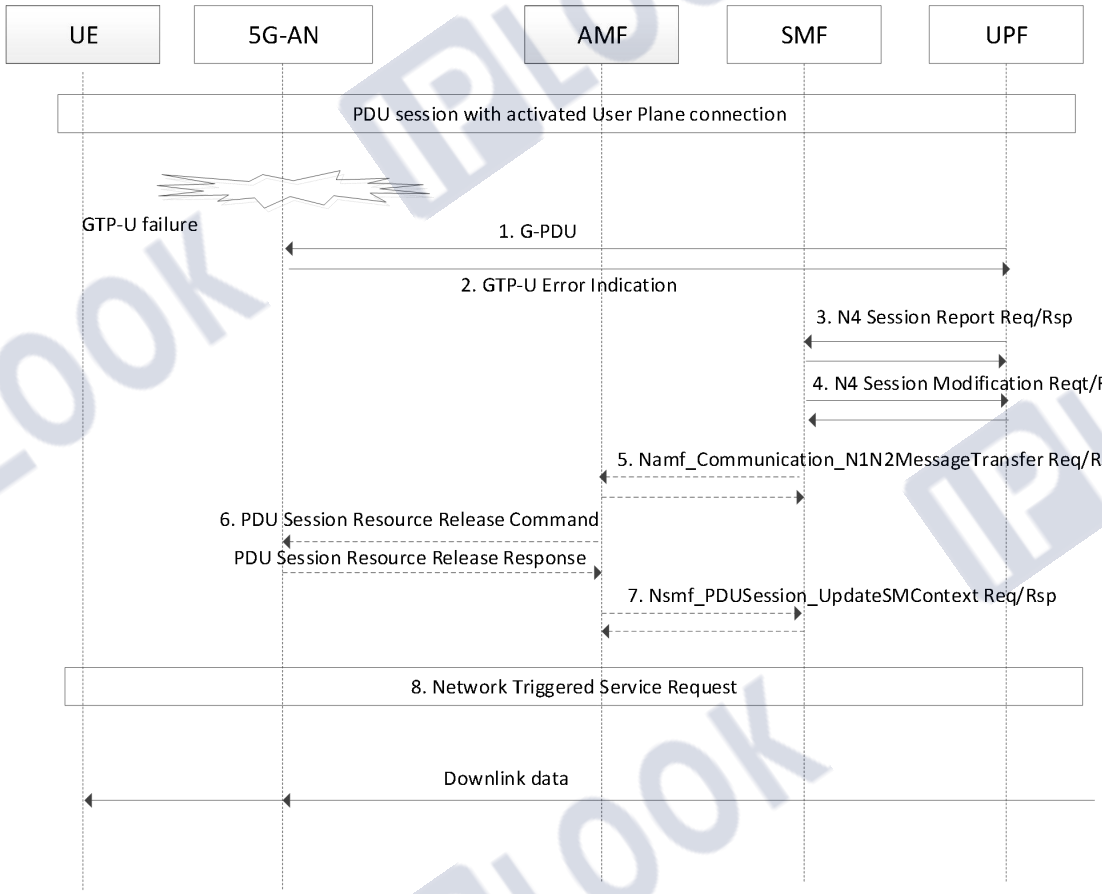


Figure2.14-1 5G-AN initiates Error Indication messages

Corresponding to steps 2 and 3 of the above diagram, the UPF will take the following steps to process at this time，

- Find the corresponding PFCP session context based on the GTP tunnel information identified in the GTP-U Error Indication message, i.e., TEID and IP address
- Initiate a PFCP Session Report request to the SMF and identify the Report Type as 'Error Indication Report' type and carry the F-TEID that triggered this Error Indication message

3.3.1 .15 User Plane inactivity detection and reporting

In the context of an established PFCP session, the SMF can provide the User Plane Inactivity Timer IE in the PFCP Session Establishment Request or PFCP Session Modification Request message to specify the user-plane inactivity detection period When the UPF detects that no user-plane data group has arrived within this period, it initiates a PFCP Session Report Request message to the SMF and identifies the Report Type as 'User Plane Inactivity Report' type. The UPF will then continue to process any subsequent user-plane packets according to the rules previously received by this PFCP session context until any new indication is received from the SMF.

3.3.1 .16 IPv6 Prefix Authorization

To assign an IPv6 network prefix shorter than the default/64 prefix to a PDN connection or PDU session, IPv6 prefix authorization can be performed via DHCPv6. In this process, the SMF performs the assignment or, provided that the UPF supports the UEIP feature, requests the UPF to perform the assignment of an IPv6 network prefix shorter than the default/64 prefix, with the following processing steps.

- In the UE IP Address IE, set the IPv6D flag to "1" and specify the length of the prefix to be delegated in the IPv6 Prefix Delegation Bits field, e.g. if the value is 4, it means that the /60 prefix is used for delegation.
- Alternatively, if the UPF supports the IP6PL feature, it can also be delegated by setting the IP6PL flag in the UE IP Address IE to "1" and specifying the length of the prefix to be delegated in the IPv6 Prefix Length field, e.g., a value of 60 means that the /60 prefix will be used. If the value is 60, it means that the /60 prefix is used for delegation.

- When the assignment is made by the SMF, the value in the IPv6 Prefix Delegation Bits or IPv6 Prefix Length field above is specified by the SMF. If the allocation is done by UPF, the value of the above two fields is 0. The specific value is determined by UPF.

3.3.1 .17 Post-routing

Post-routing supports IP networks behind the UE, allowing multiple IP addresses or multiple IPv6 prefixes to enable data interaction with remote networks through a single PDU session, for example for enterprise network connections. Post-routing is only used for PDN connections or IP type PDU sessions (IPv4 or IPv6).

The UPF can set the FRRT flag bit in the UP Function Features IE to tell the SMF that it supports post-routing features. When the SMF confirms that the UPF supports post-routing, it can instruct the UPF to enable the post-routing feature by following these steps.

- The issued PDR rules carry Framed-Route IE, Frame-Routing IE and Framed-IPv6-Route IE
- For upstream user data packets, the source IP address in the IP message needs to be matched with the IP address or IPv6 prefix in the Framed-Route IE or Framed-IPv6-Route IE.
- For downstream user data packets, the destination IP address in the IP message needs to be matched with the IP address or IPv6 prefix in the Framed-Route IE or Framed-IPv6-Route IE

3.3.1 .18 Uplink classifier and branch point

Uplink classifier and branch point is the ability of the UPF to route uplink service flows from the same PFCP session (PDU session) to two or more PDU session anchors, while routing downlink service flows from PDU session anchors to the UE on the GTP tunnel.

The uplink classifier supports IP-type PDU sessions as well as Ethernet-type PDU sessions. Routing of uplink service flows to different PDU session anchors, such as destination IP addresses/IPv6 prefixes of uplink packets based on IP-type PDU sessions.

The branch supports IPv6 multi-homing PDU sessions, i.e., a single PDU session supports multiple IPv6 prefixes. Routing of uplink service flows to different PDU session anchor points is based on the source IPv6 prefix of the uplink packet.

SMF can insert uplink classifiers or branch points during PDU session creation or modification, by following the steps below.

- Two or more uplink PDRs are issued at the uplink classifier or branch point to match the corresponding uplink service flows, and an appropriate FAR is bound to this PDR for routing these uplink service flows to the appropriate PDU session anchor point.
- Two or more downlink PDRs are issued at the uplink classifier or branch point to match the downlink traffic from the PDU session anchor point, and an appropriate FAR is bound to this PDR to route the downlink traffic on the tunnel to the UE.

SMF can remove uplink classifiers or branch points during PDU session modification, by following the steps below.

- The uplink PDR matching the uplink service flow from the uplink classifier or branch point is removed at the PDU session anchor point, while the downlink FAR of the

downlink service flow routed to the uplink classifier or branch point is removed or modified to route to the 5G-AN tunnel.

3.3.1 .19 Data forwarding during 5GS and EPS switchover

When 4G interoperates with 5G, the switching process between the 5GS system and the EPS system can use direct or indirect data forwarding to forward downlink data.

Direct data forwarding is performed directly between the source RAN and the target RAN without any UPF forwarding data involved.

The indirect data forwarding during 5GS and EPS switching is specified as follows.

- For the 5G to 4G switchover, the source NG-RAN node sends one or more End Marker packets containing a QFI from one of those QoS flows mapped to the same E-RAB, which are then sent to the UPF via a PDU session tunnel. the UPF removes the QFI and maps it to the appropriate E-RAB tunnel to the SGW. RAB tunnel.
- For 4G to 5G switchover, the source eNB forwards the received End Marker packets in the EPS bearer tunnel to the SGW, which forwards them to the UPF. the UPF adds a QFI from the QoS flow mapped to that E-RAB to the End Marker and sends them to each PDU session tunnel in of the target NG-RAN node.

In order to forward data (G-PDUs and End Marker) during the 5GS to EPS switchover, the SMF should,

- A PDR for each E-RAB (supporting data forwarding for at least one QoS flow) and a list of QFIs mapped to the E-RAB;

- Request the UPF to remove the GTP-U PDU from the data by including the GTP-U Extension Header Deletion field set to "PDU Session Container" in the Outer Header Removal IE of the PDR Session Container (including QFI);
- Associate a FAR for each PDR to forward data to the corresponding E-RAB's GTP-U tunnel, i.e., use the Outer Header Creation IE that contains the F-TEID for forwarding to the SGW for the corresponding GTP-U tunnel.

In order to forward data (G-PDUs and End Marker) during EPS to 5GS switchover, the SMF should,

- Each E-RAB provides a PDR (supports data forwarding of at least one QoS flow)
- Create a QER containing a QFI IE associated with each PDR, the value of the QFI IE is set to the QFI value of a QoS flow mapped to the E-RAB to request the UPF to insert a GTP-U PDU Session Container containing the above QFI.
- Create a FAR for each data forwarding tunnel in the 5GS (i.e., for each PDU session), where the Outer Header Creation IE contains the F-TEID of the target NG-RAN corresponding to the forwarding GTP-U tunnel.
- Associate each PDR with the corresponding FAR (i.e., forward data from each E-RAB to the data forwarding tunnel for the corresponding PDU session)

3.3.1 .20 Activation and de-activation of predefined PDR rules

To reduce signaling overhead and improve signaling efficiency in establishing PFCP sessions (for PDU sessions or PDN connections), the CP and UP functions can support activation and deactivation of a Pre-defined PDR (ADPDP) function as described below.

When both the SMF and UPF support ADPDP functionality, the SMF can activate one or more predefined PDR rules configured on the UPF for a PFCP session in a PFCP Session Establishment Request or PFCP Session Modification Request message.

The predefined PDR may contain all the necessary packet detection information to enable identification of service data flows or application traffic common to multiple PFCP sessions and may be associated with a predefined FAR, one or more predefined QERs, and/or one or more predefined URRs in the UPF.

Any PFCP session-specific information, such as service endpoint information, which is not available as part of a predefined PDR rule and is provided to the UPF before or during the activation of a predefined PDR rule.

To activate one or more predefined PDRs, the SMF will provide one or more Activate Predefined Rule IEs in the Create PDR IE of the PFCP Session Establishment Request message or in the Create PDR IE or Update PDR IE of the PFCP Session Modification Request message. The above mentioned Create PDR IE or Update PDR IE will carry the following information, while the above mentioned Create PDR IE or Update PDR IE will carry the following information

- Service endpoint information is used to match the corresponding service flow, such as Local F-TEID, UE IP Address or Traffic Endpoint ID
- Optionally, a QFI corresponding to the service flow exists to be used for matching, such as an uplink PDR for uplink QoS flow binding
- Priority of this PDR
- Optionally, provide a FAR containing corresponding instructions for the subsequent processing of the user data groupings matched by the predefined PDR; when present,

the UPF will implement the behavior indicated by this FAR rule in place of the predefined FAR associated in the predefined PDR rule

- Optionally, in addition to any URR specified in the predefined PDR, one or more URRs will be used, such as for session-level usage monitoring
- Optionally, one or more QERs will be used in addition to any QERs specified in the predefined QERs, such as the QoS implementation for APN-AMBR.

When a given PDR is used to activate a predefined PDR, the user data packet is successfully identified by the given PDR if the incoming user data packet matches the service endpoint information carried by the given PDR, the possible QFIs, and one of the activated predefined PDRs.

The SMF can update the PFCP Sessions that have been The use of predefined PDRs that have been activated in the PFCP session by updating the parameters provided in the PDR.

SMF can deactivate the predefined PDRs that are already active in the PFCP session by carrying the Deactivate Predefined Rules IE in the PFCP Session Modification Request message.

In addition, this feature allows the definition of a set of predefined PDRs that can be activated, updated and deactivated together. This allows SMF to further optimize UPF-oriented signaling.

To activate, update or deactivate a set of predefined PDRs, the SMF shall follow the same procedures as for activating, updating and deactivating individual predefined PDRs, and the SMF shall use an Activate Predefined Rules IE associated with a set of predefined PDRs.

3.3.1 .21 UE IP address/prefix assignment on the UPF side

When the UPF supports UE IP address/prefix assignment, the SMF will request the UPF to perform UE IP address/prefix assignment by the following steps.

- Setting the CHOOSE flag in the UE IP Address IE of the PDR indicates that the UE IP address/prefix is assigned by the UPF
- The PDR contains the Network Instance IE to indicate which IP address pool the assigned UE IP address/prefix belongs to,
- The PDR optionally contains the UE IP address pool identifier from which the UPF assigns the UE IP address

Also, in the PFCP Session Establishment Request or PFCP Session Modification Request message, the SMF can request the UPF to assign the same UE IP address/prefix by creating multiple new PDR rules, or in the PFCP Session Modification Request message, the SMF can request the UPF to assign the same UE IP address/prefix by creating multiple new PDR rules, or by modifying multiple existing PDR rules in the same way.

When a PDR is successfully created or modified in a PFCP Session Establishment Resquest or PFCP Session Modification Resquest message, the UPF response to the SMF in the PFCP Session Establishment Response or PFCP Session Modification Response message to the SMF will carry all the UE IP addresses/prefixes that have been assigned to this PDR.

When removing a PFCP session context, the UPF will release these UE IP address resources when removing to the last PDR associated with a UPF-assigned UE IP address/prefix.

3.3.1 .22 Downlink data transfer status with UPF buffering

If the UPF supports downlink data transfer status notification with UPF buffering, the UPF shall set the DDDS feature flag in the UP Function Features IE. If yes, the SMF can request the UPF to notify the first buffered downlink user data packet and/or the first dropped downlink user data packet matching the downlink PDR by setting the BUFF flag, BDPN flag and DDPN flag in the

Apply Action IE of the FAR. In addition, the SMF can also provide the DL Buffering Duration IE and DL Buffering Suggested Packet Count IE to the UPF in the BAR.

When the first downlink user data packet indicated to be buffered in the service data stream identified by the downlink PDR is received, the UPF initiates a PFCP Session Report Request message with a Downlink Data Report IE that contains a PDR matching the downlink user data packet being buffered. In addition, when the UPF is instructed to buffer downlink user data packets, if the time set in the DL Buffering Duration IE in the BAR or the number of packets specified in the DL Buffering Suggested Packet IE is exceeded, the UPF also reports the first dropped downlink user data packet in each service data stream identified by the PDR. Packets.

If the UPF supports downlink data transmission status notification with UPF buffering, the SMF can also request the UPF to drop the downlink user data packet directly and send a notification of this service flow matching the downlink PDR by setting the DROP flag and DDPN flag in the Apply Action IE of the FAR.

The UPF sends a PFCP Session Report Request message to report the discarded downlink user data packets in each service data stream identified by the specified PDR, and this message will contain the Downlink Data Report IE, which is used to indicate the above PDR.

3.3.1 .23 Cache uplink user data groups for online billing

If the UPF indicates in the UP Function Features IE that the Quota Action (QUOAC) feature is supported and the FAR specified in the Far ID for Quota Action IE in the URR rule is set to buffer application traffic at zero quota, the UPF shall buffer the associated uplink user data packets, provided that the Zero quota has been set in advance or the quota has been exhausted. In addition, if the UPF has instructed support for the feature UL/DL Buffering Control (UDBC), the UPF shall buffer the number of user data packets (including uplinks or downlinks)

as indicated in the Suggested Buffering Packet Count IE in the BAR rule provided by the SMF until a new instruction is received from the SMF new instructions, e.g., when a new quota is granted.

3.3.1 .24 CallTrace

CallTrace is an important analysis method in the core network system, which can collect Trace information of multiple network elements and users for daily operation and maintenance and service troubleshooting. uPF only supports Trace information collection for services on N4 interfaces, which mainly involves signaling issued during the creation, modification, deletion and reporting of N4 PFCP Sessions.

3.4 UDM/AUSF

Integrated with HSS, pls check the product description on HSS

3.5 PCF

Integrated with PCRF, pls check the product description on PCRF

3.6 NRF

3.6.1 Basic functionalities

3.6.1 .1 Overview of the basic functional features of NRF

3.6.1 .1 .1Definition

The 5GC network adopts a service-based architecture that abstracts the control plane functions into multiple independent Network Functions (hereinafter referred to as NFs), each of which supports multiple services (hereinafter referred to as NFSs).
The NRF is responsible for the automated management of all NFs/NFSs, including functions such as NF registration, NF de-registration, NF updates, NF status subscriptions, and NF status notifications.

3.6.1 .1 .2 Customer Value

beneficiaries	Description of benefits
Operator	Agile network deployment, enabling self-registration of network functions to quickly deliver the services customers need.
Subscriber	The user does not perceive the feature.

3.6.1 .1 .3 Application Scenarios

- NF **Registration: the** first time an NF comes online to provide network services, it needs to register with the NRF first.

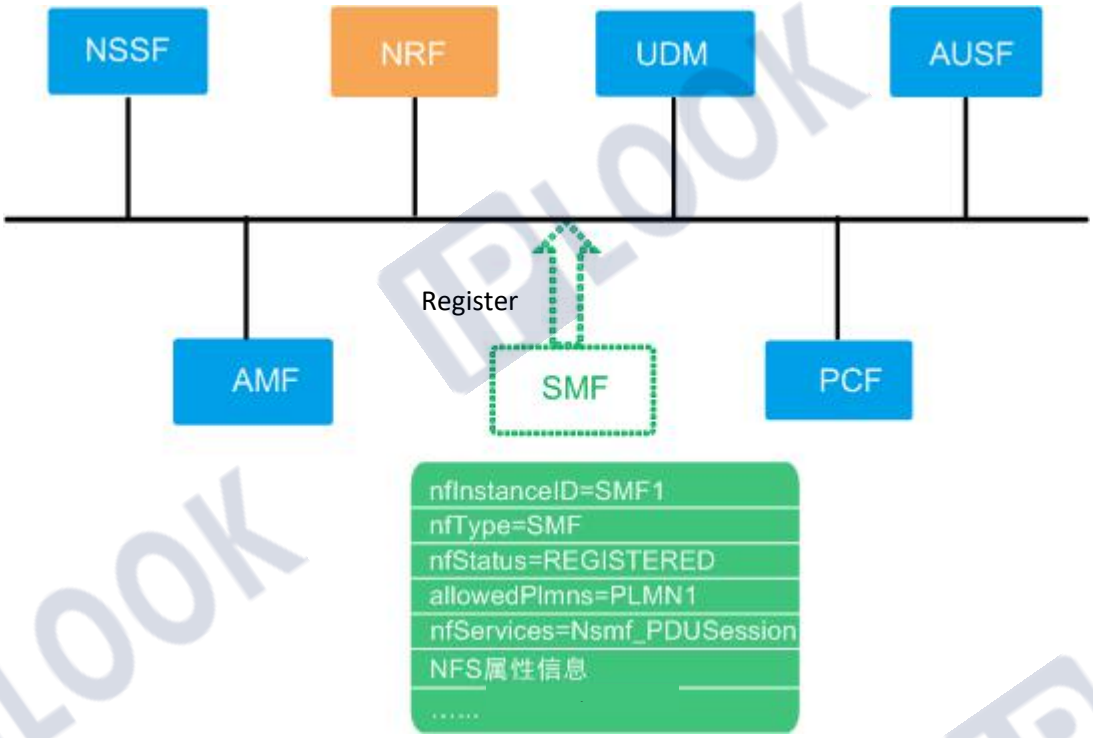


Figure 1 *Example of NF registration*

- **NF de-registration:** When NF gracefully powers down, you need to de-register.

De-

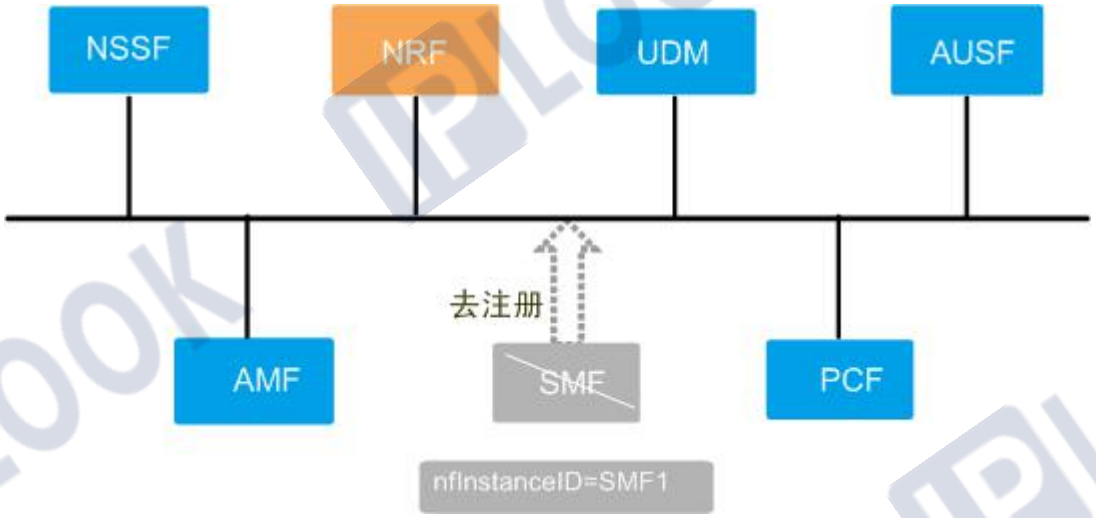


Figure 2 *Example of NF de-registration*

- NF **Update:** Changes to a registered NF/NFS Profile, such as the NF updating its capabilities by way of a software upgrade, extending the NFS, a change in the NF status, a change in the slicing of the NF service, a change in the scope of the NF accessible authorization, etc., will initiate the NF update process to the NRF.

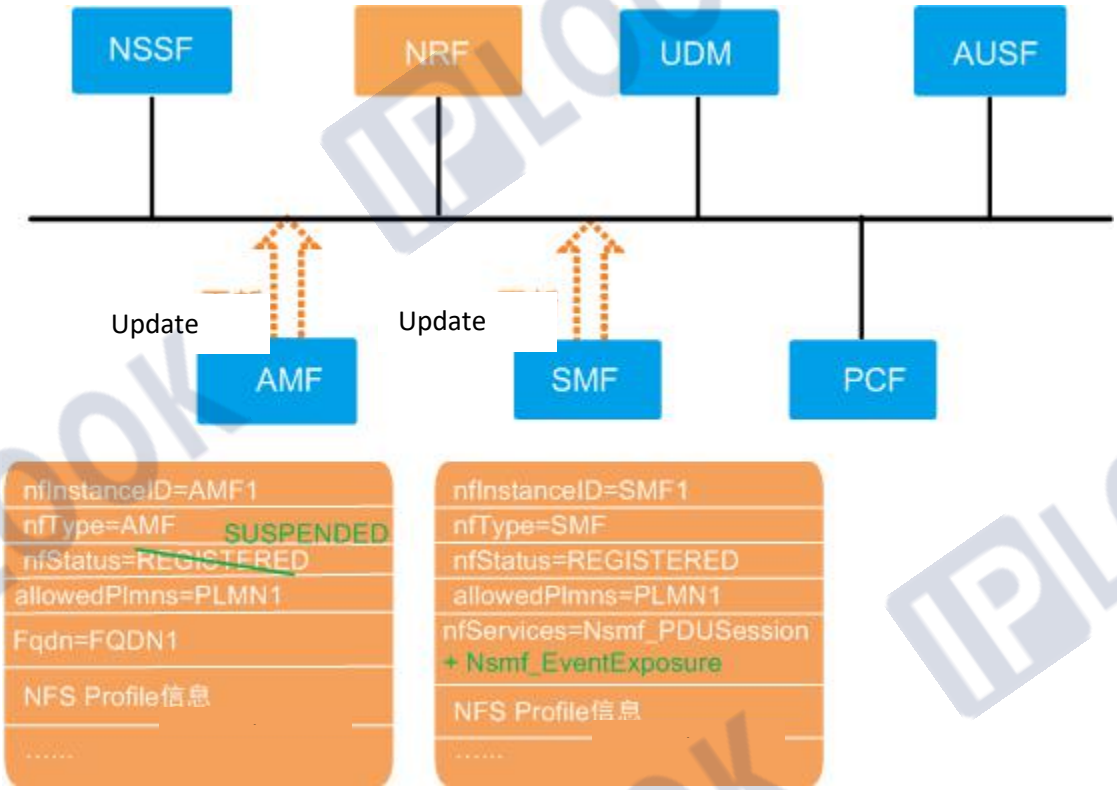


Figure 3 *Example of NF update*

- **Status subscription/notification scenario: an** NF wishing to know about registration or update or de-registration changes of other NFs/NFSs can subscribe to the NRF for the status information of this NF/NFS, as shown in Figure 4. When the state of the subscribed NF/NFS changes, the NRF sends the corresponding subscription notification.

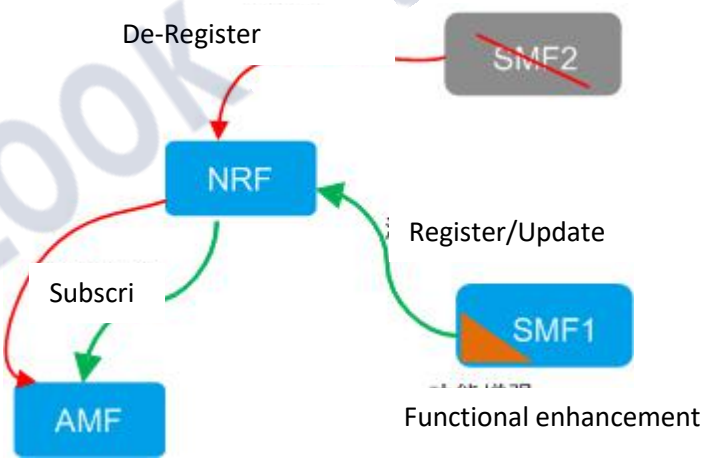


Figure 4 *AMF subscribes to SMF registration, renewal and de-registration*

3.6.1 .1 .4Accessibility

Involved NF

Involving NF	Function description
NRF	Supports NF registration, de-registration, update, and status subscription/notification functions.
Other NFs on the 5GC control surface	Supports NF registration, de-registration, update, and status subscription processes initiated to the NRF.

3.6.1 .1 .5Application restrictions

NFs can only register with the NRF to which they belong, and are not allowed to register across PLMNs (Figure 5), or across regions on the same layer (Figure 6).

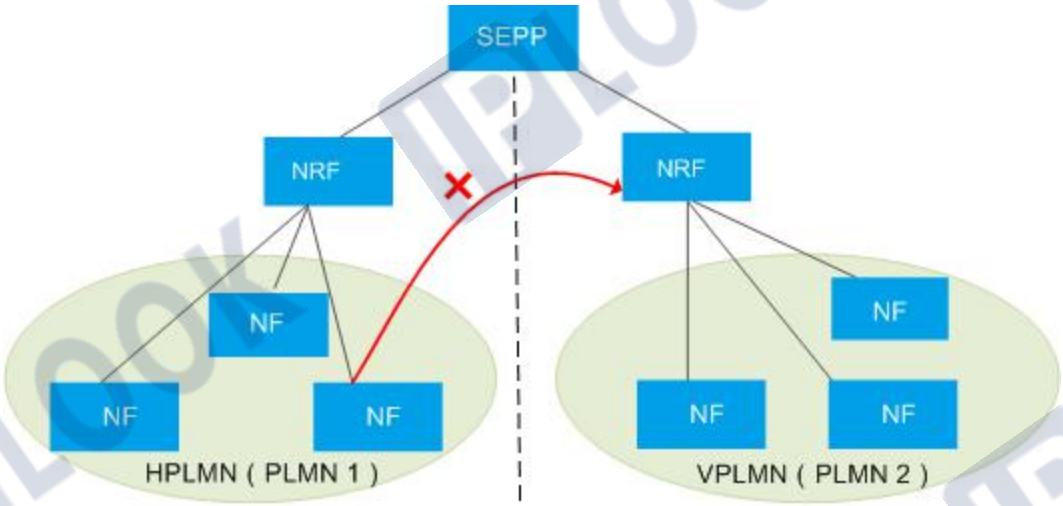


Figure 5 *Disallowing cross-PLMN registration*

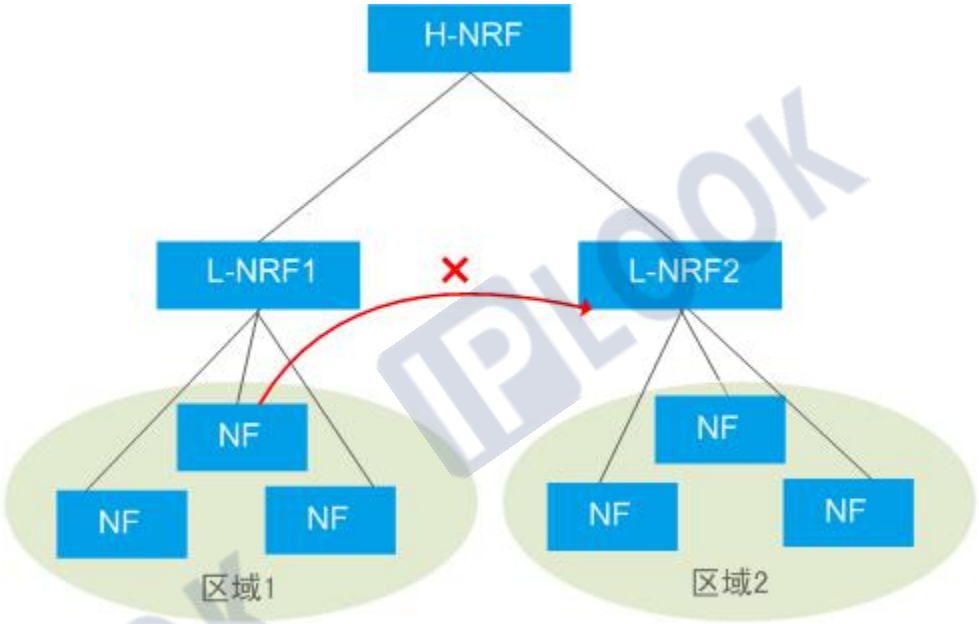


Figure 6 *Disallowing same-tier cross-regional registration*

3.6.1 .1 .6 Principle Overview

The 5GC network adopts a service-based architecture, which abstracts the control plane functions into multiple independent Network Functions (hereinafter referred to as NFs), such as AMF, SMF, NRF, NSSF, etc., as shown in Figure 7. Each NF supports multiple services (Network Function Service, hereafter referred to as NFS).NRF provides three NF registration management (Nnrf_NFManagement), NF discovery service (Nnrf_NFDiscovery), and NF Token authentication service (Nnrf_AccessToken) NFS.

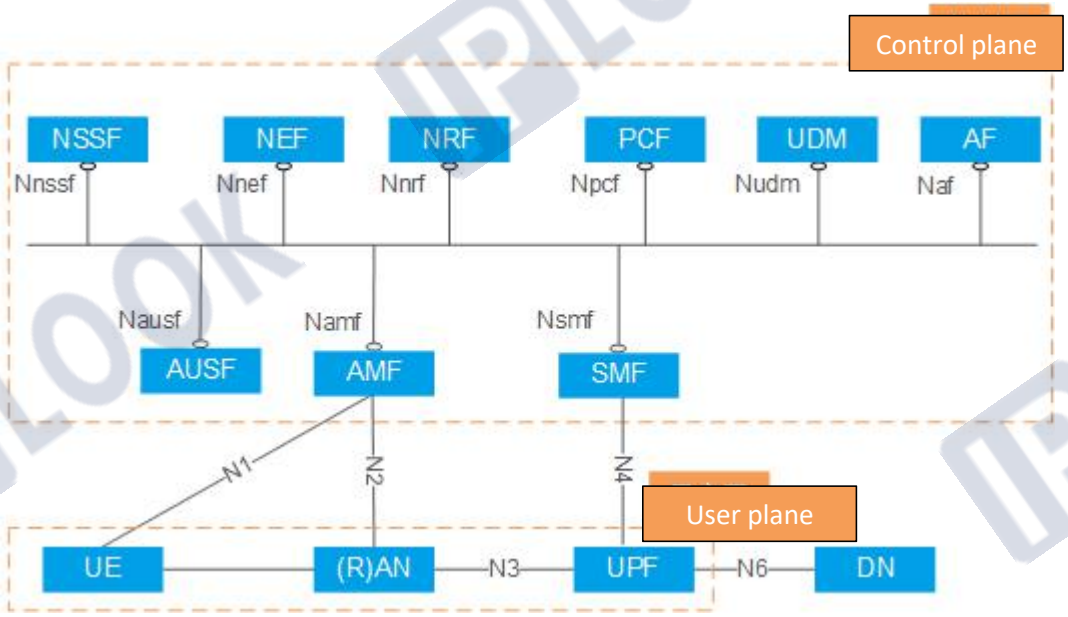


Figure 7 *5GC Network service based Architecture*

3.6.1 .1 .7 NF Registration

In the 5GC network, the NRF is responsible for the automated management of all NF/NFS, which includes NF registration and access authorization control, served by Nnrf_NFManagement.

NF Registration Process

After the NF is instantiated and the NF completes interfacing with the NRF, it initiates a registration request to the NRF to report its own NF/NFS Profile, and the registration process is shown in Figure 8.

Figure 8 *NF registration process*

1. The NF sends a Nnrf_NFManagement_NFRegister_Request message to the NRF requesting registration, carrying the NF/NFS Profile information associated with this NF (nfInstanceID, nfType, nfStatus, nfServices, heartBeatTimer, plmnList, sNssais, etc., where the nfInstanceID uniquely identifies the NF).
2. The NRF processes the registration request from the NF and performs the appropriate checks and saves the NF/NFS Profile record after passing.
3. The NRF returns the Nnrf_NFManagement_NFRegister_Response message to the NF.

NF/NFS access authorization control

- The NF/NFS may have a corresponding access authorization policy for authorization judgment and control during NF/NFS discovery. When access authorization control is applied to the NF/NFS, access to NF/NFS within the authorization range is allowed; if access authorization control is not applied, the NF/NFS can be accessed by any registered NF/NFS.
- The access authorization control policy can be carried during NF registration or NF/NFS updates, and the access authorization control policy can be configured on the NRF.

The final control strategy is shown in Table 1.

Table 1 Access authorization control policies

Type of access authorization control (select as required, multiple options available)	Control 1: Carry access authorization attribute at registration (NF, NFS can carry it separately)	Control 2: Configure access authorization on the NRF (Effective for NF, NFS synchronization)	final strategy
Allow access only to NFs within a specific PLMN	Carry allowedPlmns when registering	**ADD ALLOWEDPLMNS**	Takes the access authorization intersection.
Allow access only to specific NF types	Carry allowedNfTypes when registering	**ADD ALLOWEDNFTYPES**	
Allow access only to specific NF Domains	Carry allowedNfDomains when registering	**ADD ALLOWEDDOMAINS**	

Table 1 Access authorization control policies

Type of access authorization control (select as required, multiple options available)	Control 1: Carry access authorization attribute at registration (NF, NFS can carry it separately)	Control 2: Configure access authorization on the NRF (Effective for NF, NFS synchronization)	final strategy
Allow access only to NFs that support specific slices	Carry allowedNssais when you register	**ADD ALLOWEDNSSAIS**	

Description: If the NFS level does not carry the access authorization attribute information at the time of registration, it inherits the access authorization control information of the NF level; if both the NF level and the NFS level carry the access authorization attribute information, the NFS level access authorization control has higher priority.

NF to register

In the 5GC network, the NRF is responsible for the automated management of all NFs/NFSs, which includes NF de-registration, served by Nnrf_NFManagement. the NF side triggers de-registration by configuration, and after de-registration, the NRF removes the NF registration attribute from the NRF. NF goes through the registration process

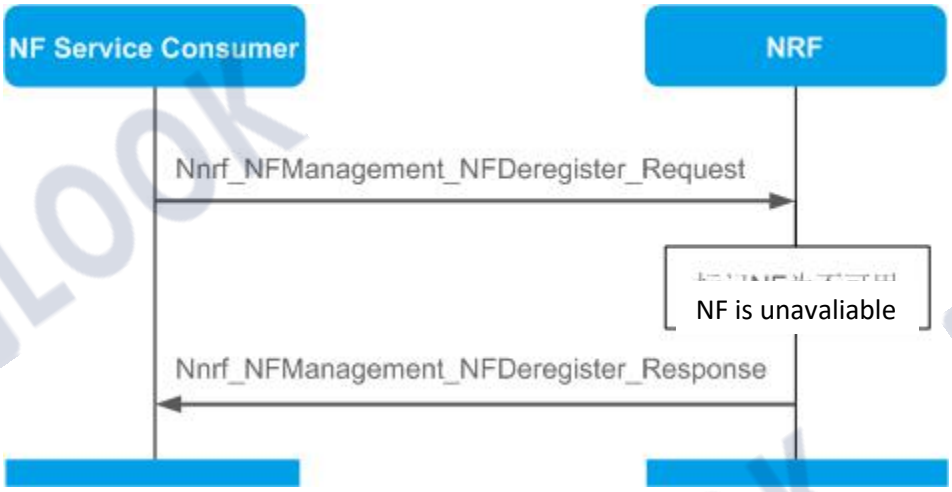


Figure 9 *NF de-registration process*

1. The NF sends a Nnrf_NFManagement_NFDeregister_Request message to the NRF requesting to register, carrying only the nfInstanceID that has been generated for that NF, and does not need to carry the NF/NFS Profile.
2. The NRF receives a de-registration request and looks up the record corresponding to this nfInstanceID and deletes this NF and all NFS Profiles associated with it.
3. The NRF returns the Nnrf_NFManagement_NFDeregister_Response response to this NF.

NF Update

In the 5GC network, the NRF is responsible for the automated management of all NF/NFS, which includes NF/NFS updates, served by Nnrf_NFManagement.

- When the used NF/NFS information changes (e.g., information changes such as services or capabilities), it needs to be updated to the NRF.The NRF update contains both full and partial updates.
- NF Full Volume Update Process

  The NF full update process is the same as the NF registration process, the difference between the NF full update process and the NF registration is that the NRF first identifies that the nfInstanceID is already in the NRF and considers it to be an NF full update, replacing all the original attributes of the nfInstanceID with information about all the attributes of the NF.

Figure 10 NF section update process

1. The registered NF/NFS sends the Nnrf_ NFManagement_ NFUpdate_ Request message to the NRF requesting update information, the request message carries only the NF/NFS Profile to be updated and the update operation (add/remove/replace) for these attribute information.
2. The NRF handles NF/NFS update requests.

3. The NRF sends the Nnrf_NFManagement_NFUpdate_Response message to the NF.

An NF that has registered with the NRF periodically sends a message to the NRF through the NF update process to inform the NRF of the valid status of the NF (later called a heartbeat). The heartbeat period can be set by command and returned to the NF by the NRF when the NF registration is successful.When the NRF detects that the NF has not sent a heartbeat message for a number of heartbeat periods (configurable), the NRF sets the NF state to SUSPENDED and this NF and the corresponding NFS are no longer discovered by other NFs.

- NF Heartbeat Process

The NRF updates the heartbeat cycle of the registered NF by carrying the new heartbeat cycle (configured by command) in the heartbeat response message of the NF in the same process as the NF part update process.

1. The registered NF sends the Nnrf_NFManagement_NFUpdate_Request message to the NRF, and the request message contains the NF status and the corresponding replacement operation.
2. The NRF handles NF update requests (heartbeat messages).
3. The NRF sends the Nnrf_NFManagement_NFUpdate_Response message to the NF.

NF Status Subscription

In the 5GC network, the NRF is responsible for the automated management of all NF/NFS, which includes NF/NFS state subscriptions, served by Nnrf_NFManagement.

When an NF wants to be notified of the status of some specific NF/NFS instance, it can request a subscription to its status from the NRF. The information carried by the subscription is shown in Table 2. After a successful subscription, the NRF assigns a "subscriptionId" that uniquely identifies the subscription to distinguish other subscription information. When the NF does not want to subscribe, it can also subscribe to the relevant information.

Table 2 Information about the attributes carried by NF subscriptions

NF subscription carry information	role	Included values	instructions
Subscribe to events	Represents a status event for the subscribed target	• NF Registration • NF to register • NF Profile Changes	• One or more may be carried. • If it does not carry a

Table 2 Information about the attributes carried by NF subscriptions

NF subscription carry information	role	Included values	instructions
	NF.		subscription event, it means that all three events are subscribed to.
Subscription conditions	Represents the filtering criteria for the subscribed target NF.	• nfInstanceId • nfType • serviceName • amfSetID of the AMF, amfRegionId of the AMF, such subscription conditions carry at least one. • guamiList • Network Slice conditions: snssaiList (required), nsiList (optional). • NFGroup condition: nfType, nfGroupId, 2 must carry.	• Only one subscription condition can be carried in each subscription request message; if you need to subscribe to multiple subscription conditions, you need to initiate multiple subscription requests. • If no subscription condition is carried represents a subscription to the corresponding subscription event for all NFs.
Subscribe to status notification conditions	Send notification conditions for target NF Profile changes on behalf of the NRF to the NF requesting the subscription.	• monitoredAttributes: the NRF only sends notifications for changes to the attributes contained in this list. • unmonitoredAttributes: the NRF sends notifications for changes to attributes other than	• Only one of the fetch values is carried when subscribing. • This message is only for NF attribute change events. the NRF automatically sends a subscription status notification when the NF

Table 2 Information about the attributes carried by NF subscriptions

NF subscription carry information	role	Included values	instructions
		those contained in this list.	subscribes to another NF registration and NF de-registration. the subscribed NF registration and NF de-registration.

- NF Status Subscription Process

An NF may conditionally subscribe to the NRF for a particular type of change to a particular NF/NFS.

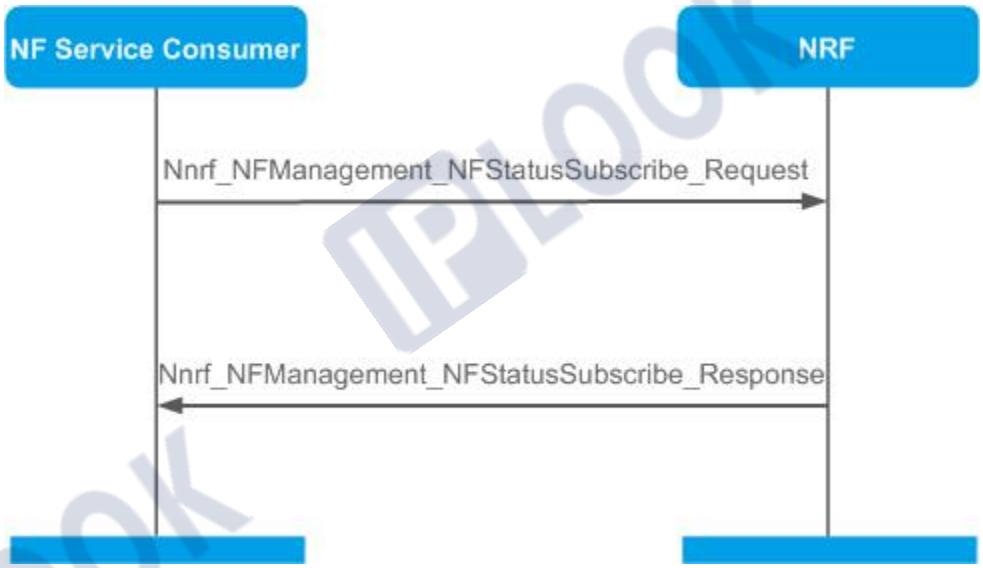


Figure 11 NF Status Subscription Process

1. The NF sends the Nnrf_NFManagement_NFStatusSubscribe_Request message to the NRF requesting to subscribe to the status information of other NF/NFS instances, carrying information such as subscription conditions, subscription events, subscription duration, and subscription notification conditions in the request message.
2. The NRF sends the Nnrf_NFManagement_NFStatusSubscribe_Response response to the NF, carrying the subscriptionID that uniquely identifies this subscription created by the NRF for this subscription.

- NF Status Subscription Update Process

NF status subscription updates are performed only for the length of time that the subscription is valid. the NF subscription is about to expire. you can update the subscription to refresh the length of time that the subscription is valid.

1. The NF sends a status subscription update request message to the NRF carrying the subscriptionId, validityTime the new subscription validity and the replacement operation, and does not update other attributes.
2. The NRF handles subscription validity refresh.
3. The NRF sends a response to the NF.

Description.

The NF may repeat the subscription to the NRF. If the repeat subscription is the same except for the "validityTime" field, the NRF updates the "validityTime" field and returns to the NF The NRF updates the "validityTime" field and returns to the NF only the old subscription information that updates the validity time of the subscription, otherwise the NRF will use the new subscription information.

- NF Status De-Subscription Process

When the NF no longer needs to get state changes for some specific NF/NFS instance, it can request to the NRF to go subscribe to its state.

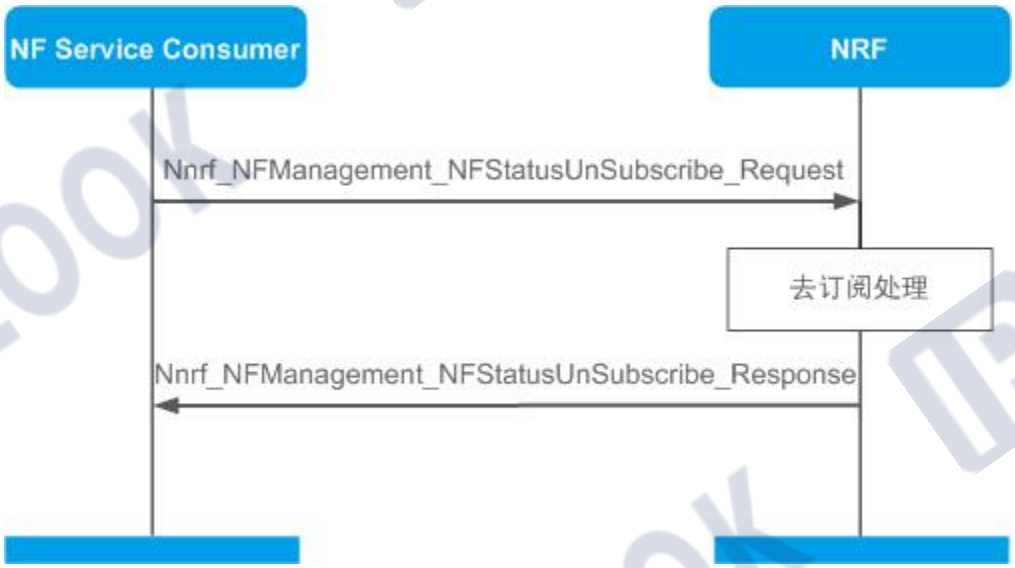


Figure 12 NF Status De-Subscription Process

1. The NF sends the Nnrf_NFManagement_NFStatusUnSubscribe_Request message to the NRF carrying the subscriptionID request to subscribe to the status information of a specific NF/NFS instance.
2. The NRF handles the de-subscription requests from the NF.
3. The NRF sends a Nnrf_NFManagement_NFStatusUnSubscribe_Response response to the NF.

Description.

The NRF removes these expired subscription messages when the subscription reaches the NF subscription validity length.

NF Status Notification

In the 5GC network, the NRF is responsible for the automated management of all NFs/NFSs, which includes NF/NFS state subscription notifications, served by Nnrf_NFManagement.When an NF subscribes to the NRF with information about the state change of an NF/NFS instance, after the successful registration, de-registration, or update process of the relevant NFs in the scope of the subscription or by the command to modify the NF The notification process is triggered after the Profile state, and the NRF actively notifies the subscribed NFs.

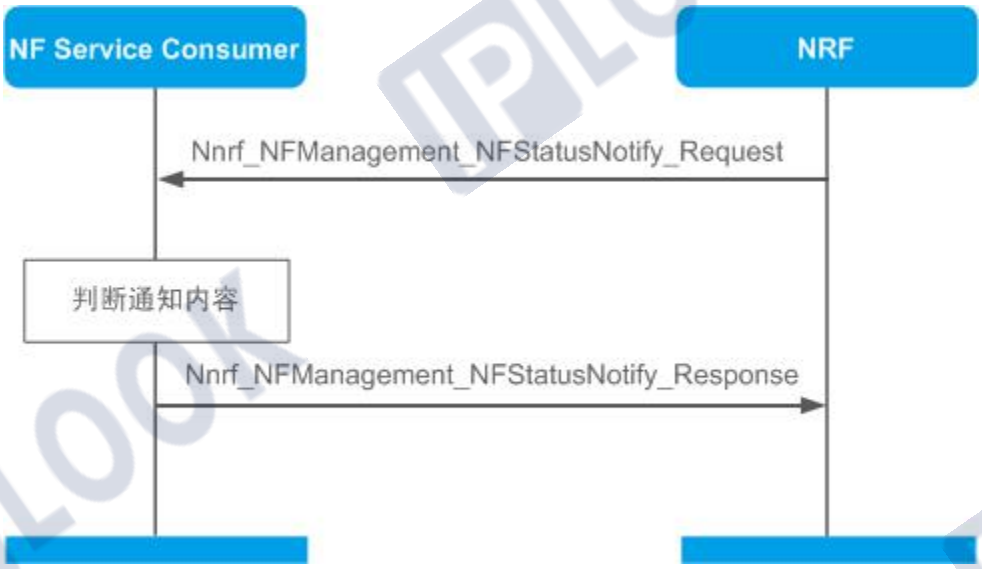


Figure 13 NF Status Notification Process

1. The NRF sends the Nnrf_NFManagement_NFStatusNotify_Request message carrying the notification type and all properties of the NF to notify the NF when the NF/NFS instance that was

successfully subscribed to undergoes NF registration, NF de-registration or NF Profile change in the corresponding subscription request.

2. NF determines if the content of the received notification is a subscribed notification message.
3. NF response Nnrf_NFManagement_NFStatusNotify_Response to NRF.

3.6.1 .1 .7 Follow the standards

standard category	Standard number	Standard name
3GPP	29.510	Technical Specification Group Core Network and Terminals;5G System;Network Function Repository Services;
	23.501	Technical Specification Group Services and System Aspects; System Architecture for the 5G System;
	23.502	Technical Specification Group Services and System Aspects; Procedures for the 5G System;
	29.571	Technical Specification Group Core Network and Terminals; 5G System; Common Data Types for Service Based Interfaces;

3.6.1.2 NF certification

3.6.1.2.1 Definition

Security considerations, NFs need to obtain authorization when requesting a certain service to prevent and reduce the risk of privilege elevation. 5GC network's servitization interface between NFs uses Oauth2.0 dynamic Token authorization (Token can be understood as a short-term token used by NFs to request access to a service, and the required service can be obtained when and only when the token is in hand), and the authorization method is Client Credentials. after the NF first requests a service for service

discovery, it requests an Access Token from the NRF, and then carries this Access Token for subsequent corresponding service requests. the NF service provider first authenticates the NF service consumer to ensure the integrity and legitimacy of the Access Token before providing the service. When the Access Token expires or the requested service changes, the NF requestor applies for a new Access Token.

3.6.1.2.2 Customer Value

Beneficiaries	Description of benefits
Operator	Prevent and mitigate NF privilege elevation risks and ensure business is conducted properly.
Subscriber	The user does not perceive the feature.

3.6.1.2.3 Application Scenarios

- When an NF first requests a certain service (e.g., PDU session establishment, AMF requesting a SMF's service to establish a session), it needs to first obtain Token authorization, and after the NRF provides the Access Token to the NF, the NF performs subsequent NF authentication and corresponding service services.
- Access Token expires or the scope of the service requested by the NF changes or there is a new service provider NF but no available Access Token, the NF requestor will also request a new Token.
- When NF requests to provide a service, it needs to carry the Access Token authorized by NRF for NF authentication, which in turn supports the subsequent completion of the business service.

3.6.1.2.4 Accessibility

Involved NF

Involving NF	Supported Versions	Function description
NRF	No special requirements	Authorization is performed on the NF requesting the service and Access Token is generated and sent to the NF.

Involving NF	Supported Versions	Function description
Other NFs on the 5GC control surface	No special requirements	• Supports initiating a service request to the NRF, obtaining the corresponding Access Token information and maintaining it for update. • Support for initiating service requests to other NFs and authentication to other NFs.

3.6.1.2.5 Principle Overview

In the Token authorization mechanism, the NF service consumer is the client, the NF service provider is the resource server, and the NRF is the NF authorization server, which acts as a centralized control point for the authority management of the Token and provides Access Token to the NF service consumer, which is served by Nnrf_AccessToken.

Access Token Application Process

When an NF service consumer requests a service, it first requests an Access Token from the NRF.

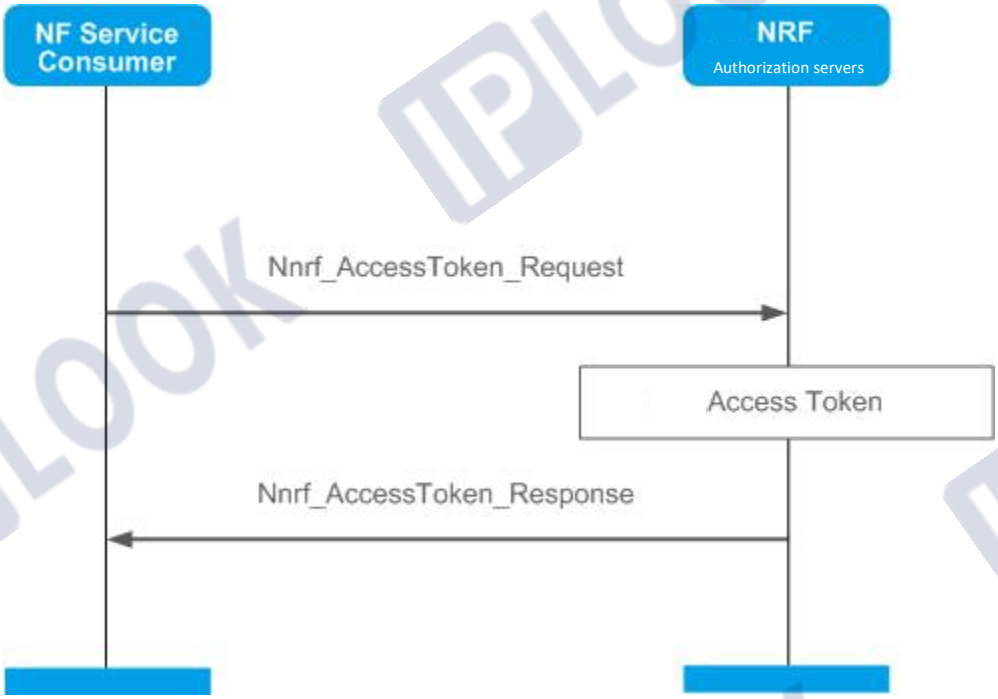


Figure 14 Access Token Application Process

1. The NF service consumer initiates a Nnrf_AccessToken_Request request to the NRF carrying the attributes grant_type, nfInstanceId and scope.
2. The NRF generates the Access Token based on the nfInstanceId of the NF service consumer and the NF service provider's NF/NFS access authorization control, etc. The Access Token contains the AccessTokenClaims (the InstanceID of the NF service consumer, the NF service provider and the NRF, the accessible NFS name, etc.), the Access Token expiration time and the NFS name to which the NF service consumer has access, etc.
3. The NRF returns the generated Access Token to the NF service consumer via the Nnrf_AccessToken_Response message.

NF Certification Process

TSL authentication at the transport layer needs to be completed first before NF authentication.

After the NF service consumer obtains the Access Token, it carries the Access Token to access the NF service provider's service. the NF service provider authenticates the NF service consumer and verifies whether the NF service consumer has permission to access its service based on the Access Token.

NF Certification Process

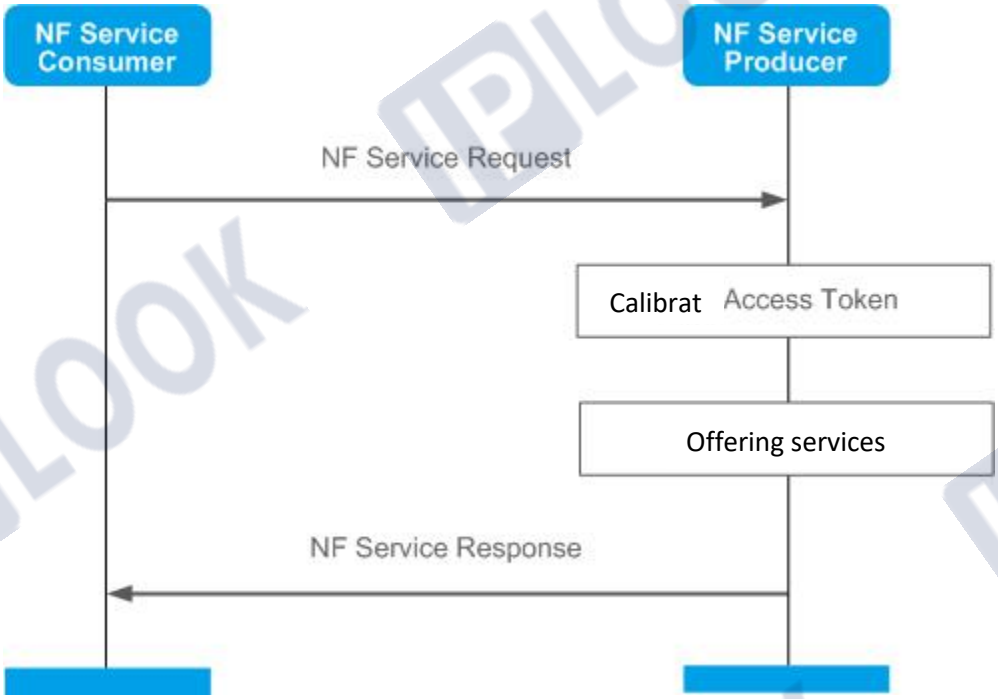


Figure 15 NF Certification Process

1. The NF service consumer initiates a service request to the NF service provider, carrying the Access Token.
2. The NF service provider authenticates the NF service consumer and uses the public key to check whether the signature in the Access Token is correct, so as to determine whether the Access Token is legitimate and valid. If the check passes, the NF service provider then checks the claims in the Access Token to determine whether the requesting NF is entitled to access its service.
3. The NF Service Provider returns an NF Service Response response to the NF Service Consumer.

3.6.1.2.6 Follow the standards

standard category	Standard number	Standard name
3GPP	29.510	Technical Specification Group Core Network and Terminals;5G System;Technical Specification Group Core Network and Terminals;5G System;Network Function Repository Services;Stage 3;

standard category	Standard number	Standard name
	33.501	Technical Specification Group Services and System Aspects;Security architecture and procedures for 5G system
IETF	RFC 6749	The OAuth 2.0 Authorization Framework

3.6.1.3 NF discovery

3.6.1.3 .1 Definition

NRF supports NF/NFS service discovery function, when NF needs some specific services, request to NRF to discover available services, NRF filter based on registered NF/NFS, and send available NF/NFS to NF.NRF supports specific NF selection based on different selection conditions, which helps NF selection under different networking methods.

3.6.1.3 .2 Customer Value

beneficiaries	Description of benefits
Operator	Based on specific selection conditions, NFs under different groupings can be selected, which helps support operators' flexible service requirements and ultimately enables intelligent selection.
Subscriber	The user does not perceive the feature.

3.6.1.3 .3 Application Scenarios

There are different application scenarios for different conditions of NF selection, see "Application Scenarios" in each feature.

3.6.1.3 .4 Accessibility

Involved NF

See "Involving NF" in each feature.

3.6.1.3 .5 Principle Overview

NF service discovery is served by Nnrf_NFDiscovery, NF service discovery process, NRF needs to do target NF discovery processing, discovery based on Table 1 and specific optional discovery attributes carried by the requesting NF and NF/NFS access authorization control of the target NF, NRF will send the available NF/NFS Profile to the requesting NF after processing. service An example of the discovery process is shown in Figure 1.

Table 1 Generic properties carried by NF service discovery

Property Name	description	Is it mandatory
target-nf-type	The target NF Profile filter condition is in an "with" relationship with other conditions.	mandatory
requester-nf-type	NF Type of the requesting NF, which can be used for access authorization determination at NF Type granularity.	mandatory
service-names	The name of the requested service.	Optional, a public attribute that is generally carried by service discovery requests.
requester-nf-instance-fqdn	The name of the requesting NF.	Optional, a public attribute that is generally carried by service discovery requests.

NF service discovery carries specific discovery attributes, see the implementation rationale for each feature, and an example of the process of AMF discovery of SMFs, using PDU session establishment as an example, is shown in Figure 1.

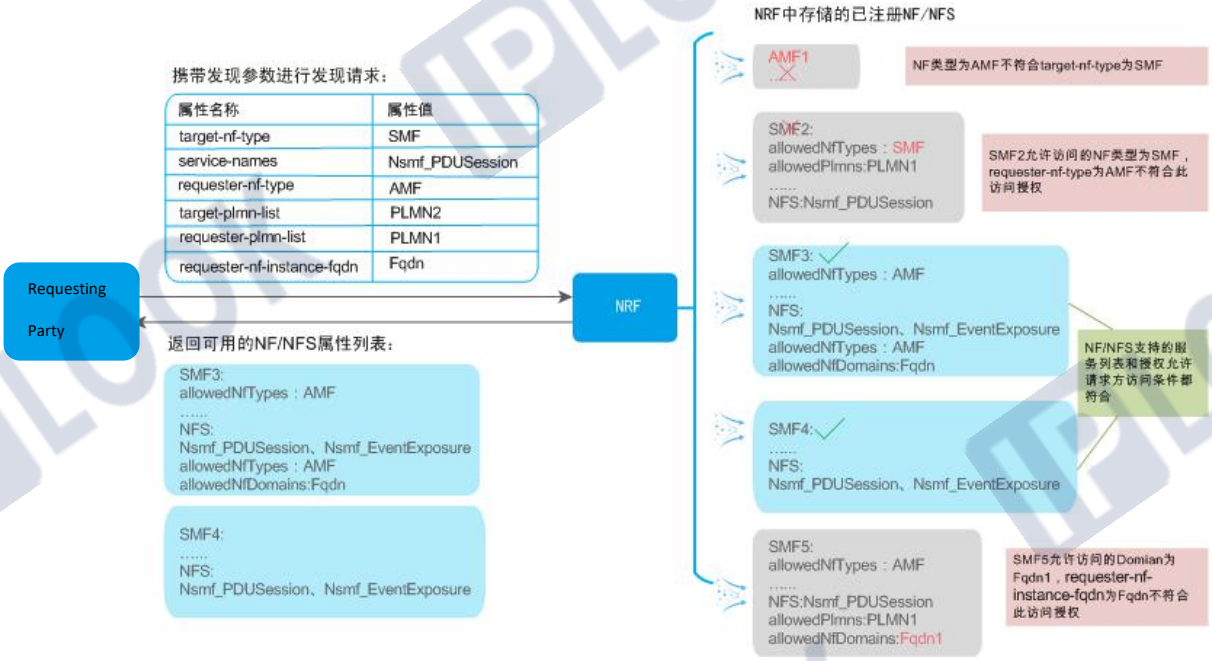


Figure 1 Service discovery process

Service Discovery Process

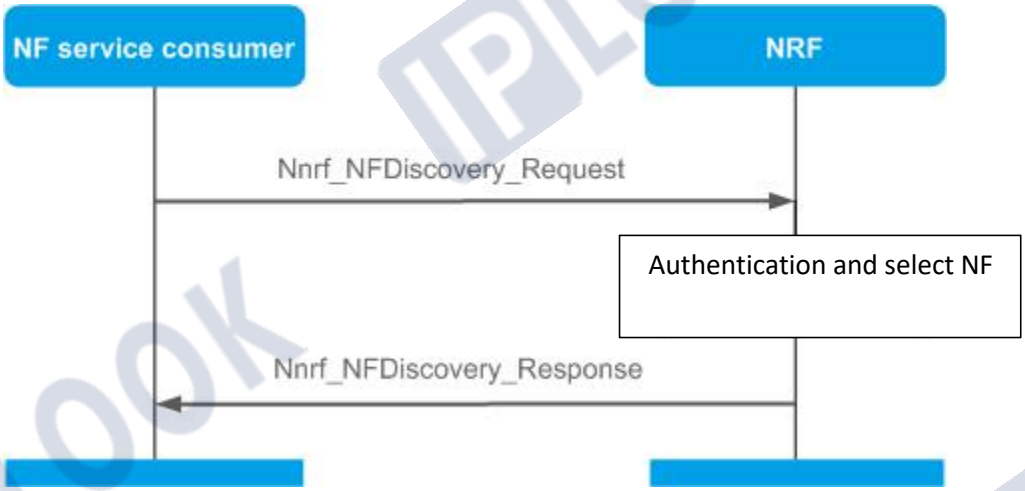


Figure 2 Service Discovery Process

1. The NF sends the Nnrf_NFDiscovery_Request message to the NRF, which carries information such as Table 1 and **condition-specific attributes** (described separately in each characteristic).
2. The NRF matches to the corresponding service provider NF list based on the attributes carried by the request message, and the service provider NF then performs NF/NFS access authorization

control on the requesting NF to determine whether the requesting NF is allowed to access the desired NFS.

Description.

When multiple condition-specific attributes are carried in the scenario, the final accessible NF list returned by the NRF is the intersection of the NF lists corresponding to each condition-specific attribute.

3. The NRF returns the Nnrf_NFDiscovery_Response message to the requesting NF.

3.6.1.3 .6 Follow the standards

standard category	Standard number	Standard name
3GPP	29.510	Technical Specification Group Core Network and Terminals;5G System;Network Function Repository Services;
3GPP	23.502	Technical Specification Group Services and System Aspects; Procedures for the 5G System;

3.6.2 Optional functionalities

3.6.2.1 Support for L-NRF registration

3.6.2.1 .1 Definition

For small operator networks, all NF/NFS are managed by a unified NRF without the need for layering. For large carrier networks, to facilitate flexible and automated network management, NRFs need to be deployed in layers, with the highest layer NRF implementing all NF/NFS management within the carrier

network. in NRF layered networking, lower layer NRFs support registration with higher layer NRFs when they first provide network services.

3.6.2.1 .2 Customer Value

Beneficiaries	Description of benefits
Operator	The relationship of each NF network in the NRF hierarchical network is clear, and it is easier for each layer to achieve flexible automatic up and down of NFs. It helps operators to realize the flat management of NF/NFS across DCs and better support 5G network self-governance.
Subscriber	The user does not perceive the feature.

3.6.2.1 .3 Application Scenarios

In NRF hierarchical networking, when a lower layer NRF first comes online to provide network services, it needs to register with the higher layer NRF first.

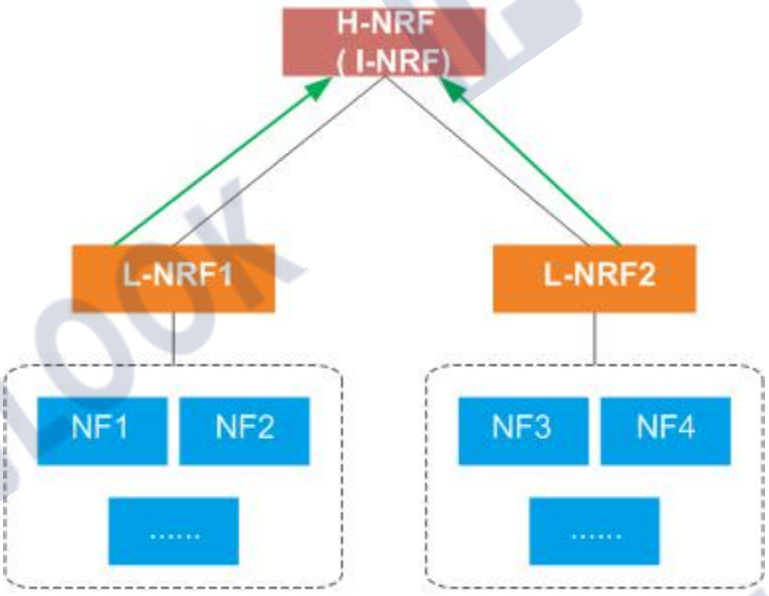


Figure 1 Example of NRF registration

3.6.2.1 .4 Application restrictions

An NRF may only register with the higher level NRF to which it belongs. The principle is the same as the "NF registration" application restriction.

3.6.2.1 .5 Principle Overview

Concept Introduction

L-NRF: The lowest layer NRF in the hierarchical network, which interacts directly with the NF.

H-NRF: The highest layer NRF in a two-tier network, the middle layer NRF in a three-tier network, and manages all L-NRF Profiles contained. the H-NRF in a three-tier network registers with the I-NRF.

I-NRF: PLMN NRF, representing the highest layer NRF of the operator, H-NRF and I-NRF in a two-tier network, and I-NRF, H-NRF and L-NRF in a single-tier network.

hierarchical networking

For medium and large operator networks, which may involve cross-province/region roaming or international roaming of users, in order to facilitate flexible and automated network management, NRFs need to be deployed in layers, with the highest layer NRFs implementing all NF/NFS management within the operator network.

NRF registration occurs in hierarchical networking, which includes NRF two-layer networking and NRF three-layer networking, and typical networking scenarios are shown in Figure 2 and Figure 3.

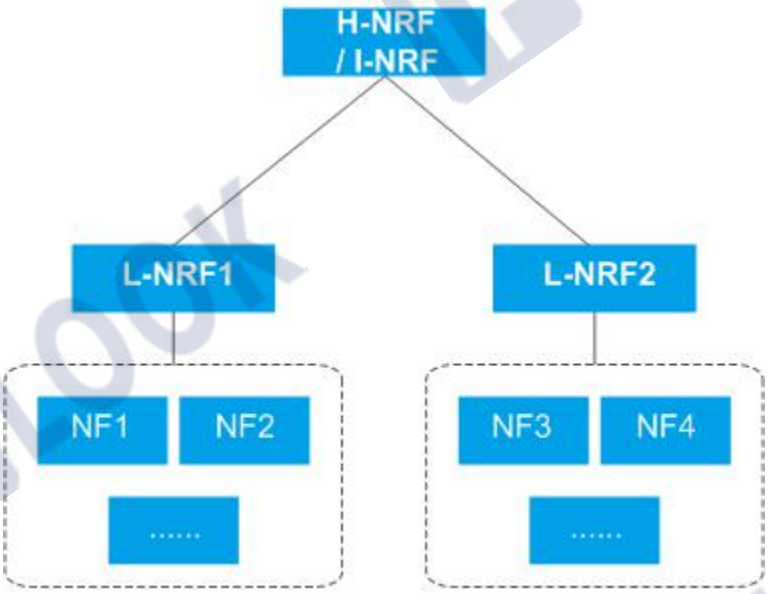


Figure 2 *Schematic diagram of the two-tier network*

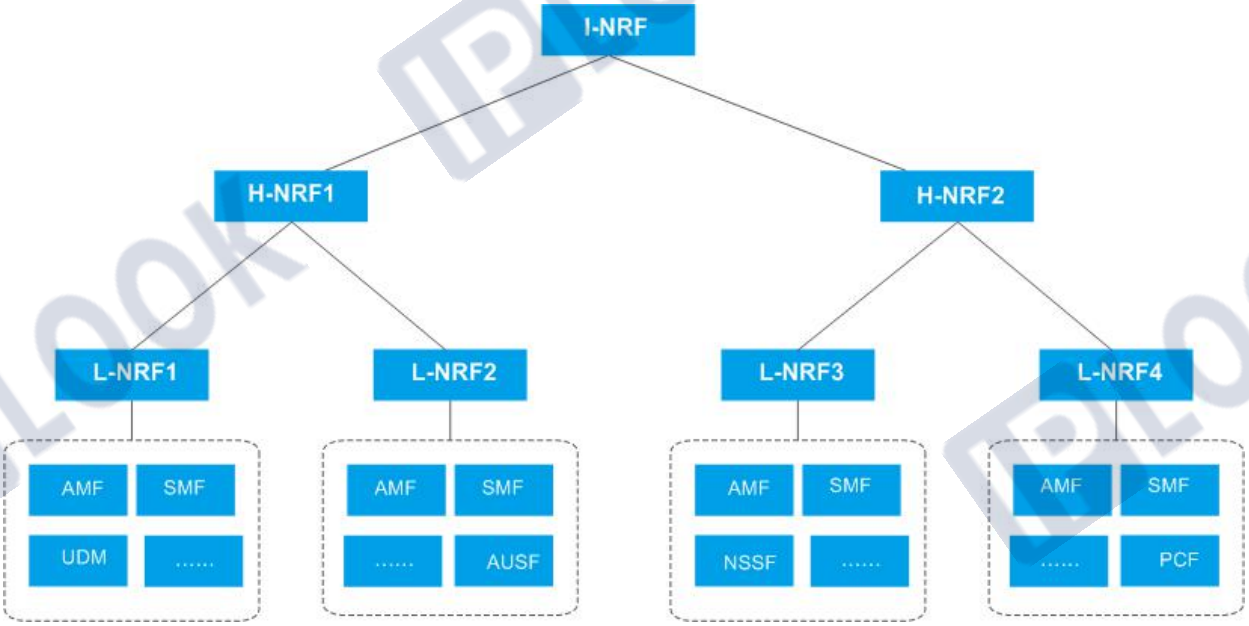


Figure 3 *Three-layer network schematic*

NRF Registration

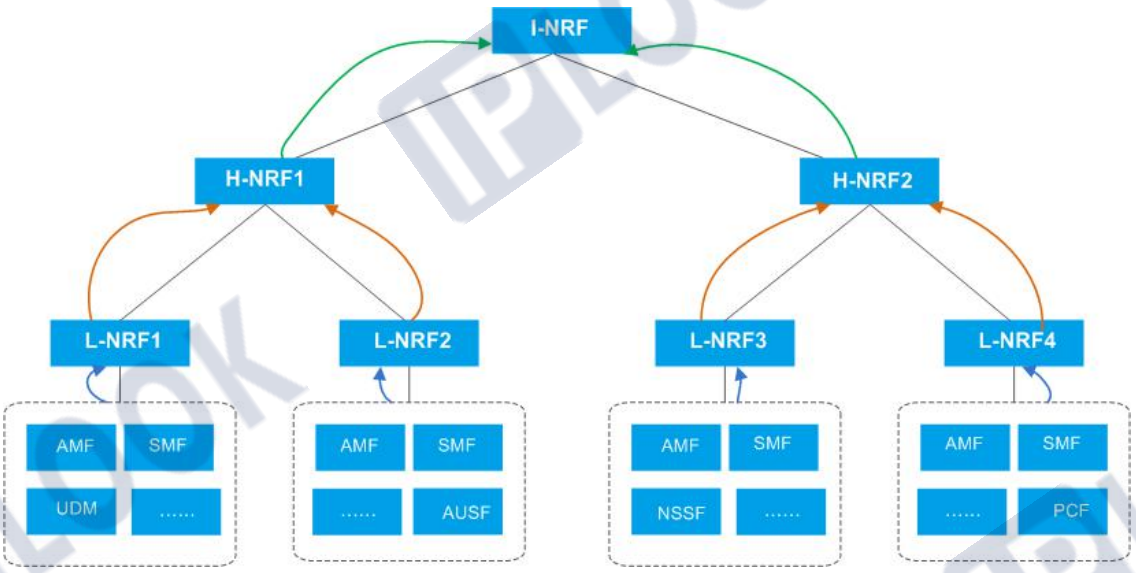


Figure 4 *Registration schematic*

In a two-layer network, when an L-NRF first provides service, it needs to carry its own L-NRF Profile to register with the attributed H-NRF, and after successful registration, the H-NRF contains all the managed L-NRF Profiles, which are used to address and determine the L-NRF. in addition, the routing relationship between the L-NRF and the NF is configured in the H-NRF, which is used to address and determine the

L-NRF to which the NF belongs The L-NRF Profile contains all the managed L-NRFs and is used to address the L-NRFs.

In a three-tier network, when an H-NRF first provides service, it needs to carry its own H-NRF Profile to register with the attributed I-NRF, and after successful registration, the I-NRF contains all the H-NRF Profiles managed, which is used for addressing to determine the H-NRF. in addition, the I-NRF configures the routing relationship between the H-NRF and the NF, which is used for addressing to determine the NF attributed to the H-NRF. other registrations and configurations are the same as for a two-tier network.

Description.

Each NF registers only to its own domain NRF, and whether the NRF is hierarchical or not has no effect on NF registration.

NRF Registration Process

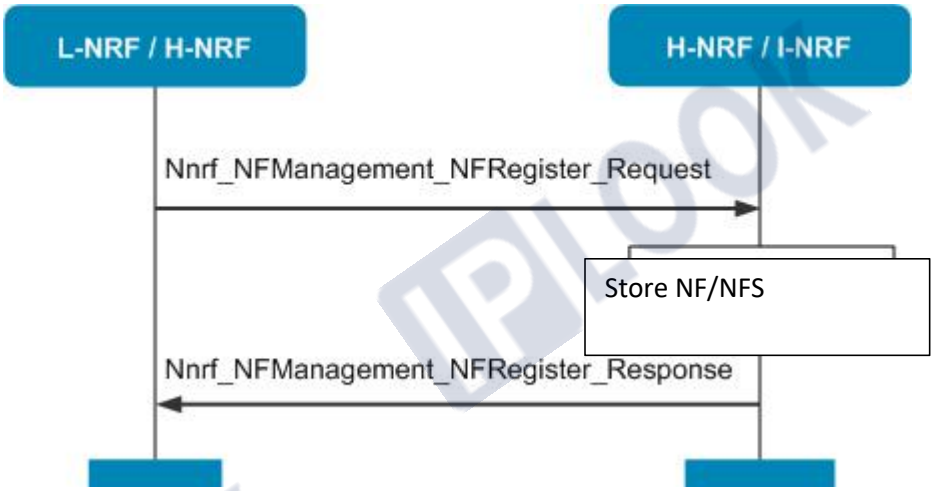


Figure 5 *NRF registration process*

1. The L-NRF sends an Nnrf_NFManagement_NFRegister_Request message to the H-NRF (H-NRF to I-NRF) requesting registration, carrying that NRF's own NF/NFS Profile.
   - Registering an NRF should be done with "nfType" as "NRF" in the NF Profile.
   - Registering an NRF should include "nnrf-disc" and "nnrf-nfm" in the "nfservice" field of the NF Profile.

   Description: Register NRF information in another NRF that is used to forward or redirect service discovery requests to locate to the registered NRF.

2. The H-NRF processes the registration request from the L-NRF (the I-NRF processes the registration request from the H-NRF) and performs the corresponding checks, and saves the NF/NFS Profile record after passing.
3. The H-NRF returns the Nnrf_NFManagement_NFRegister_Response message to the L-NRF (I-NRF to H-NRF).

3.6.2.1 .6 Follow the standards

standard category	Standard number	Standard name
3GPP	29.510	Technical Specification Group Core Network and Terminals;5G System;Network Function Repository Services;
	23.501	Technical Specification Group Services and System Aspects; System Architecture for the 5G System;
	23.502	Technical Specification Group Services and System Aspects; Procedures for the 5G System;
	29.571	Technical Specification Group Core Network and Terminals; 5G System; Common Data Types for Service Based Interfaces;

3.6.2.2 Support for L-NRF de-registration

3.6.2.2.1 Definition

In NRF hierarchical networking, the lower level NRF supports de-registration to the higher level NRF when the service is no longer provided by the lower level NRF.

3.6.2.2.2 Customer Value

Beneficiaries	Description of benefits
Operator	The relationship of each NF network in the NRF hierarchical network is clear, and it is easier for each layer to achieve flexible automatic up and down of NFs. It helps operators to realize the flat management of NF/NFS across DCs and better support 5G network self-governance.
Subscriber	The user does not perceive the feature.

3.6.2.2.3 Application Scenarios

In NRF hierarchical networking, when a lower layer NRF is gracefully powered down, it needs to go to the upper layer NRF to which it belongs to register.

3.6.2.2.4 Principle Overview

In NRF hierarchical networking, de-registration is triggered by configuration when the NRF is no longer providing services, and after de-registration, the upper layer NRF will remove this NRF registration attribute; the NRF or NF under its jurisdiction is inverted to the alternate NRF for services, otherwise the NRF or NF under its jurisdiction will also be forced to de-register.

NRF de-registration process

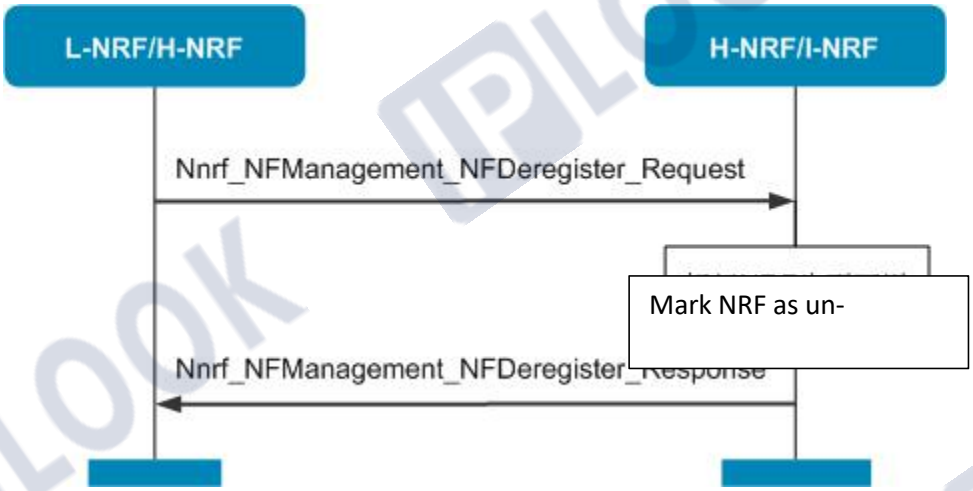


Figure 1 *NRF de-registration process*

1. The L-NRF sends a Nnrf_NFManagement_NFDeregister_Request message to the H-NRF (H-NRF to I-NRF) requesting to register, carrying only the nfInstanceID of that NRF, not the NF/NFS Profile.
2. H-NRF, I-NRF receives a de-registration request and looks up the record corresponding to this nfInstanceID and deletes this NRF and all the NFS Profiles associated with it.
3. H-NRF to L-NRF (I-NRF to H-NRF) Nnrf_NFManagement_NFDeregister_Response response.

3.6.2.2.5 Follow the standards

standard category	Standard number	Standard name
3GPP	29.510	Technical Specification Group Core Network and Terminals;5G System;Network Function Repository Services;
	23.501	Technical Specification Group Services and System Aspects; System Architecture for the 5G System;
	23.502	Technical Specification Group Services and System Aspects; Procedures for the 5G System;

standard category	Standard number	Standard name
	29.571	Technical Specification Group Core Network and Terminals; 5G System; Common Data Types for Service Based Interfaces;

3.6.2.3 Support for L-NRF updates

3.6.2.3.1 Definition

In NRF hierarchical networking, when a registered low-level NRF changes (e.g., information such as services or supported attributes changes), it needs to initiate an update to its registered high-level NRF.

3.6.2.3.2 Customer Value

Beneficiaries	Description of benefits
Operator	The relationship of each NF network in the NRF hierarchical network is clear, and it is easier for each layer to achieve flexible automatic up and down of NFs. It helps operators to realize the flat management of NF/NFS across DCs and better support 5G network self-governance.
Subscriber	The user does not perceive the feature.

3.6.2.3.3 Application Scenarios

In NRF hierarchical networking, if a registered low-level NRF Profile changes, such as if the NRF updates its capabilities by way of a software upgrade, etc., the low-level NRF initiates an update to its registered high-level NRF at that time.

3.6.2.3.4 Principle Overview

NRF Update Process

When the registered low-level NRF information changes, it needs to be updated to the upper-level NRF. NRF updates include two types of updates, full and partial, and both update types are served by Nnrf_NFManagement.

Description.

When the NF/NFS Profile governed by the underlying NRF changes, only NF updates are involved and no NRF update process is triggered.

In an NRF three-layer network, when the L-NRF Profile changes, only the NRF update process is initiated to its registered H-NRF, and the H-NRF's NRF update process is not triggered.

- NRF Full Volume Update

  The full update process of the NRF is the same as the NRF registration process, when the nfInstanceID carried in the request message of the low-level NRF within the registration process is already registered in the high-level NRF, then this registration process is the full update process of the low-level NRF, and the high-level NRF uses all the attribute information within this request message to replace the original attribute information of this nfInstanceID.

- NRF partial update

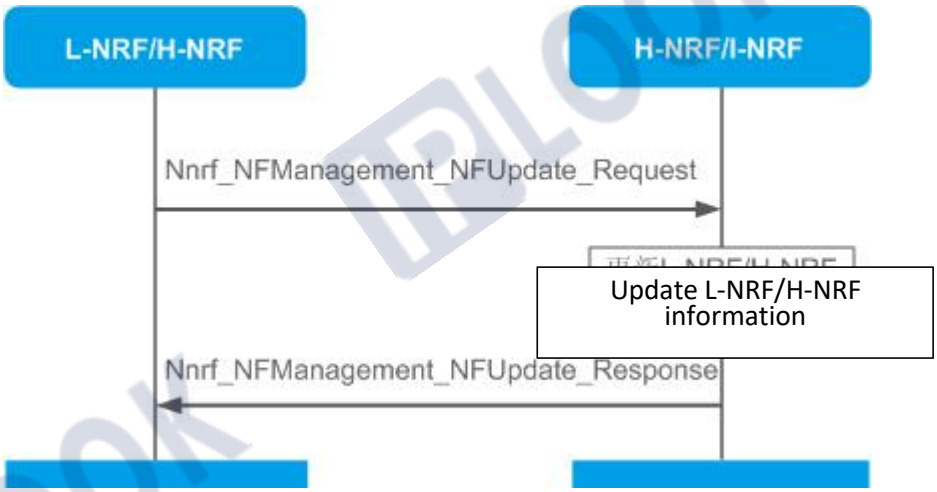


Figure 1 *NRF update flow*

1. The registered L-NRF/H-NRF sends a Nnrf_NFManagement_NFUpdate_Request message to the H-NRF/I-NRF requesting update information, carrying in the request message only the L-NRF/H-NRF Profile to be updated and the update operation (add/remove/replace) for these attribute information.
2. High-level NRFs process low-level NRF update requests.
3. the high level NRF sends the Nnrf_NFManagement_NFUpdate_Response message to the low level NRF.

NRF Heartbeat Update Process

A low-level NRF that has registered with the high-level NRF sends messages to the high-level NRF at regular intervals to inform the valid status of the low-level NRF through an NRF update process, and such update process is referred to as the NRF heartbeat update process. The fixed time interval is called the heartbeat period, which can be set by command and returned by the high-level NRF to the low-level NRF upon successful registration of the low-level NRF.When the high-level NRF detects that the low-level NRF has not sent a heartbeat message for a number of (configurable) heartbeat periods, the high-level NRF sets the status of that low-level NRF to SUSPENDED and that low-level NRF will no longer be discovered by other NRFs.

The high level NRF carries the new heartbeat cycle in the heartbeat response message (by means of command configuration) to update the heartbeat cycle of the registered low level NRF in the same process as the NRF part update.

1. The registered low-level NRF sends the Nnrf_NFManagement_NFUpdate_Request message to the high-level NRF, and the request message contains the low-level NRF status and the corresponding replacement operation.
2. The high level NRF handles update requests (heartbeat messages) from the low level NRF.
3. The high level NRF sends the Nnrf_NFManagement_NFUpdate_Response message to the low level NRF.

3.6.2.3.5 Follow the standards

standard category	Standard number	Standard name
3GPP	29.510	Technical Specification Group Core Network and Terminals;5G System;Network Function Repository Services;
	23.501	Technical Specification Group Services and System Aspects; System Architecture for the 5G System;
	23.502	Technical Specification Group Services and System Aspects; Procedures for the 5G System;
	29.571	Technical Specification Group Core Network

standard category	Standard number	Standard name
		and Terminals; 5G System; Common Data Types for Service Based Interfaces;

3.6.2.4 Support for NF recursive queries

3.6.2.4.1 Definition

Service discovery, subscription/notification, and Token requests across NRFs in NRF hierarchical networks involve recursive queries through which the NRF to which the requesting NF belongs initiates requests to higher-level NRFs one by one until it finally gets the required NF/NFS list.

3.6.2.4.2 Customer Value

beneficiaries	Description of benefits
Operator	Meet service discovery, subscription/notification, and Token requests in various layered networking scenarios for operators to better support 5G services.
Subscriber	The user does not perceive the feature.

3.6.2.4.2 Application Scenarios

Recursive queries can be used for service discovery, subscription/notification, and Token request scenarios between NFs that are not registered in the same NRF in NRF hierarchical networks. Recursive query spans a small span and does not require the higher-level NRF to have the capability to handle redirection, which is recommended when the NRF in the operator's network does not have the capability to handle redirection or when a smaller impact on the performance of the higher-level NRF is desired.

3.6.2.4.3 Principle Overview

NF service discovery, NF subscription/notification and NF Token request recursive queries across NRF are similar, and this feature introduces recursive queries as examples of NF service discovery process recursive queries across NRF, NF subscription/notification process recursive queries across NRF and NF Token request recursive queries across NRF, respectively.

Recursive queries for NF service discovery process across NRF

The UDM of AMF discovery across NRFs in a two-tier network is introduced as an example, where the NFs in different regions are registered to the L-NRFs in the corresponding regions. As shown in Figure 1.

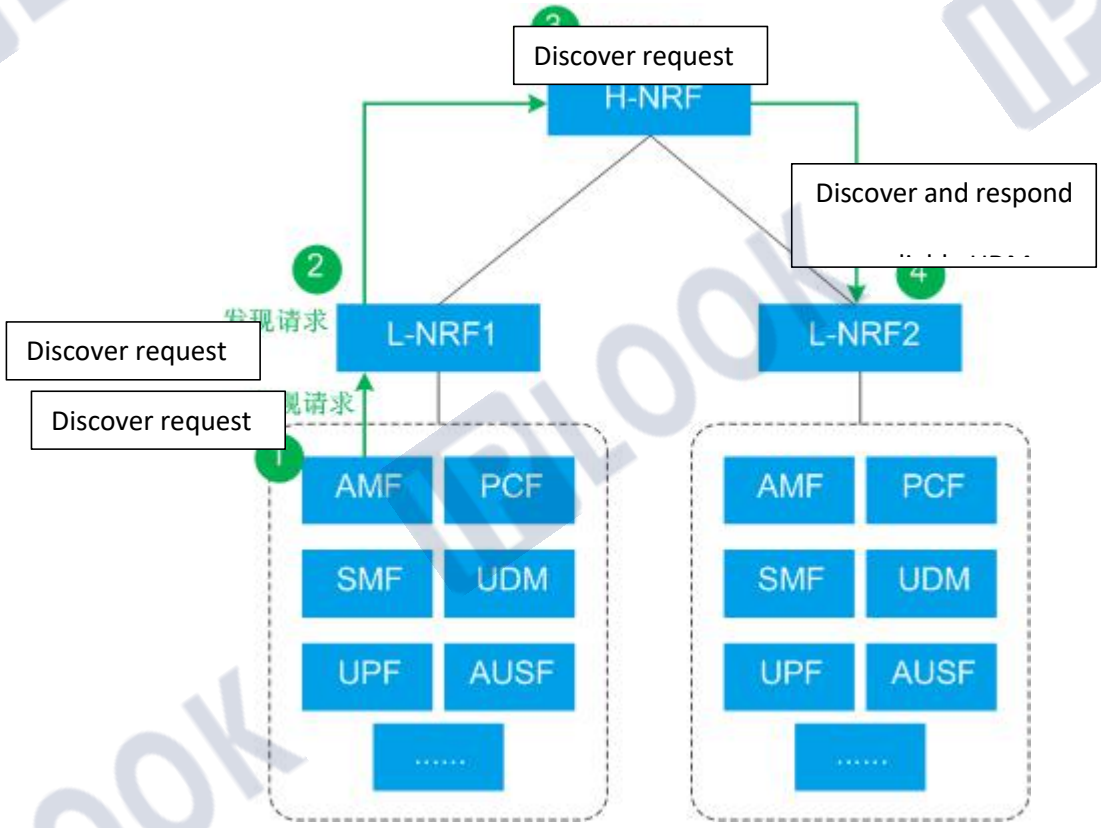


Figure 1 *Recursive query for AMF service discovery UDM across NRFs in a two-tier network within the same PLMN*

1. The AMF initiates a UDM discovery request to L-NRF1, carrying SUPI information.
2. L-NRF1 determines that this SUPI is not under the management of this L-NRF1 and initiates a request to the H-NRF.
3. The H-NRF performs L-NRF addressing based on the SUPI, determines that the number segment to which the number belongs is managed at L-NRF2, and forwards the discovery request to L-NRF2.

4. The L-NRF2 performs UDM discovery, returns a list of available UDMs to the H-NRF, and then returns them layer by layer to the requesting AMF.

Recursive queries for NF subscription/notification processes across NRF

Take the example of a two-tier network with NF1 subscribing to NF6, the NFs of different regions are registered to the L-NRFs of the corresponding regions. As shown in Figure 2.

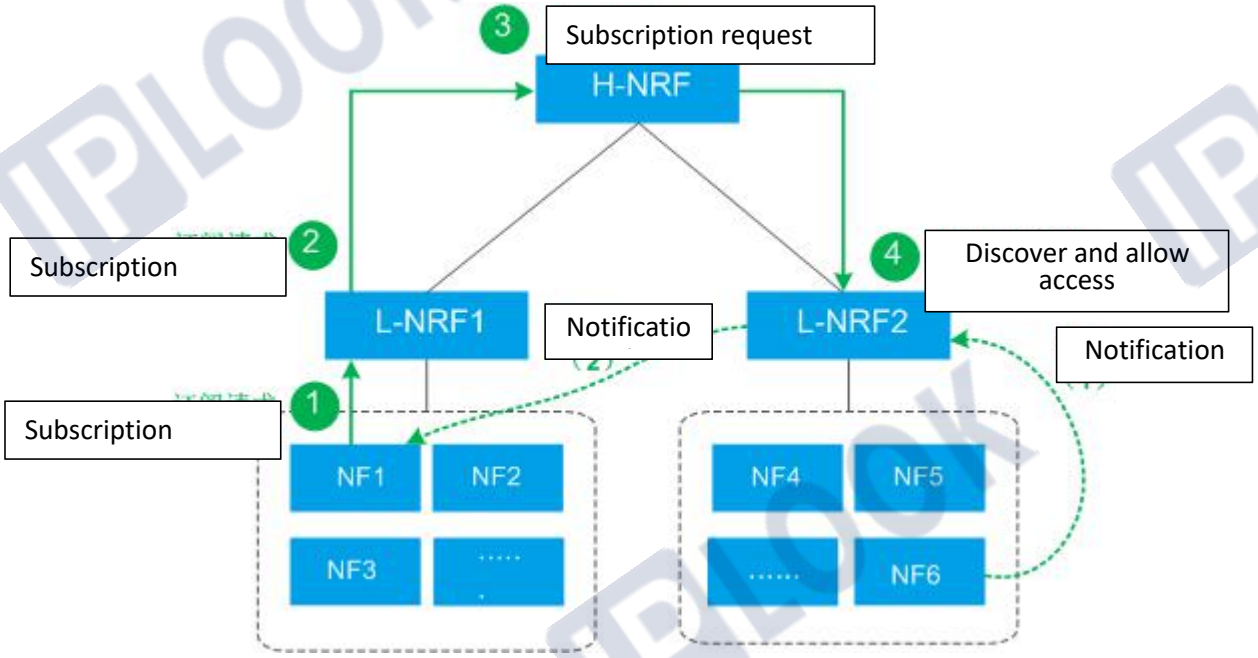


Figure 2 *Recursive query for NF1 subscription to NF6 across NRFs in a two-tier network within the same PLMN*

Subscription process (①~④).

1. NF1 initiates a subscription request to L-NRF1.
2. L-NRF1 determines that the NF corresponding to the subscription condition is not managed by this L-NRF1 and initiates a subscription request to the H-NRF.
3. The H-NRF performs L-NRF addressing based on the subscription conditions, determines that the NF to be subscribed is managed at L-NRF2, and forwards the subscription request to L-NRF2.
4. L-NRF2 performs NF6 discovery and access authorization determination, and returns the subscription success message to the subscriber NF1 layer by layer upon success.

Notification process ((1) to (2)).

NF6 is sent directly to the requesting party, NF1, without going through the H-NRF.

Recursive queries for NF Token requests across NRF

Take the example of an AMF in L-NRF1 of a three-layer network initiating a service request to an SMF in L-NRF3. the Token request needs to be made across PLMN-NRFs and the **Access Token is assigned and managed by the NRF where the NF service provider is located**. The NFs of different regions are registered to the L-NRFs of the corresponding regions. As shown in Figure 3.

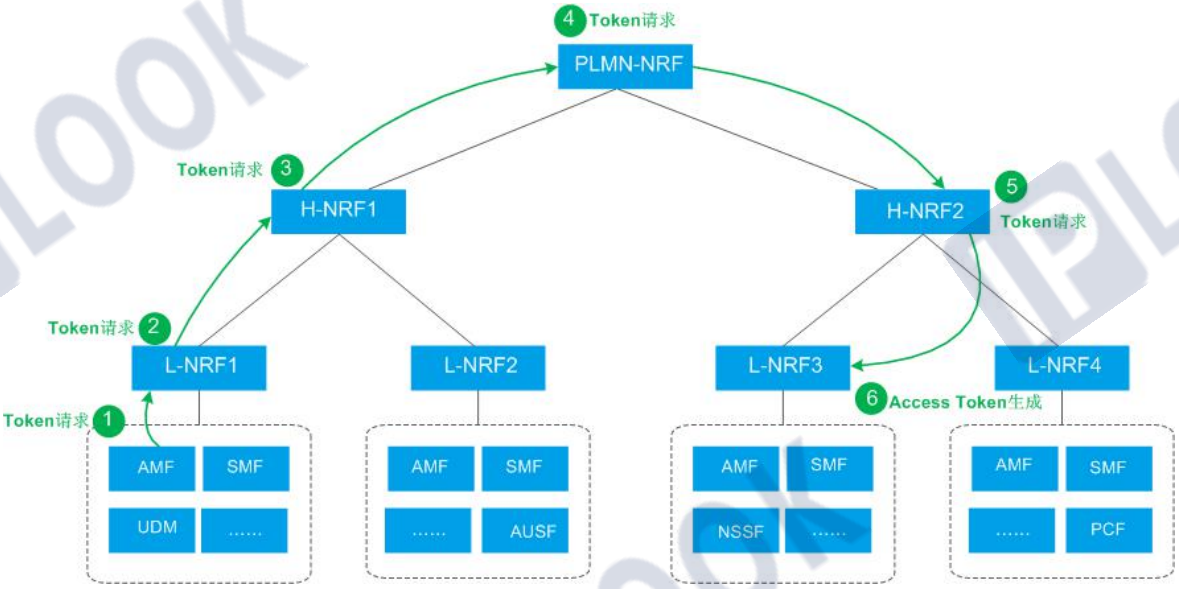


Fig. 3 *Recursive query of AMF requesting Token before service request from AMF to SMF across NRF in the same PLMN with three-layer network*

1. The AMF initiates a Token request to L-NRF1.
2. L-NRF1 determines that the attribute carried in the request message corresponds to an NF that is not managed by this L-NRF1 and initiates a Token request to the H-NRF.
3. The H-NRF determines that the attribute carried in the request message corresponds to an NF that is not managed by this H-NRF1 and proceeds to initiate a Token request to the PLMN-NRF.
4. The PLMN-NRF performs H-NRF addressing based on the Token request, determines that the NF to be discovered is managed at H-NRF2, and forwards the Token request towards H-NRF2.
5. H-NRF2 performs L-NRF addressing based on the Token request, determines that the NF to be discovered is managed at L-NRF3, and forwards the Token request to L-NRF3.
6. L-NRF3 performs Access Token generation based on the Token request. It is then returned to the requesting party AMF layer by layer.

3.6.2.4.4 Follow the standards

standard category	Standard number	Standard name

standard category	Standard number	Standard name
3GPP	29.510	Technical Specification Group Core Network and Terminals;5G System;Network Function Repository Services;

3.7 NSSF

3.7.1 Basic functionalities

3.7.1.1 Network Slice Selection

3.7.1.1.1 Definition

The 5GC network adopts a service-oriented architecture, abstracting the control plane functions into multiple independent Network Functions (hereinafter referred to as NFs), and each NF supports multiple services (hereinafter referred to as NFSs).
The NSSF is responsible for the selection of network slices, realizing flexible selection of network slices and selecting the set of network slice instances for the UE.

3.7.1.1.2 Customer Value

Beneficiaries	Description of benefits
Operators	Flexible options for network slicing to quickly deliver the services customers need
Subscriber	The subscriber does not perceive the feature.

3.7.1.1.3 Application Scenarios

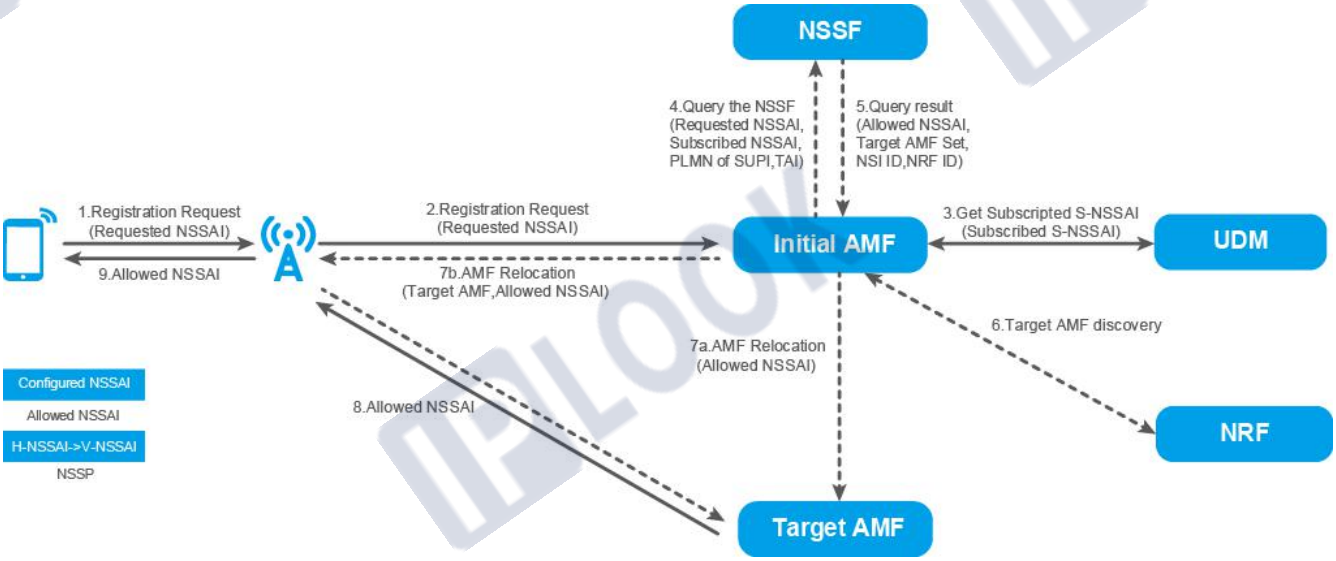
- Network Slicing Options for Serving PLMNs and HPLMNs.

- UE attachment process when AMF redistribution process, UE configuration update process, PDU session establishment SMF selection process.

- Example of user attachment process network slice selection

In the UE attachment process, the RAN first selects an AMF (i.e., the initial AMF) for the UE to provide service based on the local storage information and the UE attachment request message. However, the initial AMF may not support the network slice to be used by the UE, for example, the initial AMF only supports FWA type network slice, but the UE requests a UeMBB type network slice. If the initial AMF cannot provide service to the UE, the initial AMF queries the NSSF and selects the target AMF that can support the UE network slice, and then sends the attachment request message of the UE to the target AMF directly or indirectly, and the target AMF processes the attachment request of the UE to provide network service to the UE.

Figure 1 Slice selection in the attachment process



1. If the UE has the Configured NSSAI of this PLMN or the Allowed NSSAI of this access type for this PLMN stored on the UE, then the UE will carry the Requested NSSAI information in the NAS registration request message and the AN message The Requested NSSAI contains the S-NSSAI of the slice that the UE wants to register.
2. The RAN selects the Initial AMF based on GUAMI or Requested NSSAI. if the UE does not provide Requested NSSAI and GUAMI in the AN message, the RAN shall send the registration request message from the UE to the default AMF.
3. The Initial AMF queries the UDM to obtain the UE signup information including Subscribed S-NSSAIs.The Initial AMF determines whether it can provide service to the UE based on the received Requested NSSAI, Subscribed S-NSSAI and local configuration. If the AMF can serve the UE, the Initial AMF is still the service AMF of the UE, and then the AMF constructs an Allowed NSSAI based on the Subscribed S-NSSAI and Requested NSSAI and returns it to the UE by registering the

acceptance message. if the Initial AMF cannot serve the UE or cannot make judgment, then the AMF needs to query to the NSSF.

4. AMF sends Requested NSSAI, Subscribed S-NSSAI, PLMN of SUPI, TAI, etc. to NSSF for query.
5. Based on the information received and the local configuration, the NSSF selects the AMF Set or list of candidate AMFs that can serve the UE, the Allowed NSSAI applicable to this access type and possibly the network slice instance that serves the UE, the NRF used for NF selection within the instance, and sends this information to the Initial AMF.
6. If the Initial AMF is not in the AMF Set and no AMF address information is stored locally, the Initial AMF obtains a list of candidate AMFs by querying the NRF, which returns a list of available AMFs, including AMF Pointer and address information. If the AMF cannot obtain the list of candidate AMFs by querying the NRF, the Initial AMF needs to send the registration request message of the UE to the target AMF through the RAN, and the message sent by the Initial AMF to the RAN contains the AMF Set and Allowed NSSAI.
7. If Initial AMF decides to send the NAS message directly to the target AMF based on the local policy and signing information, Initial AMF sends the UE registration request message and any other information obtained from the NSSF other than the AMF set to the target AMF.
8. If the initial AMF decides to forward the NAS message to the target AMF via the RAN based on the local policy and signing information, the initial AMF sends a Reroute NAS message to the RAN. the Reroute NAS message includes the target AMF Set information and the registration request message, as well as the relevant information obtained from the NSSF.
9. After receiving the registration request message sent in step 7, the target AMF continues to perform the relevant steps of the registration process and finally sends a registration acceptance message to the UE, which carries the Allowed NSSAI information.

3.7.1.1.4 Accessibility

Involved in NF

Involved in NF	Function Description
NRF	Support NF discovery function.
AMF	Supports initiating network slicing service requests to NSSF.
NSSF	Support network slice selection service.

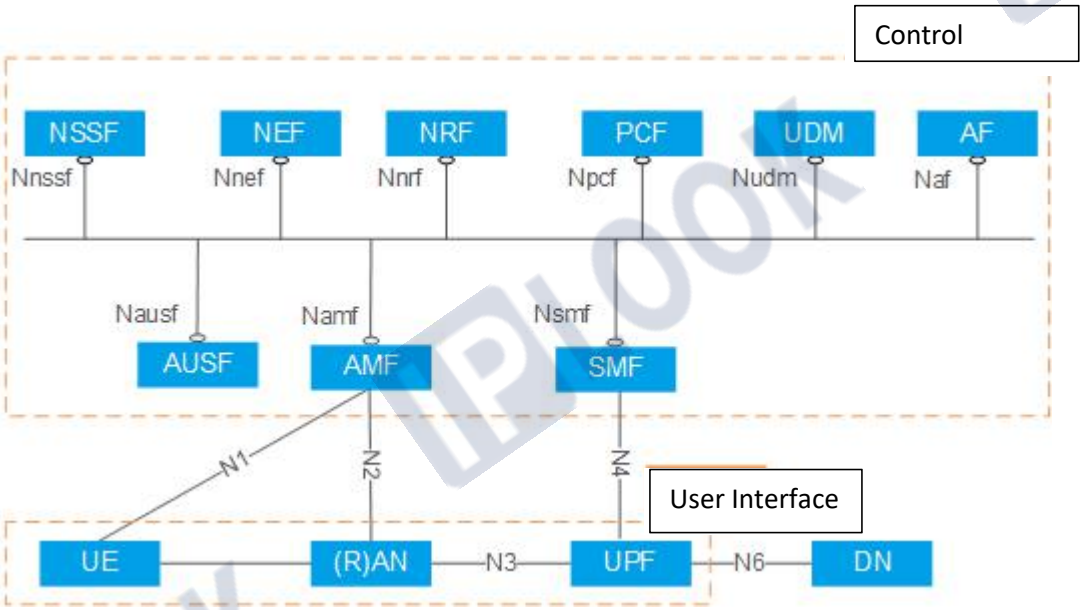
3.7.1.1.5 Application Restrictions

The AMF can only initiate service requests to the NSSF to which it belongs to the PLMN.

3.7.1.1.6 Principle Overview

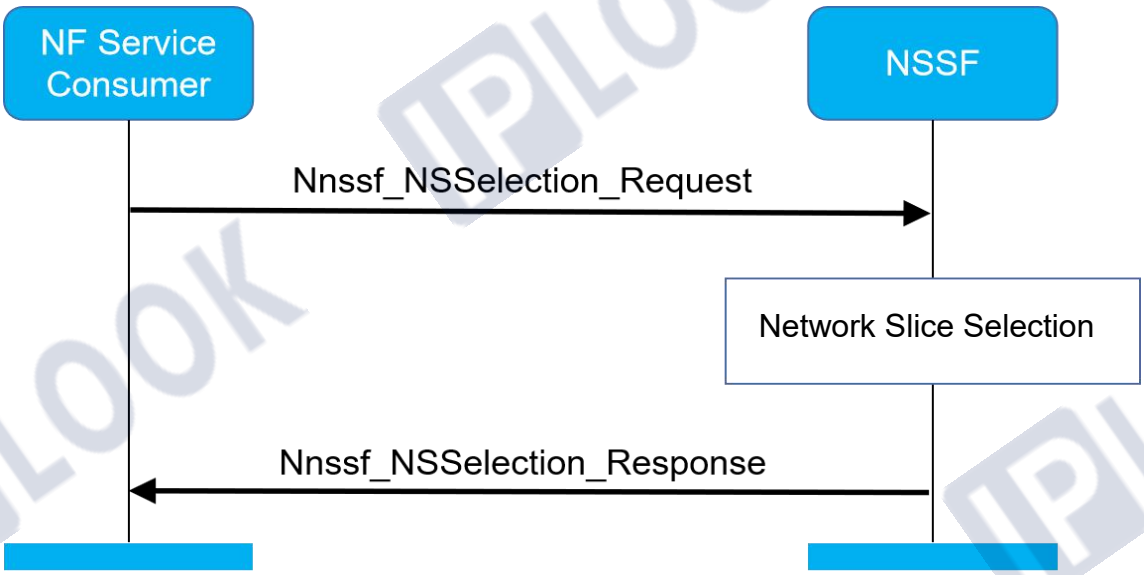
The 5GC network adopts a service-oriented architecture, abstracting the control plane functions into multiple independent Network Functions (hereinafter referred to as NFs), such as AMF, SMF, NRF, NSSF, etc., as shown in Figure 2. Each NF supports multiple services (Network Function Service, hereinafter referred to as NFS), and NSSF provides two NFSs, Network Slice Selection (Nnssf_NSSelection) and Network Slice Availability Management Service (Nssf_NSSAIAvailability).

Figure 2 5GC Network Service Architecture



Network Slicing Selection Process

The flow of an NF service consumer (usually an AMF) requesting network slice selection from an NSSF is illustrated below：



1. AMF sends Requested NSSAI, Subscribed S-NSSAI, and SUPI's PLMN and TAI to NSSF for query.
2. Based on the information received and the local configuration, the NSSF selects the AMF Set or list of candidate AMFs that can serve the UE, the Allowed NSSAI applicable to this access type, and possibly the network slice instance that serves the UE, and the NRF used for NF selection within the instance.
3. Return the selection information obtained in step 2 to the AMF.

3.7.1.1.7 Follow the standards

Standard category	Standard No.	Name of standard
3GPP	29.531	Technical Specification Group Core Network and Terminals; 5G System; Network Slice Selection Services;
	23.501	Technical Specification Group Services and System Aspects;System Architecture for the 5G System;
	23.502	Technical Specification Group Services and System Aspects;Procedures for the 5G

Standard category	Standard No.	Name of standard
		System;

3.7.1.2 Network Slicing Availability

3.7.1.2.1 Definition

This service is used by NF service consumers (e.g., AMFs) to update the AMF-supported S-NSSAI on the NSSF, subscribing and unsubscribing to notifications of changes in NSSAI availability information under each TA.

3.7.1.2.2 Customer Value

Beneficiaries	Benefit Description
Operators	It can reduce the manpower to configure the slicing of NSSF and AMF.
Subscriber	The user does not perceive the feature.

3.7.1.2.3 Application Scenarios

- **Slicing availability status update**: AAMF updates the S-NSSAI(s) supported on each TA of the NSSF.
- **Slicing status subscription/notification**：The AMF subscribes on a per-TA basis to any changes in NSSAI availability information, including s -NSSAI availability information per TA (unrestricted) and restricted s -NSSAI(s) per TA in the service PLMN of the terminal. When this information changes the NSSF notifies the corresponding AMF.

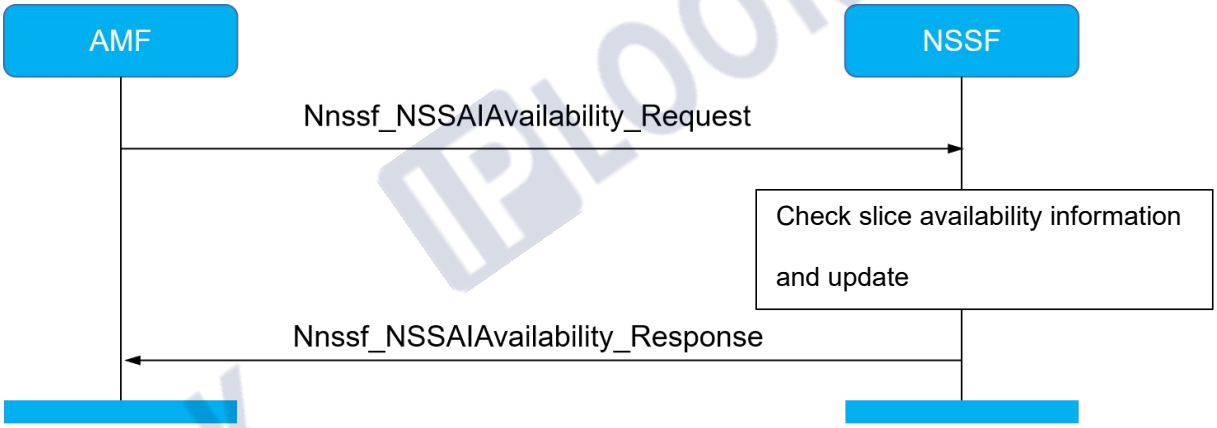
3.7.1.2.4 Accessibility

Involved in NF

Involved in NF	Support Version	Function Description
NSSF	No special requirement	• Authentication of slices to the AMF requesting the service and updating the slice availability information of the AMF. • Send notifications when the slice availability status of a TA to which AMF is subscribed changes.
AMF	No special requirement	• Supports initiating service requests to NSSF to obtain slice availability information and perform maintenance updates. • Supports initiating service requests to NSSF and subscribing to notifications of changes in NSSAI availabili information under TA.

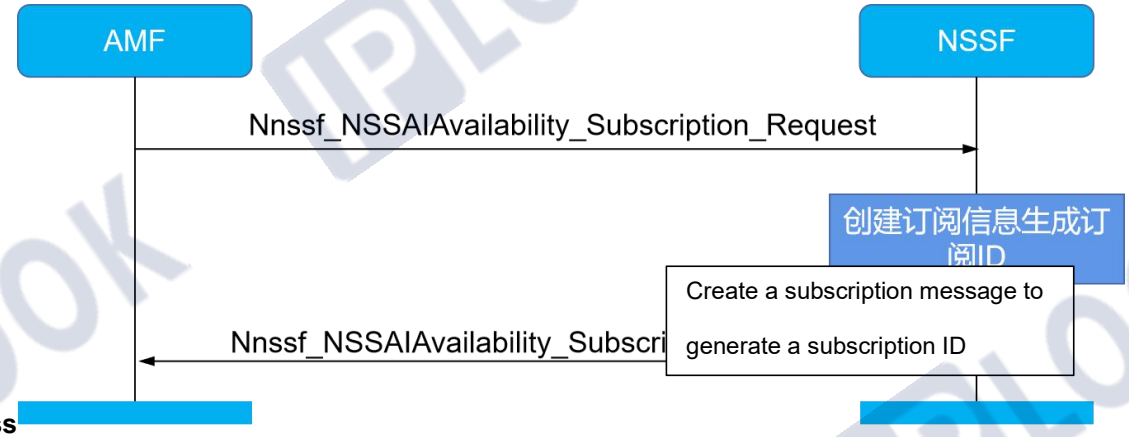
3.7.1.2.5 Principle Overview

Slicing availability update process



1. The AMF requests the Slice Availability Update service from the NSSF to replace or create NSSAIvailability information. The request carries the NssaiAvailabilityInfo, which contains one or more supported snssai information to be replaced.
2. The NSSF checks whether the NSSAI carried in this request is supported and updates the NSSAI availability information.
3. The NSSF returns the updated NSSAIvailability information, i.e. the response returns the AuthorizedNssaiAvailabilityInfo to the AMF.

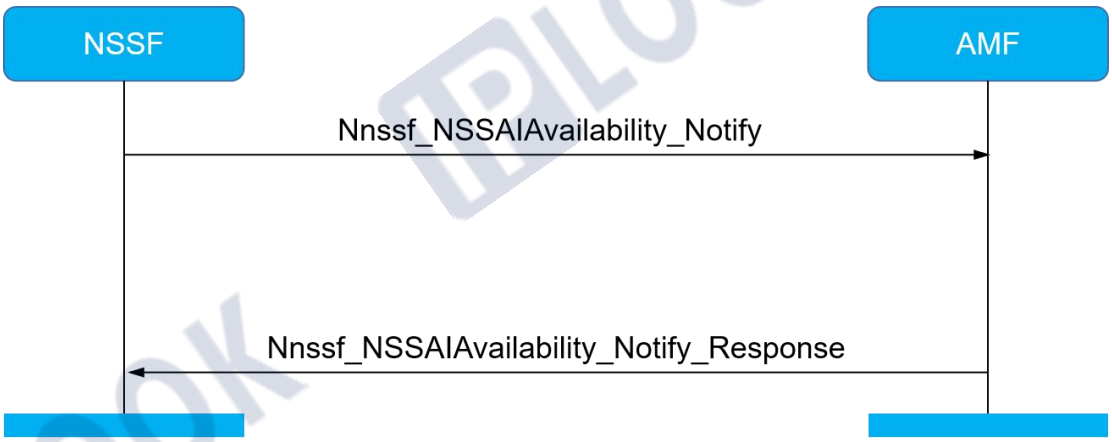
Subscription



Process

1. AMF sends Nnssf_NSSAIAvailability_Subscribe_Request message to NSSF to request subscription to NSSAI under each TA of an AMF or AMF set, carrying information such as subscription conditions, subscription events, subscription duration, and subscription notification conditions in the request message.
2. The NSSF sends the Nnssf_NSSAIAvailability_Subscribe_Response response to the AMF, carrying the subscription ID that uniquely identifies this subscription created by the NSSF.

通知流程



1. When the availability information of the slice under the corresponding TA of the subscribed AMF/AMF set changes, the NSSF sends a notification to the AMF, which is notified to the AMF via HTTP POST request.
2. The AMF receives the notification and returns a no content response.

3.7.1.2.6 Follow the standard

Standard category	Standard No.	Name of standard
3GPP	29.531	Technical Specification Group Core Network and Terminals; 5G System; Network Slice Selection Services;

4 Operation and Maintenance

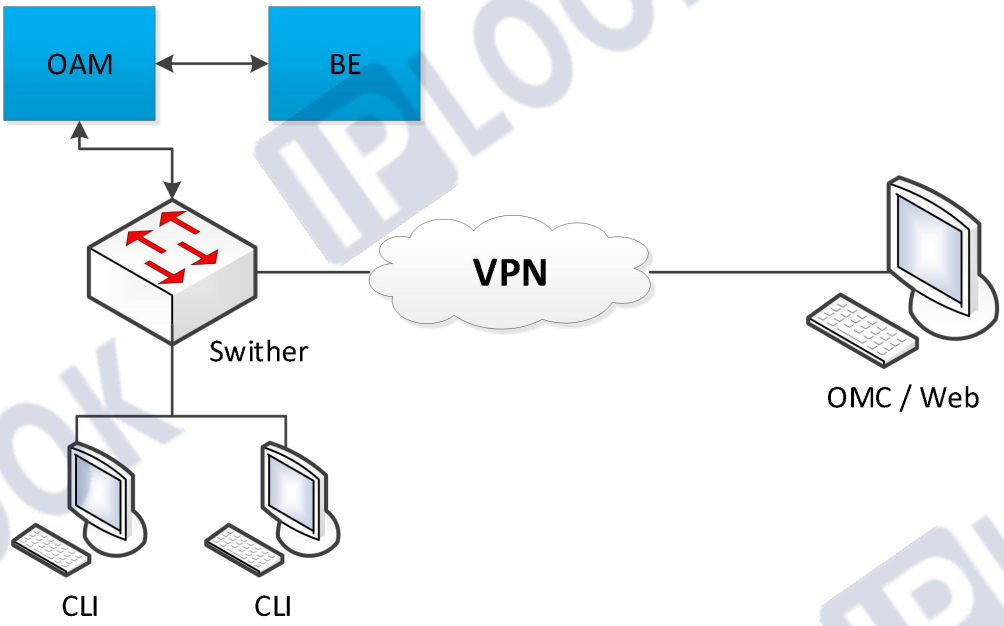
The IPLOOK provides a perfect operation and maintenance function and supports the unified EMS to implement daily maintenance and management.

Based on the Client/Server architecture, the operation and maintenance subsystem provides a GUI operation and maintenance subsystem and a Web UI performance measurement system to support customized human-machine interfaces.

The operation and maintenance subsystem supports three modes of operation:

- You can log in to the OAM server through a Web browser for management and operations
- Accessing to the OMC maintenance center for centralized management by the OMC.
- Remote operation and maintenance, accessing to the internal network through the dial-up server, and remote maintenance based on the Web.

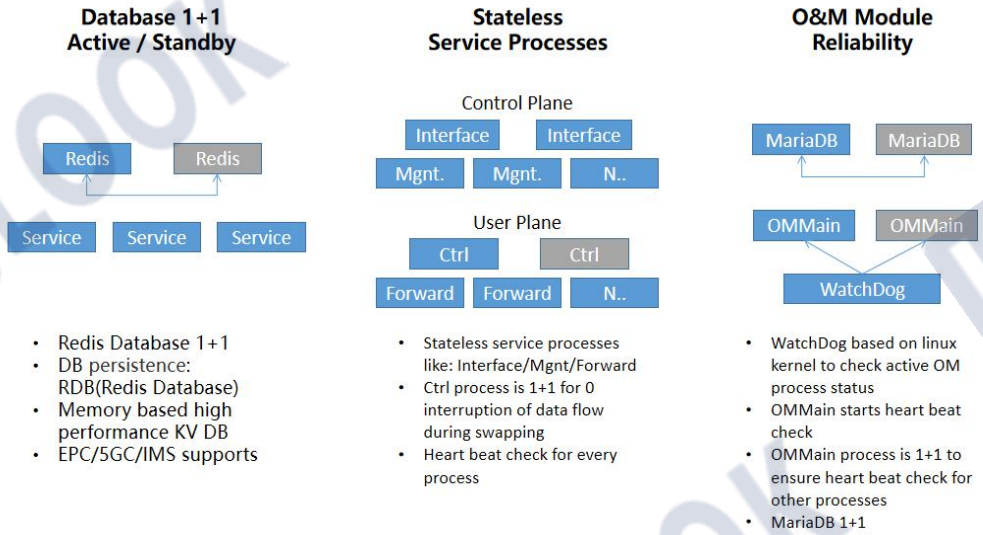
Figure 3 shows the network architecture



5 Reliability design

5.1 Software Reliability

Figure 4 software reliability



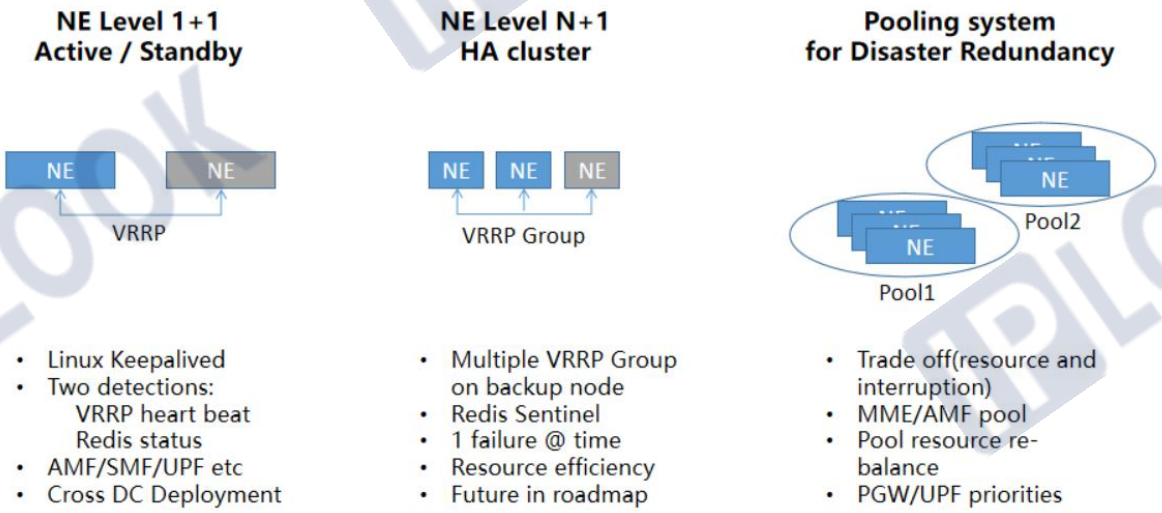
IPLOOK uses open-source database Redis in core network system, it is a memory-based Key-Value database, has great performance, and deployed as an active/standby redundancy mode. All stateful contexts of core network system are stored in this database. Other service processes are stateless such as interface message process, mobility management process, session management process and so on.

But for user plane, the session control process is deployed as active/standby mode to ensure ZERO interruption of the data flow during the service swapping procedure, for the backup forwarding table could be immediately in charge of dealing with packets.

And for O&M plane, the redundancy enforcements are deployed from the bottom at the Linux kernel, watchdog is here to check the active OM process status, this process is in charge of the heartbeat check with every other process.

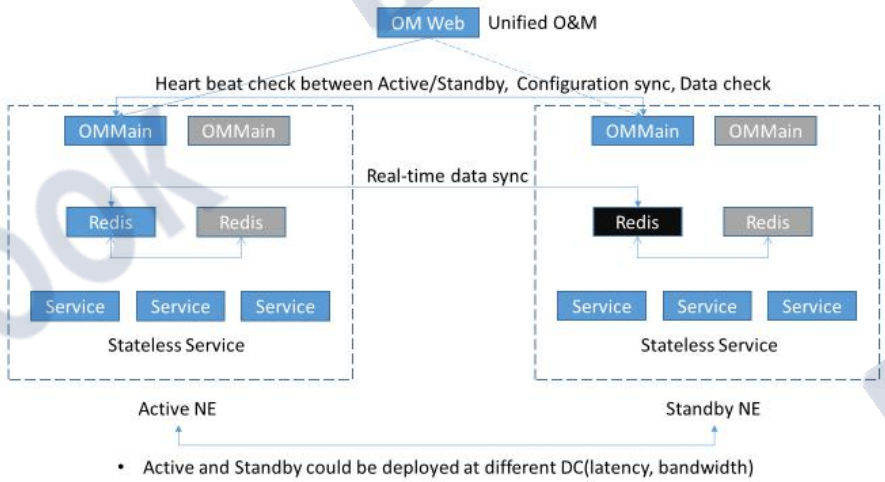
5.1 Network element Reliability

Figure 6 5GC redundancy



At NE level, IPLOOK provides pooling redundancy solution for different scenario requirement. 3GPP standard pooling system like MME pool, AMF pool, PGW/UPF DNS priorities set is for disaster redundancy.

Figure 7 OAM redundancy

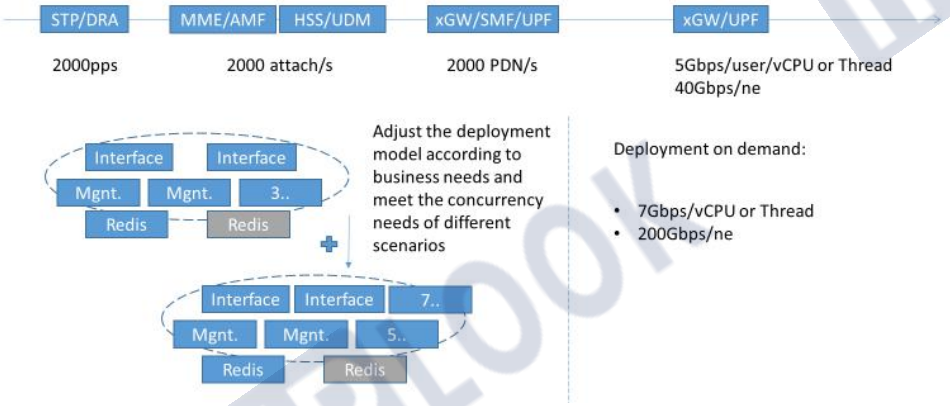


IPLOOK backup mechanism is hot backup, that means active node and standby node are synchronizing user data (context, state etc) in real-time, and they could be managed by a single unified O&M, so when the active node fails, the standby could immediately handle current service without any service interruption.

6 Dimension

6.1 Performance

Figure 8 Performance



One MME instance could support around 2000 attach/s at most, we can adjust the process deployment model according to the business needs and meet different concurrency requirements of different scenarios.

6.2 Dimension sheet

Table 5 Dimension

User/Site, Throughput	Intervals					
NE	Resource Requirement: CPU Thread(T),Memory(GB)					

User/Site	<10K/40	10K-50K/100	50K-100K/400	100K-200K/400	200K-500K/800	500K-1M/1600	1M-2M/3200
AMF/MME/SMF	8T, 16GB	20T, 32GB	40T, 64GB	40T, 64GB	2*(40T, 64GB)	4*(40T, 64GB)	8*(40T, 64GB)
UDM+AUSF+HSS+HLR	8T, 16GB	20T, 32GB	40T, 64GB	40T, 64GB	64T, 128GB	2*(64T, 128GB)	4*(64T, 128GB)
PCF+PCRF	8T, 16GB	20T, 32GB	32T, 64GB	40T, 64GB	2*(40T, 128GB)	4*(40T, 128GB)	8*(40T, 128GB)
NRF+NSSF	8T, 16GB	20T, 32GB	20T, 32GB	20T, 32GB	20T, 32GB	2*(20T, 32GB)	4*(20T, 32GB)
Throughput	<1Gbps	1-5Gbps	5-10Gbps	10-20Gbps	20-40Gbps	40-80Gbps	80-120Gbps
UPF/SGW/PGW	4T,8GB	8T, 16GB	16T,32GB	32T,64GB	48T,128GB	2*(48T,128GB)	3*(48T,128GB)

User/Site means maximum user number and eNB or gNB number to serve in specified hardware resource.

AMF/MME/SMF means they have same dimension methodologies, share same hardware resource requirements.

2*(40T, 64GB) means 2 sets of NEs or NFs to support required capacity.

Each NE/NF should have 100GB free HD space for usage.

For default virtualization deployment, 1 vCPU = 1 CPU Thread. So resource requirement set (CPU Thread(T), Memory(GB)) is equal to (vCPU, Memory(GB)).

7 Acronyms and Abbreviations

Table 6 Acronyms and Abbreviations

Abbreviations	Full Name
UPF	User Plane Function
5GC	5G Core Network
EPC	Evolved Packet Core
SGW-U	Service Gateway User Plane function
PGW-U	PDN Gateway User Plane function
RAT	Radio Access Technology
PDU	Protocol Data Unit
DN	Data Network
QoS	Quality of Service
5G-AN	5G-Access Network
GTPv1	General Packet Radio System (GPRS) Tunnelling Protocol
PFCP	Packet Forwarding Control Protocol
CP	Control Plane

SGW-C	Service Gateway Control Plane function
PGW-C	PDN Gateway Control Plane function
TDF-C	Traffic Detection Function Control Plane function
SMF	Session Management Function
PDR	Packet Detection Rule
FAR	Forwarding Action Rule
BAR	Buffering Action Rule
URR	Usage Reporting Rule
QER	QoS Enforcement Rule
PDI	Packet Detection Information
IP-CAN	IP-Connectivity Access Network
APN-AMBR	APN- Aggregate Maximum Bit Rate
GBR	Guaranteed Bit Rate
Session-AMBR	Session- Aggregate Maximum Bit Rate
QCI	QoS Class Identifier
QFI	QoS Flow Identifier

TDF-U	Traffic Detection Function User Plane function
PCC	Policy and Charging Control
ADC	Application Detection and Control
OCS	Online Charging System
F-TEID	Fully Qualified TEID
FQDN	Fully Qualified Domain Name
DHCPv6	Dynamic Host Configuration Protocol for IPv6
5GS	5G System
EPS	Evolved Packet System
GTP-U	GTP User
E-RAB	E-UTRAN Radio Access Bearer

8 Standard and specification

Number	Standard Number	Standard Name	Publishing Institution
1	TS23.003	Numbering, addressing and identification v15.4.0	3GPP
2	TS23.401	General Packet Radio Service(GPRS)enhancements for Evolved UniversalTerrestrial Radio Access Network(E-UTRAN)access	3GPP
3	TS 23.501	System Architecture for the 5G System	3GPP
4	TS 24.501	NAS Protocol for 5G-System v15.0.0	3GPP
5	TS 23.502	Procedures for the 5G System	3GPP
6	TS 23.503	Policy and Charging Control Framework for the 5G System	3GPP
7	TS 25.104	Base Station(BS)radio transmission and reception(FDD)	3GPP
8	TS 29.244	Interface between the Control Plane and the User Plane Nodes;Stage 3	3GPP
9	TS 29.281	General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U) v15.3.0	3GPP
10	TS 29.502	Session Management Services v15.0.0	3GPP
11	TS 29.518	Access and Mobility Management Services v15.0.0	3GPP
12	TS 36.420	Evolved Universal Terrestrial Radio Access Network(E-UTRAN);X2 generalaspects and principles	3GPP
13	TS 36.421	Evolved Universal Terrestrial Radio Access Network(E-UTRAN);X2 layer	3GPP
14	TS 36.422	Evolved Universal Terrestrial Radio Access Network(E-UTRAN):X2 signaling transport	3GPP
15	TS 36.423	Evolved Universal Terrestrial Radio Access Network(E-UTRAN):X2application protocol(X2AP)	3GPP
16	TS 38.201	NR;Physical layer;General description	3GPP

17	TS 38.300	NR and NG-RAN Overall Description:Stage 2	3GPP
18	TS 38.304	NR;User Equipment(UE)procedures in idle mode	3GPP
19	TS 38.211	NR;Physical channels and modulation	3GPP
20	TS 38.322	NR:Radio Link Control(RLC)protocol specification	3GPP
21	TS 38.331	NR;Radio Resource Control(RRC);Protocol specification	3GPP
22	TS 38.410	NG-RAN;NG general aspects and principles	3GPP
23	TS 38.412	NG-RAN; NG signalling transport v15.0.0	3GPP
24	TS 38.413	NG-RAN;NG Application Protocol(NGAP)	3GPP
25	TS 38.415	PDU Session User Plane protocol v15.0.0	3GPP
26	TS 38.422	NG-RAN:NG data transport NG-RAN;Xn signalling transport	3GPP
27	TS 38.423	NG-RAN:Xn Application Protocol (XnAP)	3GPP
28	TS 38.424	NG-RAN:Xn data transpdrt	3GPP
29	TS 38.425	NG-RAN;NR user plane protocol	3GPP