IPLOOK

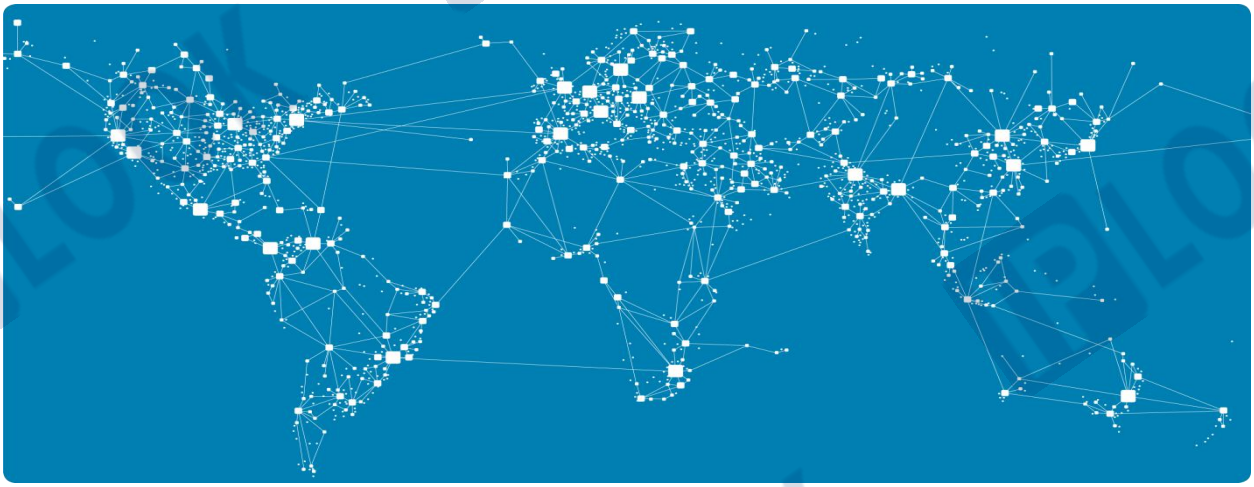
IPLOOK MME PRODUCT DESCRIPTION

IPLOOK Technologies

www.iplook.com

IPLOOK Technologies Co., Limited
Suite 1101, On Hong Commercial Building, 145 Hennessy Road, Wanchai Hong Kong

IPLOOK MME Product Information



IPLOOK Technologies / IPLOOK Technologies Co., Limited

Date (2022-01-24)

IPLOOK Technologies Co., Limited
Suite 1101, On Hong Commercial Building, 145 Hennessy Road, Wanchai Hong Kong

Revision history

Version	Usage State	Modification Summary	Reviser	Reviewer	Revision date
1.1	Initiation Version		Eddie	Li	10-08-18
1.2	Done	Add MME pool and Request information correction function.	Mark	James	21-02-21
1.3	Done	Support 5G NSA(Opt.3) networking	Mark	James	16-09-21

Table of Contents

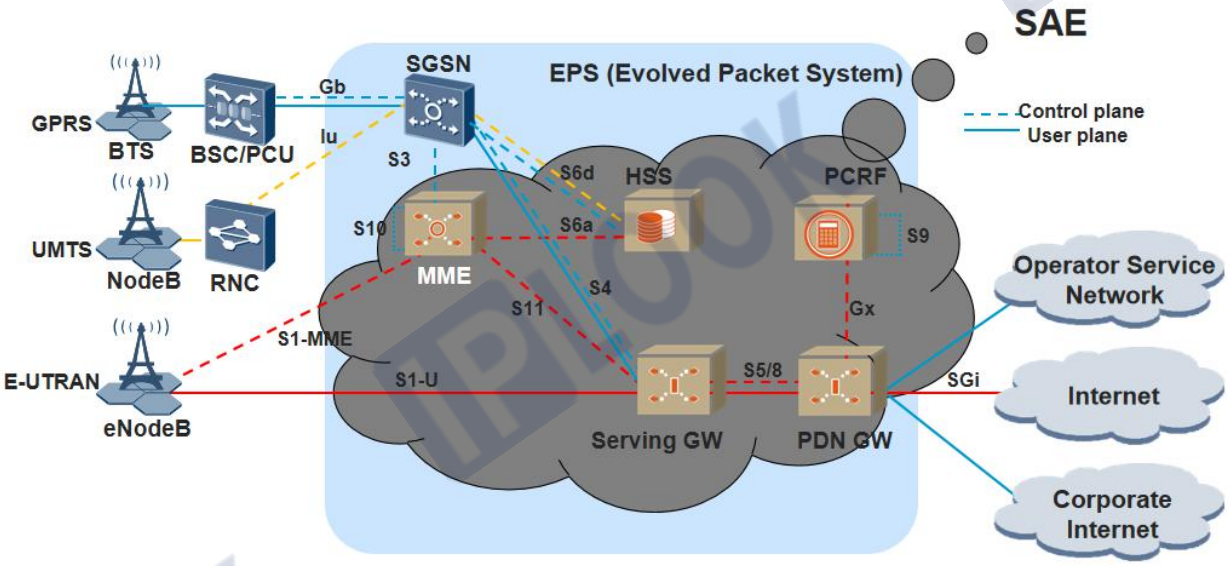
1 Introduction

1.1 MME overview

EPC refers to a core network architecture that supports LTE access networks. IPLOOK provides Long Term Evolution/Evolved Packet Core (LTC/EPC). The Mobility Management Entity (MME) represents the control plane for the User Equipments(UEs) to access the 4G LTE, or EPS network. From a UE's perspective, signaling for access control, location tracking, and bearer set up is performed via the MME. IPLOOK's manages the access control. It also validates the subscriber's location (in home network or visited network) through mobility management. It executes bearer management and provides routing functions to assist packet data forwarding between eNodeB and SGWs.

The location of MME in the EPC network is shown in Figure 1

Figure 1 Schematic Diagram



IPLOOK's MME adopts module structure and executes different functions through different modules. It is able to interconnect with different nodes in 4G, 2G or 3G network.

Table 1 Core network node description

Name	Function
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network.

Name	Function
MME	The Mobility Management Entity (MME) represents the control plane for the User Equipments(UEs) to access the 4G LTE, or EPS network. From a UE's perspective, signaling for access control, location tracking, and bearer set up is performed via the MME.
HLR/HSS	Home Location Register, which stores the subscription data and location information of subscribers and provides route information for calls from the network to subscribers. Home Subscriber Server, which stores the subscription data and location information of subscribers and implements subscriber authentication and authorization.
MSC	Mobile Switching Center, which provides the call conversion service and call control between the telephony and data systems.
CG	Charging Gateway, which lies between the Gn/Gp SGSN/GGSN and the Charging Center to send CDR files to the Charging Center.
SGW	The service gateway that implements user-plane data routing in the EPC network.
PGW/GGSN	Gateway GPRS Support Node, which provides routing and encapsulation of data packets between the 3G core-network and external data network. In EPC network, the GGSN is evolved into a PGW(the packet data network gateway) function node, that implements subscriber access to the PDN in the EPC network.
PCRF	Implements policies and charging rules.
PDN	Provides the data transmission service for subscribers.

1.2 Highlight features

1.2.1 Virtualization

Software and hardware are decoupled through virtualization. The IPLOOK MME 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 MME hardware resources are virtualized to many VMs. When the IPLOOK MME needs to increase its processing capability, more VMs can be installed.
The IPLOOK MME 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 MME 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 EPC solution, all NEs like MME, SGW, PGW, HSS, PCRF, IMS, DRA and web management functions are in a single server. It also supports Gy or Radius for external billing.
Compact EPC specification:
1U Server: 2000 UEs, 20 eNBs, up to 600Mbps
2U Server: 5000 UEs, 50 eNBs, up to 6Gbps

1.2.4 Open Interfaces and Flexible Network Architecture

The MME system provides a series of products and open standard interfaces.
The IPLOOK MME 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 MME performs daily maintenance and management through the unified EMS .
The IPLOOK MME 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 MME 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 vEPC 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.

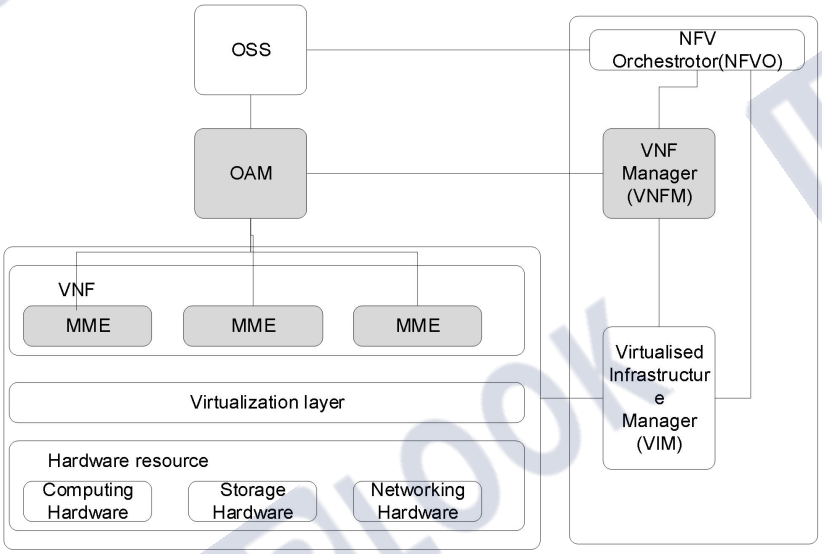
In addition, by using specific 10G, 40G or 100G NIC from Intel, the performance can be further enhanced.

2 System architecture

2.1 IPLOOK MME in the NFVI

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

Figure 2 IPLOOK MME System Architecture



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

Table 2 IPLOOK MME 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 Basic function

3.1.1 Mobility management

3.1.1.1 Definition

The mobility management function EMM (EPS mobility management) is used to control the access of UE (user equipment) in LTE / EPC and track the current status of UE Location information of the UE, i.e. TA (tracking area) / Ta list, MME (mobility management entity), etc

3.1.1.2 Dependency

UE	eNodeB	MME	S-GW	PDN-GW	PCRF	HSS
√	√	√	√	√	√	√

3.1.1.3 Principle description

The mobility management function is mainly realized through user status management, attachment, tracking area update, service request, handover, separation and access control process.These processes ensure the timely update of UE location information in relevant network entities when UE moves.

Mobility management this section includes the following:

• User status management

User status is divided into user mobility management status EMM (EPS mobility management) and user connection management status ECM (EPS connection management).

The user mobility management status EMM is generated by the attach and TAU processes.The user connection management state ECM describes the continuity of signaling between the UE and the core network.

• Attachment process

UE needs to register with the network to use network services. This registration process is called network attachment.During the process of network attachment, a default EPS bearer will be established, which provides permanent IP connection.The PCC (policy and charging control) rules applied to this default bearer can be predefined in p-gw / pgw-c and activated by p-gw / pgw-c during attachment.The attachment process may trigger the establishment process of one or more proprietary EPS bearers.

• Separation process

The separation process allows the UE to notify the network side that it will not continue to access EPS, or the network side to notify the UE that it will not continue to allow it to access EPS network.

The separation process is used in the following cases:

UE is separated from EPS service.

The UE disconnects from the last PDN.

The network notifies the UE that it can no longer access EPS.

• TAU process

The basic unit of location management is ta list.TA list consists of one or more ta (tracking area). When the UE moves out of a TA list, in order to let the MME know the location of the change, the UE needs to update the information of the tracking area where the user is located through the TAU process.

Triggering conditions of TAU (tracking area update):

The UE finds that the current TAI is not in the TA (tracking area) list of the UE registered network.

Periodic TAU.

The access type of UE, that is, RAT type (GERAN, UTRAN, E_UTRAN) is changed.

Network side load balancing triggers TAU.

TAU triggered during handovering.

• service requests

The service request process is used to send data when the user status is ecm-idle (for example, the user does not transmit data for a long time)

The process of requesting the network to re-establish S1 user plane bearer and wireless bearer.

• Handover process

In the ecm-connected state, the handovering process will be triggered after eUTRANdecides to reselect.

MME supports the following types of handovering:

Intra-EUTRANhandover

X2 based handover (where X2 interface is the interface between eNodebs)

S1-based handover

3.1.2 Authentication function

3.1.2.1Definition

The authentication function realizes the identification and authentication of users and the synchronization of keys. This function judges the validity of users' identity, so that legitimate users can use the services provided by the network.The authentication process is associated with the mobility management related processes.Authentication in SAE network is bidirectional, and users can also authenticate the network to ensure the security of access network.

3.1.2.2 Dependency

UE	MME	HSS
√	√	√

3.1.2.3 Principle overview

Similar to UMTS authentication, EPS network has not only the function of network authentication, but also the function of user authentication network and integrity protection.In addition, EPS network also uses more powerful encryption algorithm and integrity algorithm.

EPS authentication vector is composed of RAND, AUTN, XRES and Kasme.The EPS authentication vector is requested from HSS by MME.

EPS authentication Quad:

• RAND（Random Challenge）

Rand is an unpredictable random number provided by the network to UE, with a length of 16 bytes.

• AUTN（Authentication Token）

The function of autn is to provide information to UE so that UE can use it to authenticate the network.The length of autn is 17 bytes.

• XRES（Expected Response）

Xres is the desired UE authentication response parameter.It is used to compare with RES (or RES + RES_EXT) generated by UE to determine whether authentication is successful.

The length of XRES is 4-16 bytes.

• Kasme is a root key derived from CK / IK and ASME (MME) PLMN ID.Kasme is 32 bytes long.

During authentication, MME sends RAND and AUTN to UE, and USIM can decide whether to return RES or refuse authentication.

3.1.3 User identity confidentiality function

3.1.3.1 Definition

The user identity confidentiality function is realized through the distribution of GUTI.The purpose of allocating GUTI (globally unique temporary UE identity) is to provide a temporary identity for users accessing the network, and this identity will not show the user permanent identity.

3.1.3.2 Dependency

UE	MME
√	√

3.1.3.3 Principle description

Related concepts

GUTI consists of the following two parts:

• GUMMEI: GUMMEI consists of MCC, MNC and MME identification.

• M-TMSI: the length of M-TMSI is 32 bits, which uniquely identifies a UE in an MME.

GUTI distribution process

MME supports bringing GUTI to UE through attachment process, TAU process and GUTI redistribution process.

In the attachment and TAU processes, MME brings GUTI to UE through attach accept message and TAU accept message respectively.

3.1.4 NAS Signaling encryption and integrity protection

3.1.4.1 Definition

NAS (non Access Stratum) protocol is a protocol between UE and MME, which supports the transmission of service and signaling messages between the core network and UE.
NAS signaling encryption and integrity protection can encrypt and protect NAS signaling and improve the security of the system.

3.1.4.2 Dependency

UE	MME
√	√

3.1.4.4 Principle description

In EPS network, there are two different levels of security alliances between UE and network:

• RRC (radio resource control) and up (user plane) security alliance between UE and E_UTRAN.RRC security alliance protects and encrypts the integrity of RRC signaling between UE and E_UTRAN.Up security alliance encrypts the user plane data between UE and E_UTRAN.

• NAS security alliance between UE and MME.It provides encryption and integrity protection of NAS signaling.

The NAS signaling encryption and integrity algorithms supported by MME include: null encryption / null integrity algorithm, AES (Advanced Encryption Standard), SNOW 3G and ZUC.

• empty encryption / empty integrity algorithm: the algorithm flow in the empty encryption algorithm is the same as other algorithms, but the plaintext and ciphertext before and after encryption are exactly the same.The null integrity algorithm adopts all 0 32-bit message authentication code (MAC), and the use process is the same as that of other integrity algorithms. The null integrity algorithm is only used for ues that fail to pass authentication in emergency calls.

• SNOW 3G algorithm: SNOW 3G is a basic 3GPP encryption algorithm and integrity algorithm. The corresponding algorithms include EEA1 (EPS encryption algorithm 1) and eia1 (EPS integrity algorithm 1), and the key length is 128 bits

• AES algorithm: AES is the most widely used encryption, decryption and integrity algorithm in the world. The corresponding algorithms include EEA2 (EPS encryption algorithm 2) and EIA2 (EPS integrity algorithm 2), and the key length is 128 bits

• ZUC algorithm: ZUC algorithm (also known as Zu Chongzhi algorithm) is a sequence cipher algorithm for hardware design.According to the 128 bit initial key and 128 bit initial vector, the algorithm outputs a 32-bit key sequence for data encryption and integrity protection.MME supports ZUC encryption algorithm.

NAS security mode negotiation process:

1. MME negotiates the algorithm according to the supported algorithm brought by the mobile phone attach or TAU (i.e. the security capability of UE) and the supported algorithm configured by MME itself.Calculate the encryption key and integrity key according to the negotiated algorithm ID and algorithm type.

2. MME sends NAS security mode command message to the mobile phone to inform the selected algorithm of the mobile phone network.The message mainly contains: replayed UE

security capability (security capability returned to the mobile phone, which is used by the mobile phone to judge whether it has been tampered by the attacker), ENEA (negotiated encryption algorithm ID), ENIA (negotiated integrity protection algorithm ID), KSI.The message has been integrity protected with the selected integrity protection algorithm.

3. After receiving the NAS security mode command message, the phone will first check the integrity.After the integrity check, the returned mobile phone security capabilities will be compared. If the security capabilities match, the mobile phone will return the NAS security mode complete message to MME.The message has been encrypted and integrity protected.

4. After receiving the NAS security mode complete message, MME checks and decrypts the integrity and learns that UE has reached an agreement with MME.

5. After the NAS security mode command process is successful, encryption and integrity protection will be started for all distributed NAS messages, and the integrity of all incoming NAS messages will be checked and decrypted according to the security header in the message.

3.1.5 Identification function

3.1.5.1 Definition

Identification means that the network requires the user to provide various identity (including IMSI, IMEI and IMEISV) to identify the user real identity.

3.1.5.2Dependency

UE	MME
√	√

3.1.5.3 Principle description

Basic concepts

• IMSI (International Mobile Subscriber Identity): the unique identification code assigned to mobile users by EPS system.

• IMEI (International Mobile Equipment Identity): the unique device ID assigned to the mobile terminal.It consists of TAC (category batch)

Standard code), FAC (product assembly code), SNR (serial number) and spare bit.

• IMEISV (international mobile station equipment identity and software version number):

Copy version.It is composed of 16 bit hexadecimal code, including IMEI and SVN (software version number).

• GUTI (globally unique temporary UE identity): it identifies the system assigned to the mobile phone rather than the mobile station itself.GUTI by

MME allocation is only used for LTE access.

• EIR (equipment identification register): in EPS system, equipment identification register is a logical entity, which is responsible for storage

International mobile device identification.

Identification process

Circumstances triggering the identification process:

• when the UE attaches to the network with the temporary identity GUTI, and the first authentication fails, send an identity request message to obtain the IMSI of the UE to initiate the second authentication.

• when the UE attaches to the network with the temporary identity GUTI, the MME cannot recognize the temporary identity GUTI of the UE. In order to obtain the real identity of the UE (i.e. IMSI), the MME sends the identity request message identity request to the UE.

• when the UE attaches to the network with the temporary identity GUTI, the MME needs to obtain the IMEI or imeisv of the UE, and the MME will send the identity request message identity request to the UE.

3.1.6 User data management

3.1.6.1Definition

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

User data includes user signing data in HSS and data dynamically generated during user access to EPC network.

3.1.6.2 Dependency

HSS	MME
√	√

3.1.6.4 Principle description

User data

Mobile user data includes two parts:

1. Information of mobile users signing up in HSS, such as:

IMSI, MSISDN, operator determined barring, access restriction data, 3GPP charging characteristics, subscribed UE AMBR, network access mode, APN configuration, etc

2. Data dynamically generated during user access to EPC network and bearer context, including mm context and EPS bearer context, such as:

IMSI、MSISDN、MM State、GUTI、ME Identity、Tracking Area List、UE Radio Capability UE network capability, Ms network capability, selected NAS algorithm, selected as algorithm, eksi, Kasme, MME IP address for S11, MME TEID for S11, SGW IP address for S11, SGW TEID for S11, ENB UE s1ap ID, MME UE s1ap ID, ue-ambr, etc

User data management function

User data in the user data management feature refers to:

• Information signed by mobile users in HSS, including user ID IMSI / MSISDN, user EPC signing information, ODB, billing information, roaming restrictions, etc.

• Data dynamically generated in the process of user accessing EPC network and activating bearer, including user's current location information, IP address assigned to UE in current session, IP address of connected S-GW / p-gw, QoS resources actually enjoyed by users, APN used, etc.

The user data management function of MME includes the following aspects:

1. When the user attaches or the tracking area is updated to a new MME for the first time, the MME actively requests the subscription data of the user from HSS;When the user subscription data (such as QoS) in HSS changes, HSS will actively insert the updated user data into MME to modify the subscription data on MME.

2. When the MME receives the mobile user data, it checks the user signing characteristics (including ODB, service and other function items). If some of these characteristics are not supported, it will notify HSS, which will store these information locally and decide whether to allow the user to access the MME according to this information.

3. When a user is active in the MME service area, MME always retains the user's data to reduce the interactive signaling with HSS.When the user is not attached again within a period of time after separation, MME will actively clear the user data and release the occupied resources. This time can be set by the maintenance personnel.

4. When a user roams to another MME, HSS will notify the original MME to delete user data.MME provides maintenance commands for maintenance personnel to query and delete user data.The query content can be the detailed data of the specified user, such as MM Context and EPS context information can also be the statistical information of the whole system, such as the number of currently attached users of MME, the number of activated EPS bearers, etc.

User data management process

Processes related to user data management functions include:

1.Insert Subscriber Datatechnological process

2.Delete Subscriber Datatechnological process

3.Purge UEtechnological process

4.Update Locationtechnological process

5.Cancel Locationtechnological process

6.Notificationtechnological process

7.Authenticationtechnological process

3.1.7 Session management function

3.1.7.1 Definition

Session management function is the basic function of MME and the basis for users to establish a connection with external PDN for data services.The session management function of MME includes the session management initiated by the network side and the session management initiated by the UE.

3.1.7.2 Dependency

UE	MME	eNodeB	HSS	SGW	PGW	PCRF

√	√	√	√	√	√	√

3.1.7.3 Principle description

Basic concepts

The object of EPC session management is EPS bearer.Each PDN connection consists of EPS bearer and IP connection.

PDN connection: EPS provides ue with an IP connection between UE and PDN through E_UTRANnetwork and EPC network, which is called PDN connection.

EPS bearing: used to uniquely identify the common QoS service flow between UE and p-gw based on GTP protocol, or the common QoS service flow between UE and S-GW based on PMIP protocol.

Default bearer: when the UE establishes a PDN connection to a PDN, an EPS bearer will be established. This bearer will not be released during the PDN connection to provide a permanent connection to the PDN. This bearer is called the default bearer.The default bearer is deleted and the PDN connection will be released.

Proprietary bearer: a bearer connected to the same PDN other than the default bearer is called a proprietary bearer.Different proprietary bearers are established according to different QoS requirements, such as watching videos, browsing web pages, etc.

Relationship among PDN connection, default bearer and proprietary bearer:

• APN and PDN are one-to-one correspondence.A PDN is represented by an APN. Different APNs can be connected to different PDNS.A terminal can access different PDNS through multiple APNs, and there can be multiple servers (Baidu, Youku, etc.) in the PDN.

• multiple PDN connections can be established under the same APN.A default bearer must be established for the same PDN connection, and only one default bearer can be established, but

multiple proprietary bearers can be established.Due to the limitation of the wireless side, a terminal can only establish 11 bearers at most

Bearer state management

Bearer states are divided into bearer context inactive and bearer context active. The conversion relationship between them in MME is as follows:

• when the bearer context is activated, the bearer status in the MME will be converted from bearer context inactive to bearer context active.

• when the bearer context is deactivated, the bearer status in MME will be changed from bearer context active to bearer context inactive.

• when the bearer context is updated, the bearer status in the MME remains bearer context active.

Session management function

The session management function includes the session management initiated by the network side and the session management initiated by the UE.Due to the needs of different services of users, the UE side can request the proprietary EPS bearer activation process, EPS bearer modification process or EPS bearer deactivation process. If the network side receives the UE's request, the network side will initiate the EPS bearer activation process, EPS bearer modification process or EPS bearer deactivation process. The network side is the initiator of the final process.

1.Session management initiated on the network side:

Proprietary EPS bearer activation: the purpose is to establish specific QoS and TFT bearer between UE and EPC.

EPS bearer modification: the purpose is to modify the QoS and TFT of EPS bearer

EPS bearer deactivation: the purpose is to deactivate one EPS bearer or all EPS bearers to the PDN

2.UEInitiated session management:

Default bearer context activation: establish a default EPS bearer context between UE and EPC.

UE requests PDN connection establishment: requests the establishment of a default bearer to a PDN.

UE requests PDN connection disconnection: UE requests disconnection from PDN.

UE requests bearer resource allocation and modification: UE requests bearer resource allocation, which is used for ue to allocate bearer resources for new service data flow requests.UE request bearer resource modification is used for ue to request modification of bearer resources for existing service data flow.

Typical trigger scenarios of session management process:

Default bearer activation:

After the 4G user turns on the mobile phone, the UE side initiates the default bearer and establishes a PDN connection. At this time, the user can surf the Internet normally.The PDN connection and the default bearer are established synchronously.

Proprietary bearer activation:

The activation process of proprietary bearer is initiated by the network side.

If dynamic PCC is deployed, PCRF sends rar message to p-gw to trigger proprietary bearer establishment, and the message contains qospolicy.

If the dynamic PCC is not deployed, the p-gw applies the local QoS policy to initiate a proprietary bearer establishment process

Bearer updates:

The bearer update process initiated by HSS is used to modify EPS bearer QoS parameters, such as QCI and ARP, or to modify ue-ambr and apn-ambr.

Bearer update process initiated by p-gw.The p-gw initiates a proprietary bearer update process with QoS update, which is used to modify EPS bearer QoS parameters, such as QCI, GBR,

MBR or ARP, or apn-ambr.For example, PCRF configures FUP service and initiates IP-CAN modification (QCI / GBR / MBR / ARP change) process for online users.P-gw can initiate a proprietary bearer update process without QoS update, which is no different from the proprietary bearer update process with QoS update initiated by p-gw. The main difference is that QoS update refers to the update of QCI, ARP and other parameters in EPS bearer QoS. QoS non update refers to the update of TFT, while the QoS parameters in EPS bearer QoS are not updated.

Bearer deactivation:

ENodeB / MME initiates bearer deactivation and only deactivates proprietary bearer.

When eNodeB sends a bear release request message to MME, it carries EPS bear identity cell.

MME initiates the bearer deactivation process through OAM (operation, administration and maintenance).

PGW initiates bearer deactivation. In this scenario, a proprietary bearer or all bearers of a PDN link are deactivated.

3.1.8 Support multiple PDN / PDU functions

3.1.8.1 Definition

Multi PDN / PDU (packet data network) function means that a UE creates multiple PDN connections (EPC) to access multiple external PDN networks at the same time to meet the requirements of users accessing multiple networks at the same time.

3.1.8.2 Dependency

UE	MME	SGW	PGW

√	√	√	√

3.1.8.3 Principle description

EPC supports multiple PDN functions

EPC supports a UE to create multiple PDN connections at the same time, and conduct IP service exchange with multiple PDN networks through one or more pgw-c.

After the UE initiates the PDN connection establishment request, the MME determines the SGW and PGW that should be used for each PDN connection.During or after the default bearer establishment, PGW assigns an independent IP address to UE for each PDN connection, and UE uses these IP addresses to access the corresponding PDN.Each PDN connection can trigger the establishment of one or more proprietary bearers.See the default bearer activation process in 4G network mobility management features for the detailed process.

The user's multi PDN connection has the following limitations:

There are up to 11 PDN connections per user at the same time.When the total number of PDN connections existing at the same time exceeds 11, MME will refuse to establish a new PDN connection.

3.1.9 Path management

3.1.9.1Definition

Path management refers to a mechanism in which the local end sends relevant signaling to the opposite end to judge whether the path is normal by checking whether the opposite end responds, so as to clear the invalid path in time.

3.1.9.2 Dependency

SGW	MME
√	√

3.1.9.4 Principle description

Basic concepts

A path is a one-way or two-way channel with no connection between two endpoints.Path management is to detect the communication path failure with the opposite network element and the working state of the opposite network element by sending a path management message.Path message types include:

Echo request and echo response messages based on GTP protocol.

System implementation

On the communication path, the local end can send an echo request message to the peer device to confirm whether the communication path and the peer ne work normally.After receiving an echo request, the opposite ne returns an echo response message to the local ne.After receiving the response message, confirm that the communication path and the opposite NE are working normally.

If the MME does not receive the response message returned by the peer ne within the time period configured by the system, it will resend the detection message.If no response is received after the maximum number of retransmissions configured by the system is reached, it is considered that the communication path or the opposite ne is faulty.

Path management function is an important fault detection function in the network. Using path management function is an important guarantee for the basic communication of the network.

3.1.10 S1-MME Interface

3.1.10.1Definition

S1 interface is the interface between eNodeB and core network (CN) in EPC system.Signaling exchange and service transmission between UE and CN shall pass through S1 interface.

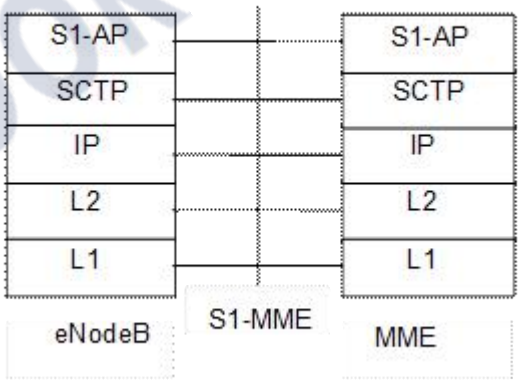
S1-MME interface is the control plane interface between eNodeB and MME. the signaling connection function of s1-MME interface provides reliable transmission for wireless network signaling.

3.1.10.2 Dependency

eNodeB	MME
√	√

3.1.10.3 Principle description

S1-MME interface protocol stack:



S1-AP (S1 Application Protocol): the application layer protocol between eNodeB and MME.

SCTP: this protocol is used to ensure signaling message transmission between eNodeB and MME.

3.1.11 S6a Interface

3.1.11.1Definition

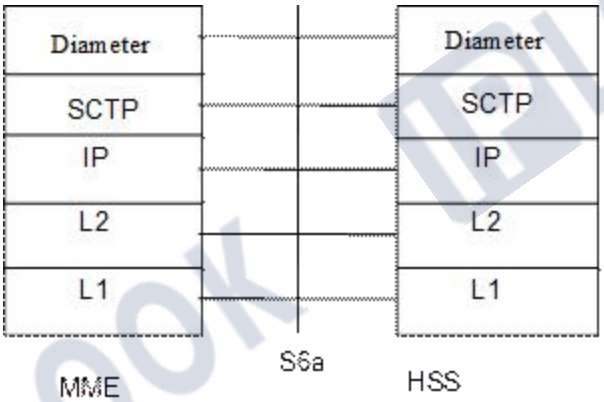
S6a interface is the interface between MME and HSS in EPC system.It is used to provide functions related to user signing data management and authentication.In the roaming scene, The MME also needs to be connected to the HSS where the user belongs through the S6a interface.

3.1.11.2 Dependency

HSS	MME
√	√

3.1.11.3 Principle description

S6a interface protocol stack:



Diameter: this protocol is used to support MME and HSS to transfer signing and authentication data to authorize users to access EPS network.SCTP: this protocol is used to ensure signaling message transmission between MME and HSS.

3.1.12 S11 Interface

3.1.12.1Definition

S11 interface is the signaling interface between MME and S-GW / sgw-c. it is mainly used for transmitting bearer creation, update and deletion request messages between MME and S-GW / sgw-c. when UE is in ecm-idle state, it is used for S-GW / sgw-c to notify MME to page UE and restore S1 bearer.

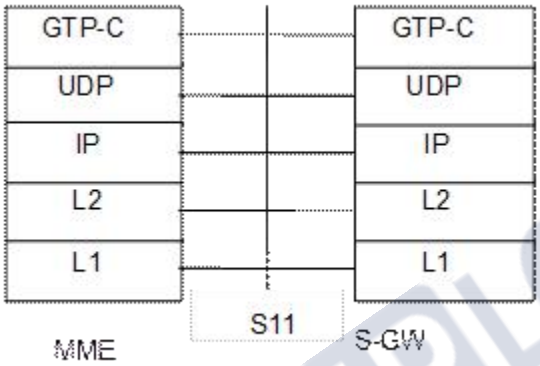
S11-u interface is the user interface between MME and S-GW / sgw-u, which is used to transmit uplink and downlink user interface data between MME and S-GW / sgw-u and realize Internet of things services.

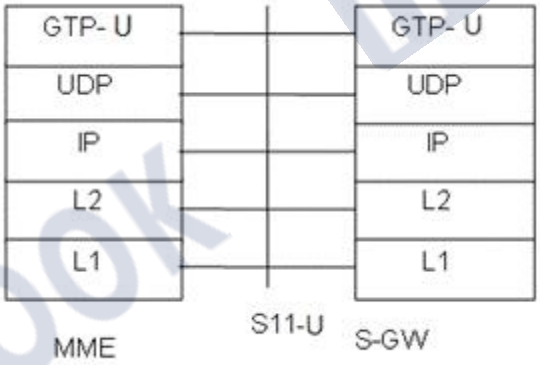
3.1.12.2 Dependency

SGW	MME
√	√

3.1.12.3 Principle description

S11 interface and S11-u interface protocol stack:





GTP-C (GPRS tunneling protocol for the control plane): use the tunneling protocol to transmit signaling between gsns in the backbone network.

The main signaling includes path management, tunnel management, mobile management and location management to realize backbone network channel maintenance, session establishment / modification / deletion and user information interaction.

GTP-U (GPRS tunneling protocol for the user plane): use the tunneling protocol to transmit user data between the gsns of the backbone network, use the tunneling protocol to transmit data, shield the influence of the upper layer protocol, and provide a session level two-way fast transmission channel.In addition to data packets, the GTP protocol user plane also includes data transmission error indication, echo message, supported extension header list and other user plane transmission auxiliary signaling.

• GTP-C version is gtpv2.

• GTP-U version is gtpv1.

3.1.13 IPv4v6Dual stack access

3.1.13.1 Definition

This feature supports the simultaneous allocation of IPv4 and IPv6 addresses to the UE in the PDN connection establishment process, so that the UE can be connected later

The IPv4v6 address is used for data transmission to provide users with IPv4v6 dual stack access service.

3.1.13.2 Dependency

UE	MME	PGW	SGW	HSS
√	√	√	√	√

3.1.13.4 Principle description

Ipv4v6 process involved in PDN connection:

The following description is only made for the ipv4v6 dual stack control process:

1.Modify the control strategy through the signing data, so that the user can support IPv4v6 services.

2. After the UE sends a PDN connection request to the MME, the MME selects a pgw-c according to the APN, establishes a default bearer, and assigns a bearer ID to the default bearer.After pgw-c is selected, if UE requests ipv4v6 dual stack, start ipv4v6 dual stack control strategy.

3. After the PDN type is determined as ipv4v6 dual stack, MME sends a create session request message to sgw-c, which carries the dual stack ID (dual address bearer flag = 1) and PDN type.Sgw-c sends this message to pgw-c.Pgw-c replies create sessionresponse to sgw-c and transparently transmits it to MME, carrying dual stack information, including PDN type and PDN address.Pgw-c can accept the dual stack request or reject the dual stack request. When rejected, the dual stack will be corrected to a single stack. Pgw-c directly sends the single stack address to UE and carries the reason value as follows:

• "new PDP type due to network preference" indicates that pgw-c has selected a PDN type that is inconsistent with the UE request.

• "new PDP type due to single address bearer only" means that UE requests dual stack. Pgw-c supports IPv4 and IPv6, but does not support dual stack.

4. MME sends a setup bearer request message to eNodeB, which also contains a NAS message, activate default epsbearer request.In case of IPv4v6 dual stack, the NAS message carries the dual stack information.

3.1.14 MME Pool

3.1.14.1 Definition

The MME pool feature is that multiple MMEs simultaneously serve the same wireless area (MME pool area). MMEs in the pool are interconnected with all enodebs in the pool area. Resource sharing and service load sharing are realized among MMEs in the pool.Which MME the UE accesses is related to the load balancing strategy of the eNodeB, so the eNodeB needs to perceive the equipment state of the MME.If it is detected that the MME is unavailable, the load balancing strategy needs to be adjusted in time to allocate the new access service request message to other MMEs in normal state.In addition, eNodeB needs to obtain the load weight of MME and select the MME for ue in combination with the load weight.

1.14.2 Dependency

UE	MME	eNodeB
√	√	√

3.1.14.3 Principle description

MME pool Networking:

A group of MMEs can form an MME pool, and the area served by the MME pool is called the MME pool area.From the perspective of TA, if one or more TAS belong to an MME pool, all the business areas of these TAS constitute the MME pool area, and the users in the MME pool area are jointly served by the MMEs in the pool.The function of MME pool has been considered

in the formulation of lte-epc standard, so the ne ID of MME initially contains the information required by the pool.

The networking of MME pool and non pool is not very different in terms of network topology.However, in terms of routing strategy, MME pool requires that all routes between MME and eNodeB in the pool area can be reached.

Load balancing principle:

In the networking of the MME pool, because an eNodeB is connected with multiple MMEs in the MME pool, when the UE in the TA service area initiates a new service, in order for the eNodeB to select a service MME from the pool for the UE according to the principles of load balancing, the MME needs to send the load weight to the eNodeB.

Assuming that the effective user capacity of MME1 is 4 and the effective user capacity of MME2 is 3, eNodeB will access ue to MME1 and MME2 in a ratio of 4:3. The specific distribution effect depends on the implementation mode of eNodeB.MME notifies eNodeB of its own load weight (when s1ap connection is established)

In the MME pool, an eNodeB is connected to multiple MMEs in the MME pool. Therefore, when establishing a dedicated S1 connection, it is necessary to select a service MME for the UE. The selection function here is called "node selection function".ENodeB is selected according to the "load weight" proportion corresponding to each MME, and the load weight value of MME is sent to eNodeB in the pool area through s1ap message.The load weight value of MME is set according to the available capacity of other MME nodes in the pool.The load weight value can be carried to eNodeB through S1 setup response message or MME configuration update message.

3.1.15 Request information correction

3.1.15.1 Definition

When the user requests to access the network, it is necessary to match the signing data.Signing data matching means that during the activation of PDP context / PDN connection, MME will check whether the PDN type, PDN address and APN triplet requested by the user match the triplet signed by the user in HSS according to the matching rules defined in 3GPP TS 23.060 protocol, so as to ensure the legitimacy of user access.In the actual network operation, it is usually caused by the user's wrong setting of mobile phone parameters or repeated signing data, which leads to the failure of signing data matching and the user's request is rejected.In order to reduce the occurrence of such problems, MME provides the function of requesting information correction.The request information correction function corrects the user's request information after the contract data matching fails (matching to multiple groups is also considered as matching failure), selects the PDN type, PDN address and APN triplet actually available to the user, and re matches the contract data, so as to reduce the activation failure caused by wrong Mobile phone parameter setting or repeated contract data.

3.1.15.2 Dependency

MME	HSS
√	√

3.1.15.3 Principle description

When it is found that the request data is inconsistent with the subscription data on HSS, the request data of UE can be corrected to the subscription data on HSS.

3.2 Optional Features

3.2.1 NB-IoT device standard access

3.2.1.1 Definition

This feature supports NB-IoT (Narrow band Internet of things) standard terminals to access MME through NB-IoT RAN to realize mobility management and session management of NB-IoT terminals.

3.2.1.2 Dependency

UE	eNodeB	MME	S-GW	PDN-GW	HSS
√	√	√	√	√	√

3.2.1.3 Principle description

NB-IoT technology has the advantages of low power consumption, wide coverage, low cost and large capacity, so it can be widely used in a variety of vertical industries, such as intelligent meter reading, intelligent lighting, intelligent trash can, intelligent pet health tracking, intelligent agriculture, etc.This feature is not only the basic feature of supporting NB-IoT terminal access to MME, but also the key feature of layout NB-IoT network.

NB-IoT terminal accesses EPC through NB-IoT RANto realize data transmission with IOT platform and application server.NB-IoT RAN adopts independent rat to realize massive connection of NB-IoT.

NB-IoT service can select the following data transmission methods to transmit data packets:

S1-u data transmission mode: service data packets are transmitted to S-GW through s1-u interface.

CP-CIoT data transmission mode: service data packets are carried to MME through NAS signaling and then transmitted to S-GW through s11-u interface. This data transmission mode can improve the efficiency of network transmission of NB-IoT data packets. See WSFD-111407 data transmission characteristics based on signaling surface.

Up ciot data transmission mode: service data packets are transmitted to S-GW through s1-u interface. The characteristic of this data transmission mode is that when the terminal enters idle state, UE, eNodeB and MME save s1ap Association, UE context and bearer context data for connection recovery.When restoring data transmission, there is no need for frequent E-RAB reconstruction. This data transmission method can improve data transmission efficiency.

3.2.2 M2M Long period timer

3.2.2.1 Definition

This feature allocates an extended periodic timer for M2M terminals that are stationary or not moving frequently for a long time, which is used to extend the cycle of terminal location update (TAU) and reduce the TAU frequency, so as to reduce the power consumption of such terminals and the signal load of the network.

3.2.2.2 Dependency

UE	MME	HSS
√	√	√

3.2.2.4 Principle description

1.Check whether the terminal supports long-period timer

If the extended periodic timer bit of the MS network feature support cell in the attach request / TAU request message from the terminal is 1, MME determines that the terminal supports a long-period timer.

2.If the terminal supports a long-period timer, judge whether it is configured locally, whether the terminal carries it in the attach request / TAU request message, or whether the terminal has signed up for a long-period timer, and send it to the terminal through the attach accept / TAU accept message.

• Get long cycle timer from HSS

If the user signs a long-period timer in HSS, MME obtains the signing data from update location answer and insert subscriber data request messages and parses the subscribed periodic RAU TAU timer.

• Locally configured long cycle timer

MME supports local configuration based on APN configuration of extended periodic timer.

• The terminal carries a long-period timer in the attach request / TAU request message

The system supports identifying the T3312 / T3412 extended value cell value from the attach request / TAU request message and sending this cell value to the terminal as a long-period timer.

3.2.3 PSM mode

3.2.3.1 Definition

PSM is the main technology for M2M terminal to save battery power consumption and prolong battery life.The terminal obtains an active timer timer (configurable) from the MME through the NAS message, and starts the timer after the terminal enters the idle state. After the timer expires, if the terminal is still in the idle state, it enters PSM, closes the access layer function to save power, and ignores downlink services and paging.In PSM status, when the terminal itself needs to send data to the M2M server to trigger the service request / control plane service request process, or the periodic TAU timer expires, it will exit PSM.

3.2.3.2 Dependency

UE	MME
√	√

3.2.3.3 Principle description

Terminal enters PSM

The terminal can request the active timer timer through the T3324 cell carried in the attach request / TAU request message. MME supports issuing the active timer according to the T3324 cell carried by the terminal, and also supports issuing the active timer configured locally.

1.Configure an active timer for APN.

2. UE initiates an attach / TAU message with T3324 value ie (active timer) indicating support for PSM mode.

3. MME obtains signing data from HSS, including APN and other signing data.

4. MME obtains the configured active timer according to APN.

5. MME carries T3324 value ie in the attach / TAU accept message, notifies ue of the active timer duration, and UE saves the active timer.

6.The terminal enters idle state. After the active timer expires, if the UE is still in idle state, it enters PSM.

3.2.4 Data transmission of control plane optimization

3.2.4.1 Definition

The service layer data is transmitted between the terminal and MME through NAS messages, and the service layer data is transmitted between MME and S-GW through s11-u interface. There is no need to repeatedly establish and delete air interface wireless data bearer DRB and s1-u connections, which effectively improves the data transmission efficiency and reduces the signaling load on the network.

3.2.4.2 Dependency

UE	eNodeB	MME	S-GW	PDN-GW
√	√	√	√	√

3.2.4.4 Principle description

The small data transmission process based on NAS signaling includes the terminal sending data process mo (mobile originated) and receiving data process MT (mobile terminated),

hereinafter referred to as Mo process and MT process.NAS is the signaling control message between the terminal and MME. in order to meet the demand of IOT terminal for low power consumption, cell processing is added at the NAS level.Under this mechanism, the terminal will indicate the time to release the S1 connection to the MME through the release assistance indication cell, so as to control the occupancy time of the S1 connection and reduce the invalid waiting time.

MO process

• when the idle terminal needs to send uplink data, it will carry the uplink data to the MME through the control plane service request message after the RRC connection is established.When the terminal enters the connected state, it transmits uplink and downlink data through ESM data transport message.

• the MME can indicate when the eNodeB releases the S1 connection according to the release assistance indication cell carried by the terminal in the ESM data transport message.

If ESM data transport message does not carry Release assistance indication cell, then S1 release is triggered by eNodeB triggering simultaneous interpreting with traditional 4G processing.

If the ESM data transport message carries a release assistance indication cell, and the cell indicates "downlink data transmission subsequence to the uplink data transmission is not expected", it indicates that there is no corresponding downlink response for the uplink data. The MME immediately notifies eNodeB to release the S1 connection after transmitting the data to the S-GW.When the cell indicates "downlink data transmission subsequence to the uplink data transmission is expected", it indicates that it needs to wait for the downlink response, and the MME releases the S1 connection after receiving the downlink data.

3.2.5 Non-IP Data transmission process

3.2.5.1 Definition

When the IoT packet is small (10-200 bytes), the UE sends the packet without IP header, and the p-gw proxy the UE's IP and transport layer protocol, which can greatly improve the data transmission efficiency.

3.2.5.2 Dependency

UE	MME
√	√

3.2.5.3 Principle description

Non IP user attach process.

When a non IP user initiates an attachment request, it will carry the non IP ID in the PAA (PDN address allocation) cell and PDN type cell in the attach request / create session request message. MME / S-GW / p-gw determines that the user is a non IP user based on the non IP ID and controls the access of non IP users.

Non IP user data transmission process

The IP address and port number of IOT platform or application server have been configured according to APN granularity on p-gw.

• Uplink data transmission: after receiving the uplink non IP data, the p-gw obtains the destination IP and port number of the IOT platform or application server according to the APN.

The source IP is the IP assigned by the p-gw to the UE. The source port can use the locally configured port to construct the transport layer / IP packet and forward it.

• Downlink data transmission: for the UE downlink transport layer / IP packet received by the p-gw, the source address is the IOT platform or application server address, and the destination address is the UE address assigned by the p-gw. If the p-gw knows that the UE is a non IP Bearer according to the IP index context information, it will delete the transport layer / IP header and forward the non IP data to the UE.

3.2.6 Voice service based on CSFB

3.2.6.1Definition

The voice service based on CSFB (circuit switched fallback) is a voice solution to realize voice call by using the existing Gu (GSM / UMTS) network without introducing IMS (IP multimedia subsystem).In this scheme, when the user carries out voice service, the EPS (evolved packet system) network instructs the user to fall back to the target GSM / UMTS circuit domain (CS) network before initiating voice call.

3.2.6.2 Dependency

UE	MME	eNodeB	HSS	MSC
√	√	√	√	√

3.2.6.3 Principle description

CSFB based voice service provides a circuit domain fallback mechanism to ensure that users are registered in EPS network and traditional circuit domain network at the same time. When users conduct voice service, EPS network instructs users to fall back to the target circuit domain network before initiating voice call.

The network decides to instruct the UE to fall back to the target GSM / UMTS Network, including:

• If the UE and the target network support PS handover, the eNodeB instructs the UE to fall back through the PS handover process.

• If the UE or the target network does not support PS handover, but supports the cell change order (CCO) of different systems and the target system is GERAN, eNodeB obtains the target access network information through the NAcc (network assisted cell change) process and instructs the UE to fall back through CCO.

• If the UE or the target network neither supports PS handover nor cell change instruction (CCO) to different systems of GERAN, eNodeB instructs the UE to fall back through RRC connection release with redirection information.

In order to realize the above functions, MME needs to complete the following processing:

• Calling voice service

• Called voice service

• Circuit domain mobility management

Calling voice service

UE can initiate CSFB voice calling service in RRC (radio resource control) idle state and RRC connected state.

It mainly includes the following service processes:

1. UE initiates the calling voice service.

2. The MME indicates that the eNodeB needs to drop the UE back to the GSM / UMTS Network.

3. ENodeB takes corresponding measures to drop the UE back to the GSM / UMTS Network according to the UE capability.

4. UE initiates calling voice service in GSM / UMTS Network.

Called voice service

The MSC receives the called voice request to the UE and knows which MME the UE is attached to through the existing SGS Association and the EPS attached state of the UE.The MSC sends a message to the MME

When initiating a paging request, MME can know that the current UE is in the idle state or connected state through the MM context of the UE.If the UE is in the idle state, the MME passes through the eNodeB

Paging the UE on the air interface;If the UE is connected, the MME notifies the UE of a call request from the CS domain through a NAS message.

It mainly includes the following service processes:

1. The MSC notifies the MME of the called voice service of the UE.

2. The MME indicates that the eNodeB needs to drop the UE back to the GSM / UMTS Network (if the UE is idle, it needs to first instruct the eNodeB to initiate the paging process and wait for the UE

After re accessing the LTE network, instruct eNodeB to drop the UE back to the GSM / UMTS Network).

3. ENodeB takes corresponding measures to drop the UE back to the GSM / UMTS Network according to the UE capability.

4. UE establishes circuit domain connection in GSM / UMTS Network to complete voice call.

Circuit domain mobility management

In order to provide voice services through CSFB, MME needs to assist MSC to complete mobility management in circuit domain. The specific contents are as follows:

1. UE registers circuit domain services through EPS network.
2. UE completes the notification of circuit domain location change through EPS network.
3. MSc performs circuit domain paging on UE through EPS network.
4. UE cancels the circuit domain service through EPS network.

3.2.7 Realization of short message through SGs interface

3.2.7.1 Definition

The short message is realized based on SGS interface, that is, the user's short message is transmitted between EPS network and traditional circuit domain network to provide short message service without falling back to the target circuit domain network.

3.2.7.2 Dependency

UE	MME	eNodeB	HSS	MSC
√	√	√	√	√

3.2.7.3 Principle description

New interfaces for related concepts:

In the implementation of short message features based on SGS interface, the most important interface is SGs interface, which is the interface between MME and MSC server. It is used to

deal with mobility management and short message service paging processes between EPS and CS domain. These processes are expanded on the basis of the existing Gs interface processes.SGs interface protocol stack is shown in Figure 1.

Figure 1 SGs interface protocol stack

The short message is realized based on SGS interface, that is, the user's short message is transmitted between EPS network and traditional circuit domain network to provide short message service without falling back to the target circuit domain network.In order to realize the above functions, MME needs to complete the following processing:

• Assist MSC to complete CS domain mobility management

• Short message service

Calling short message service

The calling short message process initiated by the user can be divided into idle state and connected state.

Called short message service

The short message center initiates the called short message process, which is divided into idle state and connected state according to the state of UE.

System implementation

• Short message service:

When there is a short message service, MME acts as an intermediate forwarding node to complete the forwarding of UE and MSc messages and assist UE and MSC to complete the short message function.

The main difference between the short message function and the voice function is that the short message function does not need to drop the UE back to the GERAN/ UTRANnetwork, and directly uses the E_UTRAN network to provide the short message service for the UE.

• Assist MSC to complete CS domain mobility management:

In order to implement short message service based on SGS interface, MME needs to assist MSC to complete mobility management in circuit domain. The specific contents are as follows:

UE registers circuit domain services through EPS network.

UE completes the notification of circuit domain location change through EPS network.

The MSC performs circuit domain paging on the UE through the EPS network.

UE cancels the circuit domain service through EPS network.

3.2.8 5G NSA(Opt.3) networking

3.2.8.1 Definition

5G NSA Option3 / 3a / 3x networking refers to a networking solution to smoothly evolve the EPC network to 5g NSA network architecture by upgrading EPC core network equipment and

deploying NR NodeB (gNodebs) in LTE wireless network.By shunting user plane data to gNodebs, the high bandwidth processing capability of gNodebs is used to provide users with high-speed broadband wireless services.

3.2.8.2 Dependency

UE	MME	eNodeB	HSS	MSC
√	√	√	√	√

3.2.8.3 Principle description

5G NSA (opt. 3) networking introduction

For the three networking solutions of 5G NSA (opt. 3), the control plane signaling is sent through LTE eNodeB;User plane data is shunted to LTE eNodeB and gNodebs and sent to UE. According to different shunting methods, it can be divided into three forms: Option3, Option3a and Option3x.

Characteristic realization principle

In the three networking scenarios, eNodeB determines whether to divert UE user plane data according to the current air interface environment, service type (such as volte voice and high bandwidth service).The user plane data diversion process under the three networking scenarios is as follows:

•Option 3

ENodeB directly establishes the user plane transmission path to gNodebs to divert user data (without the participation of the core network).

•Option 3a

ENodeB initiates the e-rab modification indication process to trigger gNodebs and S-GW to establish s1-u transmission path, switch the bearer to be shunted to the new s1-u, and dispose the flow to eNodeB and gNodebs in S-GW.

•Option 3x

The principle of option 3x user plane data shunting in S-GW is consistent with the principle of option 3A above.By initiating the e-rab modification indication process, eNodeB triggers gNodebs and S-GW to establish s1-u transmission path, switches the bearer to be shunted to the new s1-u, and the user plane data flows to eNodeB and gNodebs at the disposal of S-GW. In addition, in the option 3x networking scenario, the gNodebs can also divert the user plane data to the eNodeB as needed (for example, when the gNodebss bandwidth is about to reach the bottleneck).If shunting is required, the gNodebss directly establishes a user plane transmission path to the eNodeB for user plane data shunting (this step does not require the participation of the core network).

The detailed steps of e-rab modification indication process are as follows:

1. After eNodeB judges that it is necessary to create a new NR bearer for the user according to the current user service type, air interface status and other information, it sends an e-rab modification indication message to MME to point the bearer IP address to be shunted to gNodebs.

2. MME sends a modify bearer request message (carrying the gNodebs IP address information) to the S-GW to notify the S-GW to switch the user plane transmission path from eNodeB to gNodebs.

3. After the S-GW updates the IP address information of the corresponding bearer, it returns the update result to the MME through the modify bearer response message.

4. MME notifies eNodeB of the update result of e-rab modification confirm message.

4 Operation and Maintenance

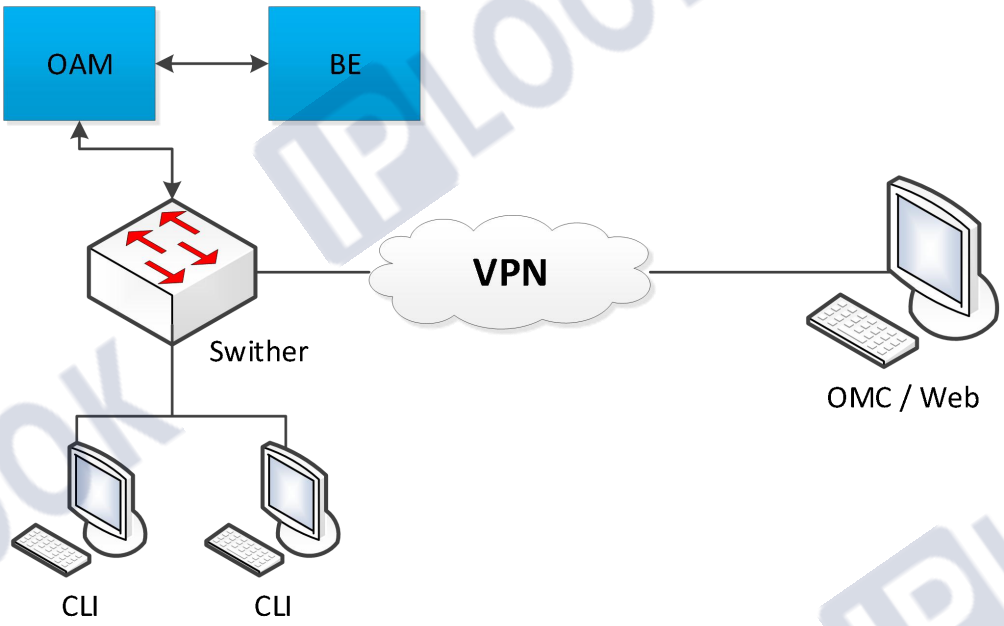
The IPLOOK provides a perfect operation and maintenance function and supports the unified EMS to implement daily maintenance and management.

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.

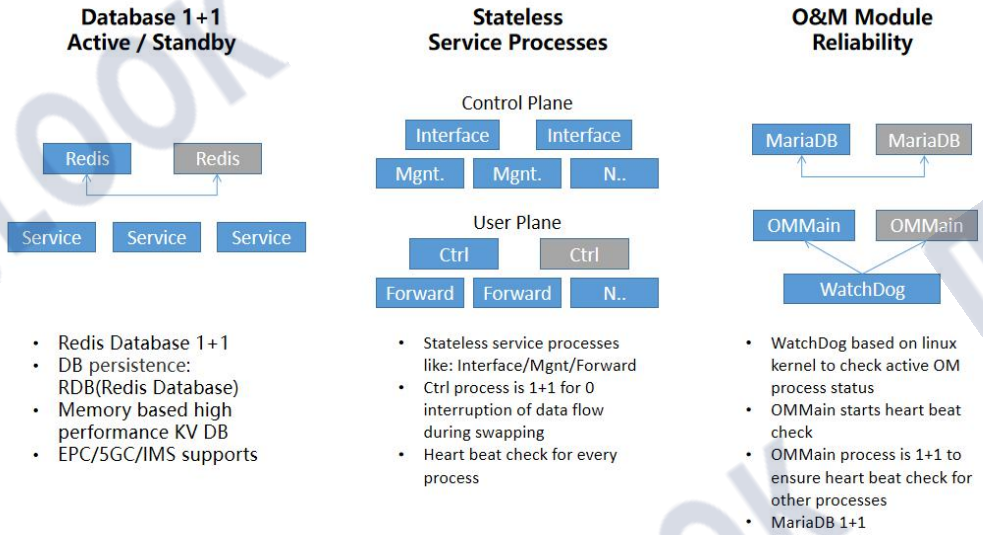
Figure 3 shows the network architecture



5 Reliability design

5.1 Software Reliability

Figure 4 software reliability



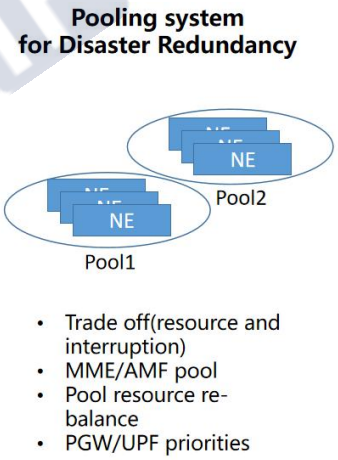
IPLOOK uses open-source database Redis in core network system, it is a memory-based Key-Value database, has great performance, and deployed as an active/standby redundancy mode. All stateful contexts of core network system are stored in this database. Other service processes are stateless such as interface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

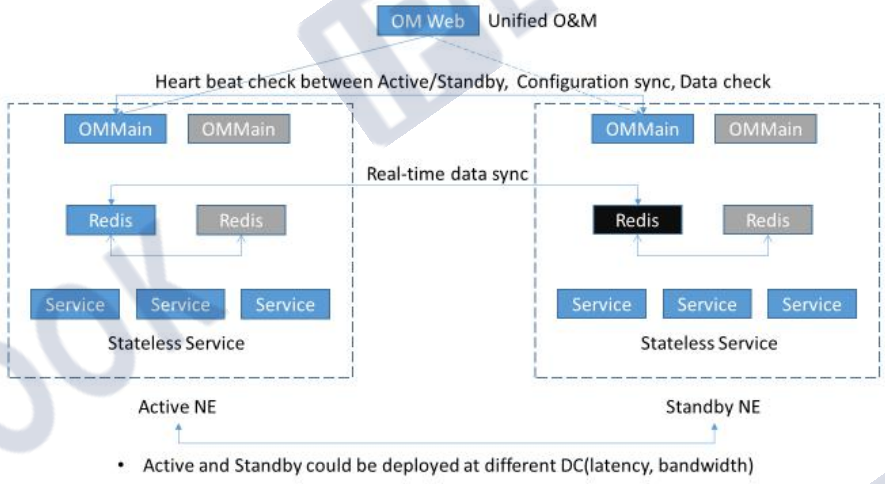
5.1 Network element Reliability

Figure 6 MME pool



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 Interfaces and Protocols

The related 3GPP interfaces, protocols and functions of IPLOOK MME are listed in Table 16.

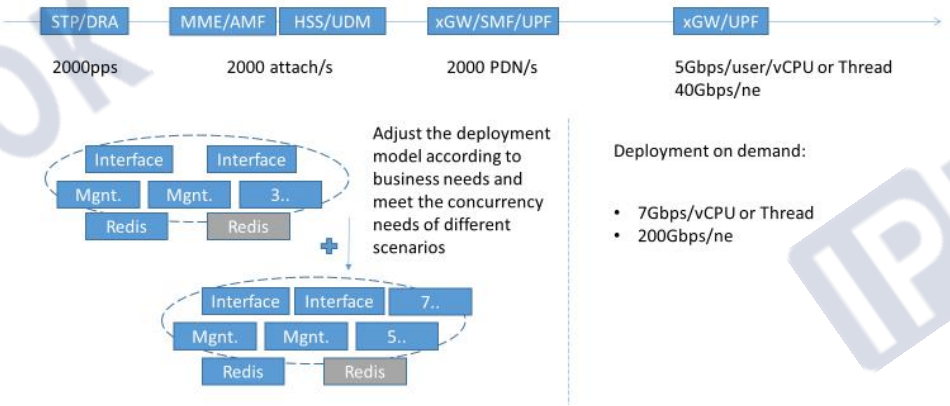
Table 4 3GPP Related Interfaces and Protocols of IPLOOK MME

Interface	Description	Protocol	Standard
S1-MME	Interface between E-UTRAN and MME.	S1AP	3GPP TS 36.413
S6a	Interface between MME and HSS.	Diameter	3GPP TS 29.272
S3/S4	Implementing mobility management between SGSNs with GTPv2 in EPC network	GTPv2/ GTP v1	3GPP TS 29.274 3GPP TS 29.281
S10	Interface between MME and MME.	GTPv2	3GPP TS 29.274
S11	Interface between MME and SGW.	GTPv2	3GPP TS 29.274
S13	Interface between MME and EIR.	Diameter	3GPP TS 29.272
SGs	Interface between MME and MSC for CSFB or SMS.	SGsAP	3GPP TS 29.118

7 Dimension

7.1 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.

7.2 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)
User	<200k		200k-500k		500k-1M		1M-2M
OMC	6T,16GB		12T,32GB		24T,64GB		48T,128GB

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

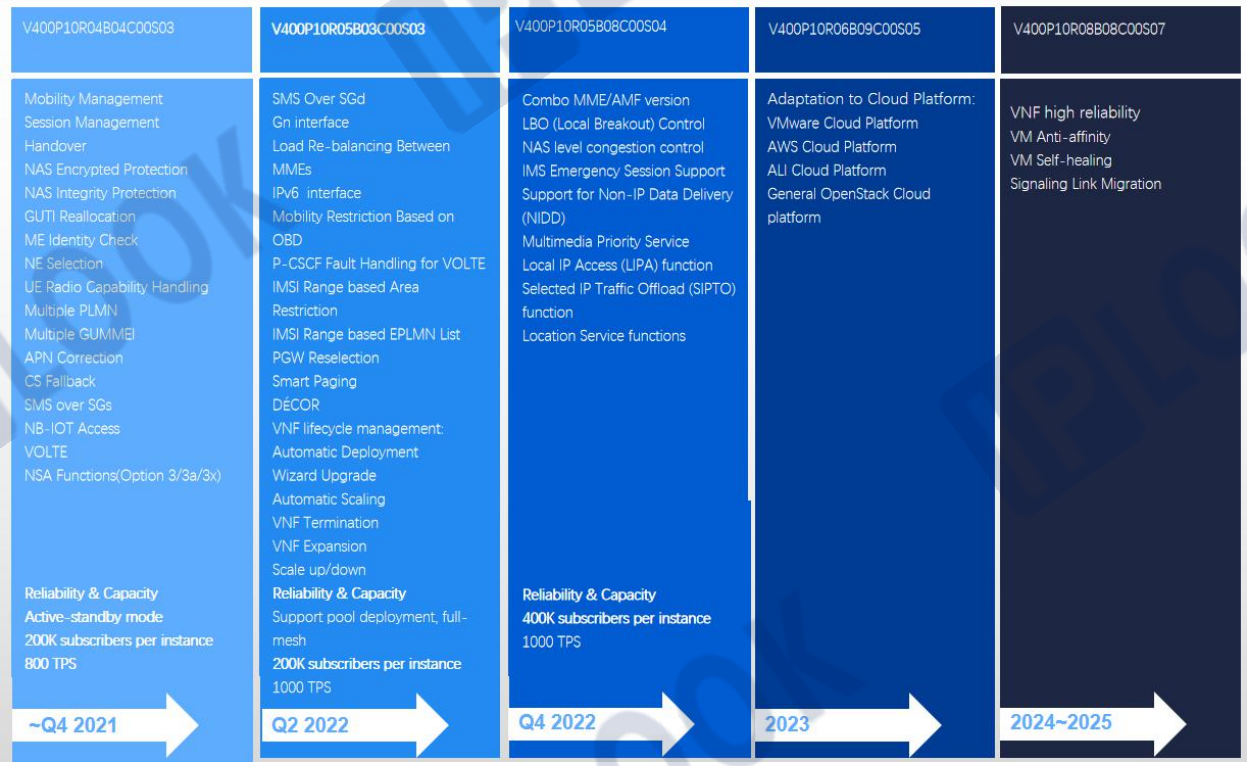
AMF/MME/SMF means they have same dimension methodologies, share same hardware resource requirements.

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)).

8 Roadmap


V400P10R04B04C00S03
Mobility Management
Session Management
Handover
NAS Encrypted Protection
NAS Integrity Protection
GUTI Reallocation
ME Identity Check
NE Selection
UE Radio Capability Handling
Multiple PLMN
Multiple GUMMEI
APN Correction
CS Fallback
SMS over SGs
NB-IOT Access
VOLTE
NSA Functions(Option 3/3a/3x)
Reliability & Capacity
Active-standby mode
200K subscribers per instance
800 TPS
~Q4 2021
V400P10R05B03C00S03
SMS Over SGd
Gn interface
Load Re-balancing Between MMEs
IPv6 interface
Mobility Restriction Based on OBD
P-CSCF Fault Handling for VOLTE
IMSI Range based Area Restriction
IMSI Range based EPLMN List
PGW Reselection
Smart Paging
DECOR
VNF lifecycle management:
Automatic Deployment
Wizard Upgrade
Automatic Scaling
VNF Termination
VNF Expansion
Scale up/down
Reliability & Capacity
Support pool deployment, full-mesh
200K subscribers per instance
1000 TPS
Q2 2022
V400P10R05B08C00S04
Combo MME/AMF version
LBO (Local Breakout) Control
NAS level congestion control
IMS Emergency Session Support
Support for Non-IP Data Delivery (NIDD)
Multimedia Priority Service
Local IP Access (LIPA) function
Selected IP Traffic Offload (SIPTO) function
Location Service functions
Reliability & Capacity
400K subscribers per instance
1000 TPS
Q4 2022
V400P10R06B09C00S05
Adaptation to Cloud Platform:
VMware Cloud Platform
AWS Cloud Platform
ALI Cloud Platform
General OpenStack Cloud platform
2023
V400P10R08B08C00S07
VNF high reliability
VM Anti-affinity
VM Self-healing
Signaling Link Migration
2024~2025

9 Acronyms and Abbreviations

Table 6 Acronyms and Abbreviations

Name	Explanation
2G	Second Generation
3G	the third Generation mobile communications
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
ATM	Asynchronous Transfer Mode
AUC	Authentication Center
AVP	Attribute Value Pair
BOSS	Business Operator and Supporting System
BSC	Base Station Controller
CAMEL	Customized Application for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CAPEX	Capital Expenditure
CBC	Content Based Charging
CCG	Content based Charging Gateway
CG	Charge Gateway
CN	Core Network
COTS	Commercial Off The Shelf
CS	Circuit Service
CSCF	Call Session Control Function
EIR	Equipment Identity Register
EMS	Element Management System

EPS	Evolved Packet System
EUTRAN	Evolved Universal Terrestrial Radio Access Network
FCAPS	Fault, Configuration, Accounting , Performance, Security
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscriber Server
IM-SSF	IMS – Service Switch Function
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IOT	Inter-Operation Test
ITU	International Telecom Union
LAI	Location Area Identity
MAP	Mobile Application Part
MME	Mobility Management Entity
MMS	Multimedia Message Services
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	MS ISDN
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NAT	Network Address Translation

NE	Network element
NFV	Network Function Virtualization
NM	Network Management
NRI	Network Resource Identifier
OMC	Operation and Maintenance Center
OCS	Online Charging System
OPEX	Operating Expense
PDP	Packet Data Protoco1
PLMN	Public Land Mobile Network
POS	Packet Over SONET/SDH
PS	Packet Service
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RANAP	Radio Access Network Application Part
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRU	Remote Radio Unit
SCTP	Stream Control Transmission Protocol
SGW	Serving Gateway
SGSN	Serving GPRS Support Node
SIGTRAN	Signaling Transport
SMS	Short Message Service
SMSC	Short Message Service Center

SMTP	Simple Mail Transfer Protocol
SS7	Signaling System Number 7
TCP/IP	Transmission Control Protocol/Internet Protocol
TECS	Tulip Elastic Computing System
UMTS	Universal mobile telecommunication system