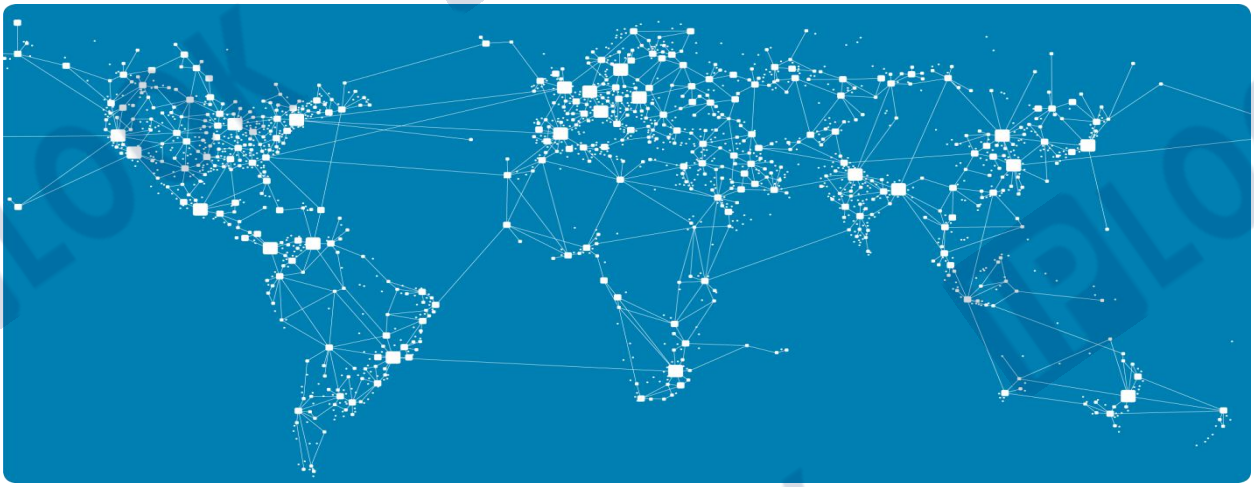
IPLOOK HSS/HLR PRODUCT DESCRIPTION

IPLOOK Technologies

www.iplook.com

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

IPLOOK HSS/HLR Product Information



IPLOOK Technologies / IPLOOK Technologies Co., Limited

Date (2022-01-24)

IPLOOK Tecnologies 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		Cole	Li	23-07-18
1.2	Done	Support Roaming restrictions in user area	Cole	Li	06-02-20
1.3	Done	Add General configuration APN function	Ben	James	9-05-21
1.4	Done	Add Multi HPLMN function	Ben	James	11-10-21

Table of Contents

1 Introduction

1.1 HSS overview

EPC refers to a core network architecture that supports LTE access networks. IPLOOK provides Long Term Evolution/Evolved Packet Core (LTC/EPC).Conform to the 3GPP R10 29.272 and 29.002 protocol specifications, IPLOOK HSS / HLR (Referred to as HSS / HLR) implements HSS and HLR functions in the SAE network architecture which stores all the information related to services in the SAE network, and provides subscriber information management and User location management.

The HSS / HLR is logically divided into two parts: BE (back end) and FE (front end), which achieves the separation of user data and logic processing of service.

The operator signs LTE mobility management for users. The signed services include PDN data and QoS data, which are stored in HSS. In the process of location update or user data insertion, HSS sends the service data to MME / S4-SGSN / 3GPPAAA.

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

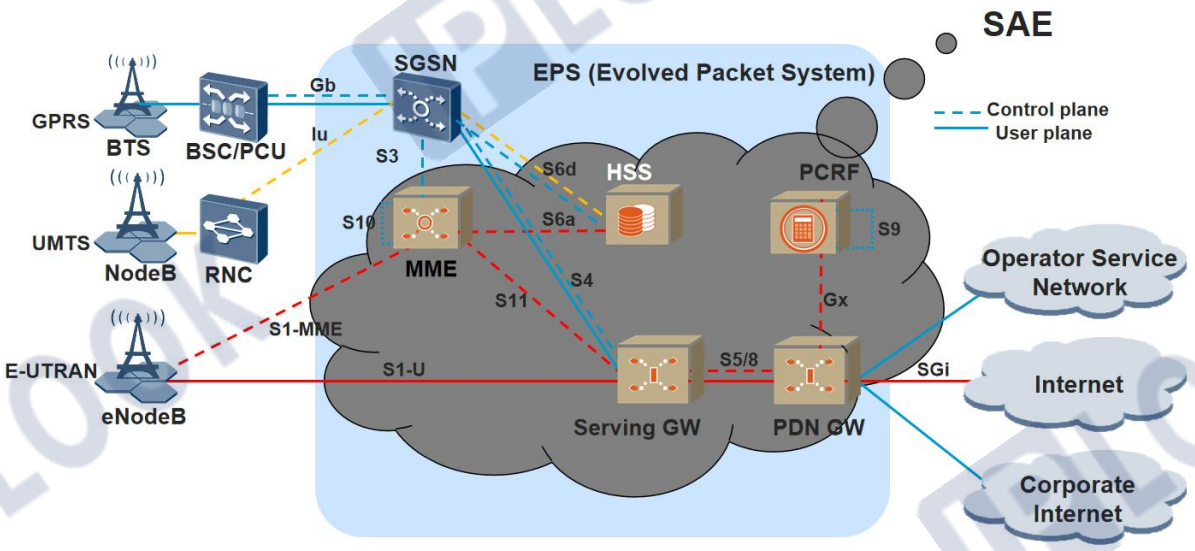


Figure 1 Schematic Diagram

IPLOOK's HSS 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.
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

Name	Function
	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 HSS 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 HSS hardware resources are virtualized to many VMs. When the IPLOOK HSS needs to increase its processing capability, more VMs can be installed.
The IPLOOK HSS 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 HSS 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 HSS system provides a series of products and open standard interfaces.
The IPLOOK HSS 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 HSS performs daily maintenance and management through the unified EMS .

The IPLOOK HSS 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 HSS 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.

2 System architecture

2.1 IPLOOK HSS in the NFVI

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

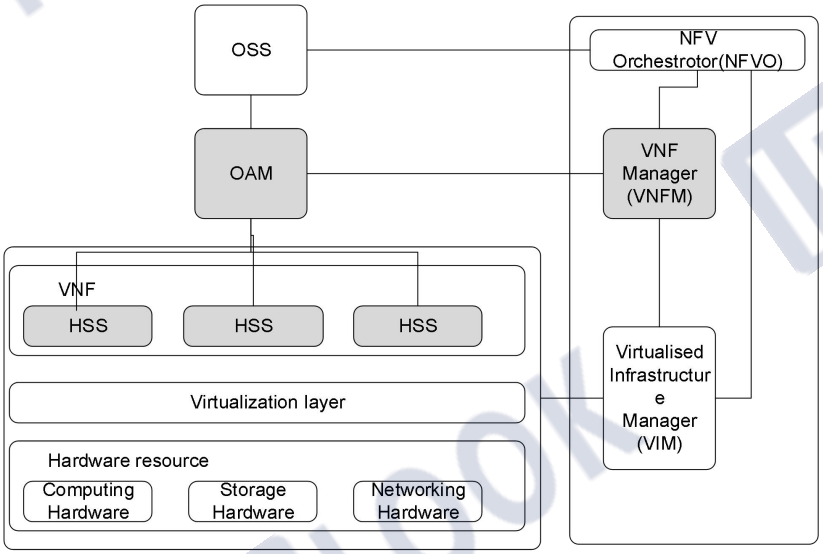


Figure 2 IPLOOK HSS System Architecture

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

Table 2 IPLOOK HSS 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 HSS.
NFVI	Network functions virtualization infrastructure, which refers to physical resources.

Node	Description
	The NFVI is provided and managed by the cloud platform.
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 HSS 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 LTE mobility management

3.1.1 Definition

EPS (Evolved Packet System) is the subsequent evolution technology of 3G, which provides users with packet data services with higher rate and lower delay.Support voice, video, data file exchange and other services.

EPS has the following characteristics:

1.The spectrum efficiency is higher, and the advanced OFDM (orthogonal frequency division multiplexing) and MIMO (multiple input multiple output) technologies are adopted.

2.The network is more flat, the signaling plane is completely separated from the user plane, supports end-to-end QoS guarantee, and can perform QoS control on each bearer.

3.Support users' roaming and switching between different access networks, and maintain business continuity.

3.1.2 Dependency

UE	MME	HSS
√	√	√

3.1.3 Principle description

The operator signs LTE mobility management for users. The signed services include PDN data and QoS data, which are stored in HSS. In the process of location update or user data insertion, HSS sends the service data to MME / S4-SGSN / 3GPPAAA.

The following is the E-UTRAN initial attach process for mobility management:

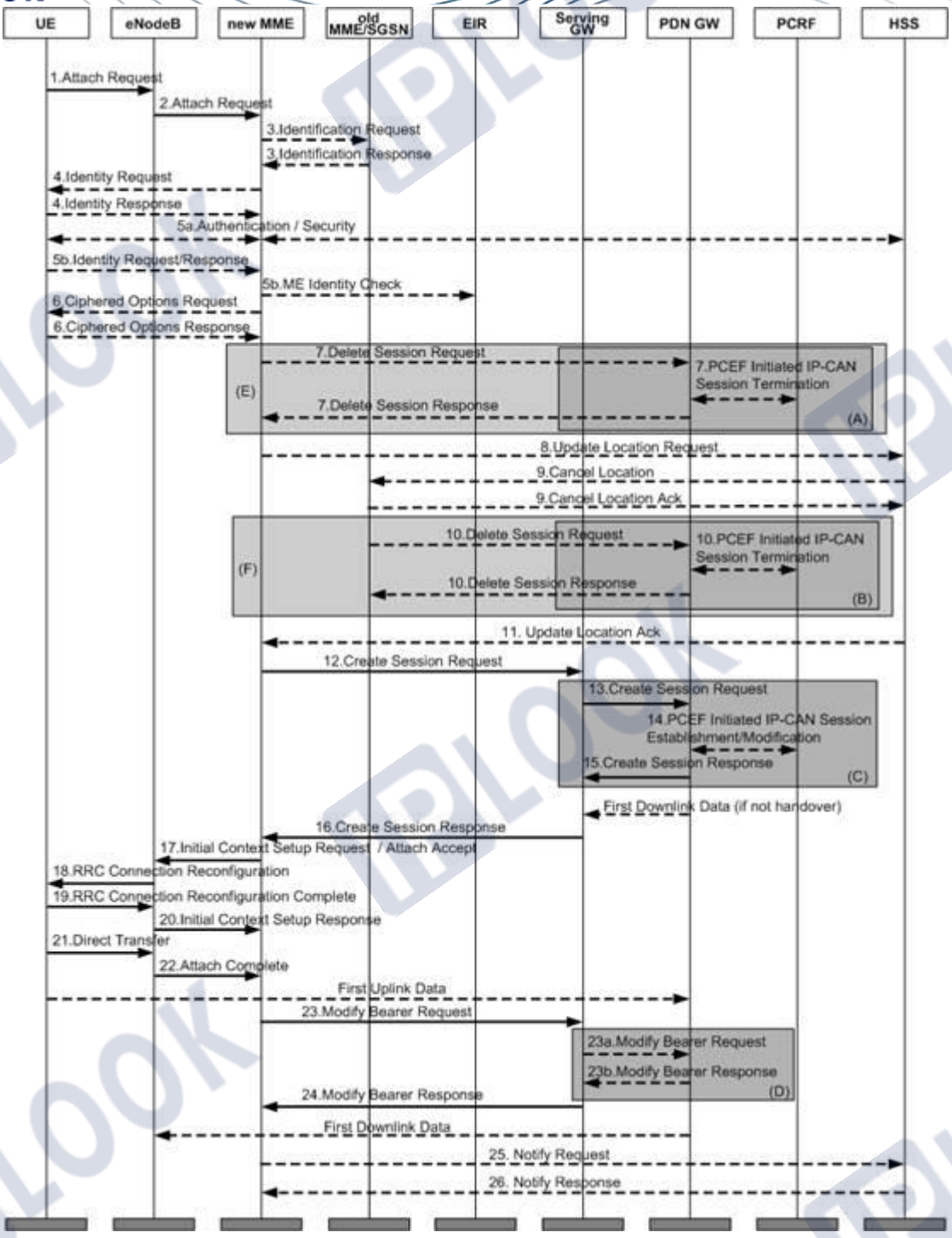


Figure 3 IPLOOK HSS System initial attachment process of E-UTRAN

1. The UE initiates an initial attachment request to the eNodeB.

2. ENodeB enables the MME selection process, selects an appropriate MME, and sends an attachment request to this MME.

3. If there is a GUTI ID on the UE and it is found that the current service MME has changed compared with the last time, the current MME deduces the old MME / SGSN address according to the GUTI and sends an "identity request" message to it to obtain the IMSI and MME context of the current UE.

4. If the old and new MMEs do not know the user's IMSI, the MME directly initiates an "identity request" to the UE.

5. a. If the security context or integrity protection of the UE is missing in the network, the authentication and NAS security establishment processes are performed.

b. The UE responds the identity identification to the MME in encrypted form, and performs IMEI legitimacy check if necessary.

6.If the "encryption option" transmission flag bit is carried in the initial attachment request, the MME obtains the "encryption option" from the UE.

7. MME deletes the remaining bearer of this ue on MME.

8. MME initiates a location update request to HSS.

9. HSS sends a location deletion request to the old MME / SGSN.

10.The old MME deletes the bearer activated for this ue on it.

11. HSS returns the location update response to MME, which carries the user's signing data.

12.If the UE carries an APN, the APN is used as the default bearer; otherwise, the contracted APN is used as the default bearer.MME starts the "S-GW selection process" and selects an appropriate S-GW, so that APN initiates a "session establishment" request to S-GW.

13. The S-GW creates this session and initiates a "session establishment" request to the PDN-GW indicated by the MME.

14. The PDN-GW initiates the IP-CAN session establishment process to the PCRF, thereby obtaining the default PCC rules of the UE.

15. PDN-GW creates this session and generates a billing ID.After the session is established, the PDN-GW can route the user's data packets in the S-GW and data network and start billing.After that, PDN-GW sends a "establish session" response to S-GW.

16. The S-GW sends a "establish session" response to MME.

17. MME returns the "attach accept" response message to eNode.Meanwhile, MME sends an "initial context establishment" request to eNode.

18. The eNodeB initiates a "RRC link reconfiguration" request to the UE, including an attachment confirmation response message.

19. The UE returns the "RRC link reconfiguration complete" response message to eNode.

20. ENodeB sends "initial context response" message to MME.

21. The UE sends the "direct transfer" message to the eNodeB, including the "attachment completion" message.

22. ENodeB forwards the attach complete message to MME.

23.After receiving the "attachment completion" message and the "initial context response" message, MME sends the "modify bearer request" message to S-GW.

a. If the message received by the S-GW contains a handover instruction, a "modify bearer request" message is sent to the PDN-GW, instructing it to iMMEdiately implement the handover from non-3GPP access to 3GPP access, and route subsequent data packets to the S-GW.

b. PDN-GW sends "modify bearing response" message to S-GW.

24. s-gw returns the "modify bearing response" message to MME.

25. MME reports the currently selected PDN-GW identity to HSS for subsequent application between and non-3GPP access.

26. HSS stores the PDN-GW identity in the database and returns a response message to MME.

The following is the tracking area update process of mobility management:

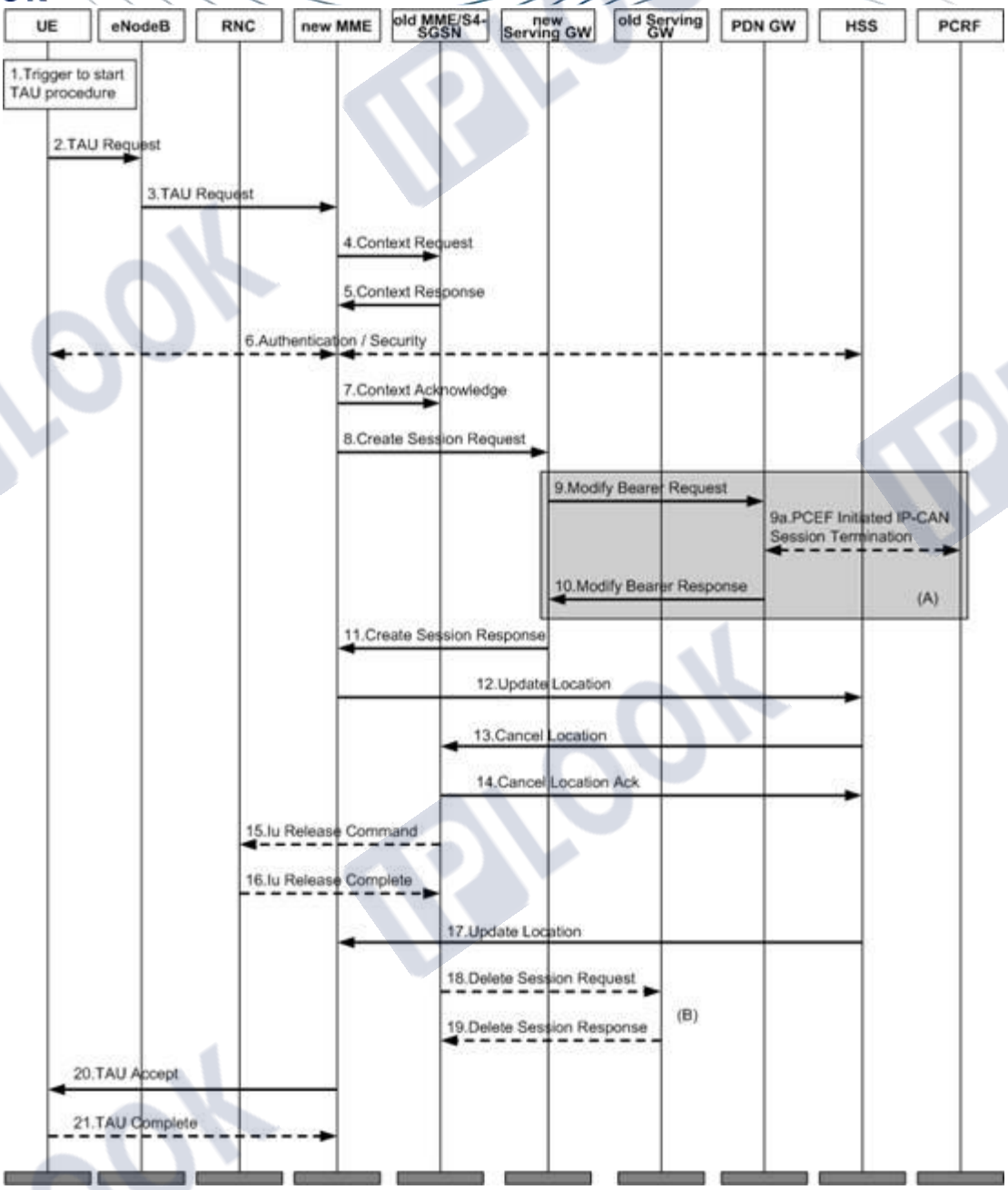


Figure 4 IPLOOK HSS System update process of tracking area

1. An event has occurred that caused the initial attachment (for example, entering a new tracking area).

2. The UE initiates a "tau request" to the eNode.

3. ENodeB identifies the current service MME according to the information carried in the request message and forwards the "tau request" to the MME.

4. MME derives the MME / S4-SGSN address of the previous service according to GUTI and sends a "context request" to it to obtain user information.

5. The old MME / S4-SGSN sends the relevant information of the current user to the new MME.

6. If the integrity check of the TAU request message fails, the authentication process will be initiated.

7. The new MME sends a "context confirmation message" to the old MME / S4-SGSN, and the old MME / S4-SGSN selects a new S-GW for the UE according to this message.Meanwhile, the old MME / S4-SGSN marks its own UE context as invalid.

8. MME starts the "S-GW selection process" and selects an appropriate S-GW, so that APN initiates a "session establishment" request to S-GW.

9. The S-GW creates this session and sends a "modify bearer request" to the PDN-GW indicated by the MME.

a. The PDN-GW initiates the IP-CAN session establishment process to the PCRF, thereby obtaining the default PCC rules of the UE.

10. PDN-GW updates its own session context and sends a "establish session" response to S-GW.

11. The S-GW updates its session context and sends a "establish session" response to MME.And transmit the uplink data packet from eNodeB to PDN-GW.

12. MME sends location update message to HSS and supports location update between MMES.

13. HSS sends cancellation location registration to the old MME.

14. The old MME deletes its own MM context and sends a "cancel location registration response" message to HSS.

15. The old S4-SGSN receives the "context confirmation message" and returns the "IU release" message to the RNC.

16. RNC returns the response message "IU release completed".

17. HSS sends a location update response message to MME.

18. The old MME / S4-SGSN sends a "delete session request" to the old S-GW and instructs the S-GW not to initiate the session deletion process to the PDN-GW.

19. The S-GW returns the "delete session response" message.And discard all data packets cached for the UE.

20. The MME returns a TAU complete message to the UE.

21. If the "TAU complete" message contains GUTI, the UE returns the "TAU complete" response message to the MME.

The following is the E-UTRAN detachment process initiated by UE:

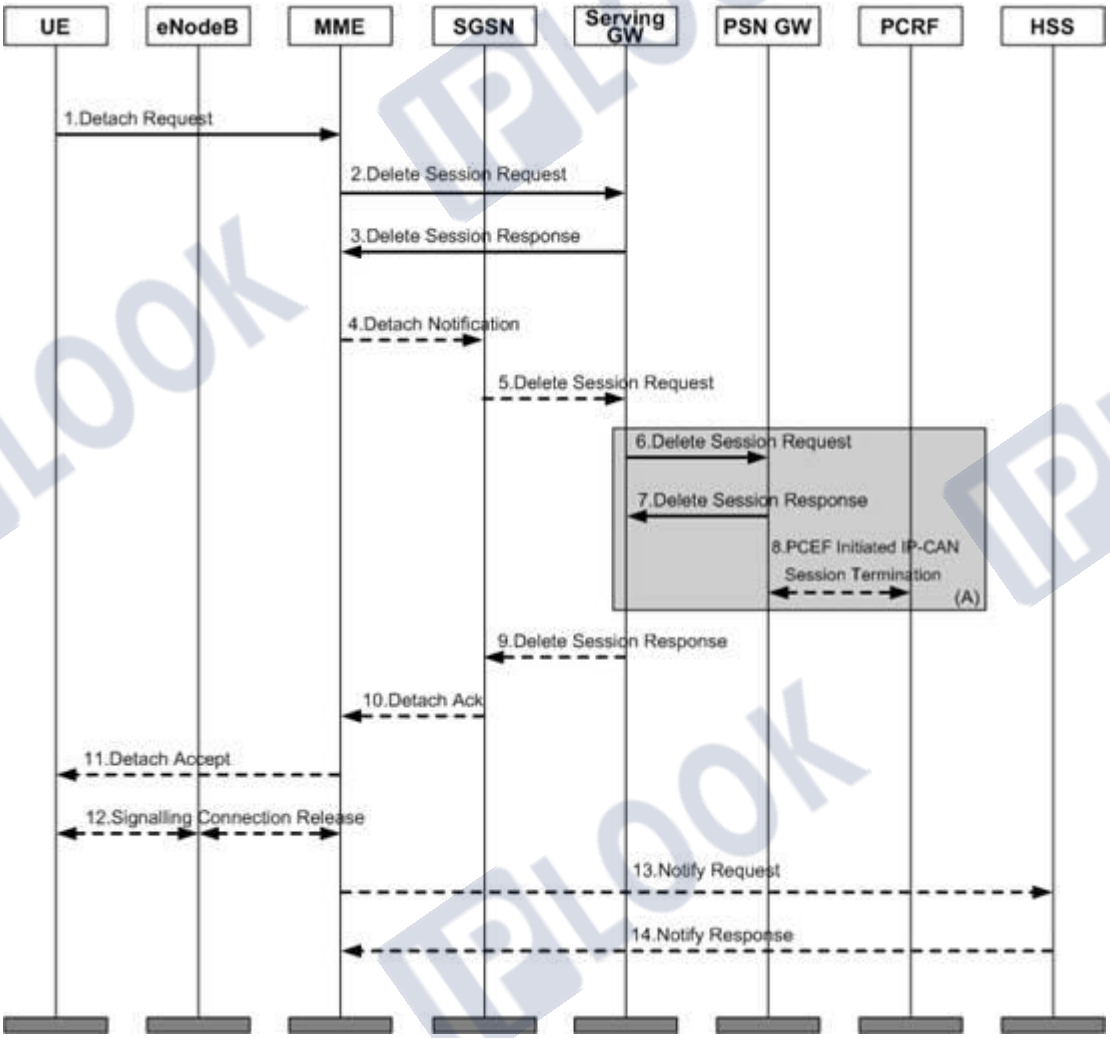


Figure 5 IPLOOK HSS System E-UTRAN detachment process initiated by UE

1. The UE sends a "detachment request" to the MME.

2. The MME sends a "delete session request" to the S-GW, and the S-GW deactivates all bearers of the UE.

3. The S-GW returns the "delete session response" message.

4. If ISR is activated, MME sends a "detachment indication" message to its associated SGSN and indicates complete detachment.

5. The SGSN sends a "delete session request" to the S-GW, and the S-GW deactivates all PDP contexts of the UE.

6. The S-GW deactivates the IDR and sends a "delete session request" to the PDN-GW.

7. PDN-GW returns "delete session response" to S-GW.

8. The PDN-GW sends the "IP-CAN session termination" process to the PCRF to notify it that the EPS bearer has been released.

9. PDN-GW returns "delete session response" to SGSN.

10. SGSN returns the "detachment confirmation message" to MME.

11. MME returns the "detachment confirmation" message to UE.

12. MME sends "S1 release" command to eNodeB.

13. After receiving the "delete session response" message sent by S-GW, MME sends a "notification request" to HSS to instruct HSS to delete the PDN-GW identity corresponding to the saved APN.

The following is the process of inserting user data:

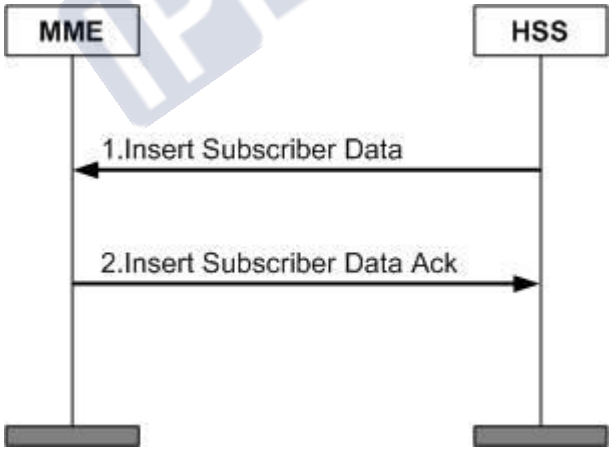


Figure 6 IPLOOK HSS System process of inserting user data

1. If the user's subscription data changes, HSS sends a "insert user data" request to MME.

2. MME updates its saved user subscription data and sends the "insert user data response" message.MME performs corresponding operations according to the new data issued by HSS. For example, if the new data does not allow users to roam in the current network, MME initiates the "detachment" process.

3.2 EAP-AKA authentication function

3.2.1 Definition

Authentication refers to the process of network checking the legitimacy of users. It is a part of mobile network security management. It is used to realize the confidentiality and data integrity of mobile network.EPS-AKA (evolved packet system authentication and key agreement) authentication refers to the authentication of LTE network.

3.2.2 Dependency

UE	MME	HSS
√	√	√

3.2.3 Principle description

EPS-AKA authentication occurs when EPS users access the LTE network.

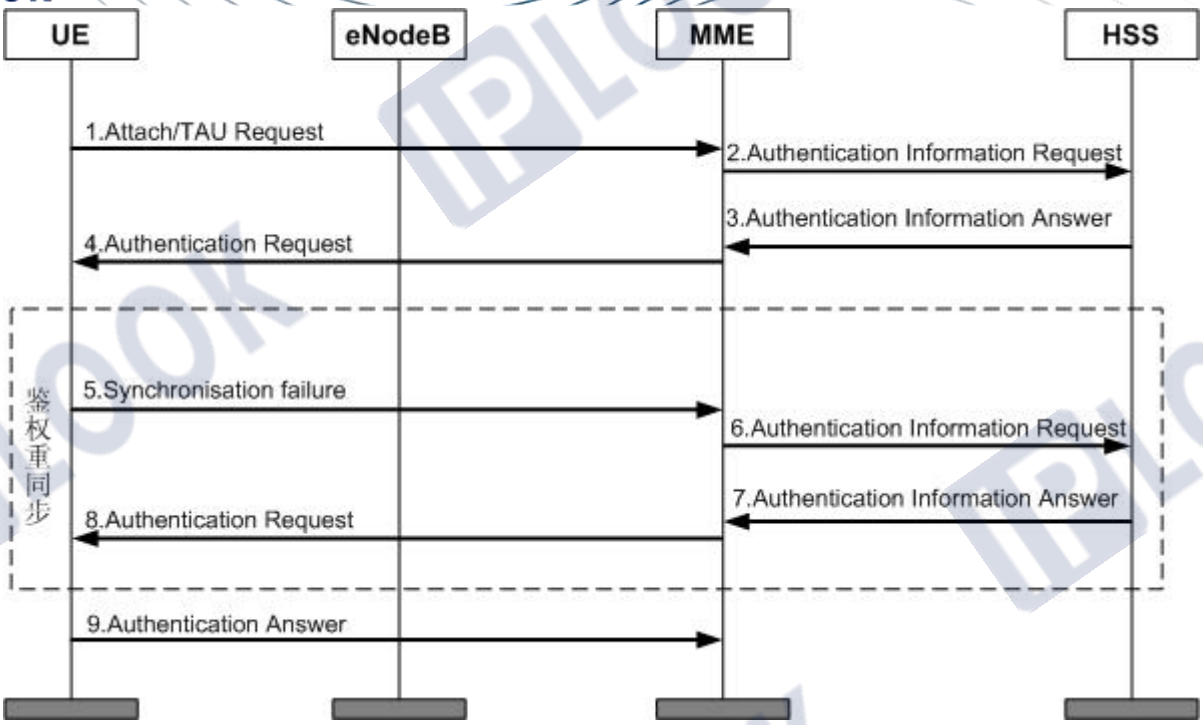


Figure 7 IPLOOK HSS System EPS-AKA authentication process

The authentication process is as follows:

1. The UE sends an attach request message to the eNodeB to attach to the LTE / SAE network or sends a tau request message to update the location;ENodeB sends the attach request message or tau (tracking area update) request message sent by UE to MME in advance.

2. MME sends an authentication information request message to HSS to initiate an authentication vector request, including IMSI, service network ID Sn ID (such as MCC + MNC) and network access type (such as E-UTRAN).

3. After receiving the message, HSS starts to calculate the EPS authentication vector, which calculates the root key K in the EPS authentication vector according to the service network ID and CK / IK_ASME and returned to MME through authentication information answer message, which carries a complete set of authentication vector quadruplets {RAND, AUTN, XRES,

K_ASME}. If multiple sets of authentication vectors need to be returned, they are sorted according to the sequence number Sqn (sequence number);Since the access network type is E-UTRAN, HSS sets the "separator" in the AMF field in autn to 1 to inform ue that the authentication vector is only used for AKA processes of LTE / SAE. If the "separator" is set to 0, the vector is only used for non LTE / SAE contexts (such as GSM and UMTS).

4. MME selects a set of authentication vectors from the database according to the first in first out criterion for this AKA process, and saves XRES and K_ASME in the authentication vector,sends an authentication request message to the UE, and the UE transmits the RANDom number RAND and authentication token autn in the authentication vector AV (authentication vector) contained in the message to the USIM card. In addition, the message also assigned K_ASME's identification KSI (key set identifier) to UE.

5. After receiving the AUTN and RAND from the network side, USIM calculates the SQN and compares it with the maximum Sqn number SQNMS stored by itself to ensure that the new SQN must be greater than the SQNMS, so as to ensure that the received authentication vector is a new and unused authentication group.When the received SQN is less than or equal to the SQNMS saved by USIM, it sends a synchronization failure message to MME, takes the SQNMS saved by itself as the input parameter, calculates the AUTS parameter （AUTS = SQNMS ⊕f5*K（RAND） || f1*K（SQNMS || RAND || AMF）），and initiates the authentication weight synchronization process to the network side.

6. After receiving the synchronization failure message sent by UE, MME sends authentication information request message to HSS again;The Requested-EUTRAN-Authentication-Info parameter contains Re-Synchronization-Info AVP, which is composed of RAND and AUTS.

7. HSS parses the SQNMS saved by USIM from the AUTS and verifies the AUTS. If the verification is passed, the SQNHE saved in SAE-HSS and tracking the UE is set as the SQNMS of the UE, and based on this, a new SQN and authentication vector are generated and returned to MME, while ensuring that the new SQN can be accepted by USIM.

8. MME saves XRES and K_ASME in the authentication vector, sends the authentication request message to the UE again, and the UE transmits the RANDom number RAND and authentication token AUTN in the authentication vector AV (authentication vector) contained in the message to the USIM card. In addition, the message also assigns K_ASME's identification KSI (key set identifier) of to UE.

9.When USIM confirms that the received authentication group is an unused authentication group, it calculates whether the autn is correct according to the random number RAND, so as to authenticate the network. Then it calculates the RES according to the random number RAND and AUTN, and sends it to MME in the response message authentication answer. If the MME checks if RES is consistent with XRES, the network authenticates the UE.In addition, the USIM card also calculates CK / IK through AUTN and RAND and transmits it to the UE. The UE calculates K_ASME in combination with CK / IK and service network ID and store.

3.3 Roaming local breakout function

3.3.1 Definition

The roaming local breakout function allows users to access the network directly using the PDN GW (packet data network gateway) of the roaming place without detouring back to the home place for network access.

3.3.2 Dependency

UE	MME	HSS
√	√	√

3.3.3 Principle description

The PDN GW used by the user to access the network is mainly selected by MME / S4 SGSN / AAA, and HSS is only responsible for the storage and distribution of signing information.

1. By signing this feature, users can access the network using PDN GW in roaming and home places.

2. Without signing this feature, users can only access the network using the PDN GW of their home location.

The effectiveness of this feature needs to be determined by the local breakout attribute based on APN level and the local breakout attribute based on UE PLMN level. The relationship between the two is as follows:

1. If the user does not sign up for the UE PLMN template, the local breakout attribute of APN level shall prevail.

2. If the user signs up for the UE PLMN template, but the template does not define the PLMN ID of the current user, the local breakout attribute of APN level shall prevail.

3. If the user signs up for the UE PLMN template, the template contains the current PLMN ID of the user and defines the local breakout attribute of the UE PLMN level, that is, the local breakout function is allowed only when the two local breakout attributes are set to allow the user to access the PDP / PDN network from the VPLMN.

Business process:

1. If the user does not sign up for roaming local breakout on the network, HSS will send the relevant user signing data to MME / S4 SGSN / AAA through the location update process.

2. If the user signs up / goes to sign up for roaming local breakout on the network, HSS will notify MME / S4 SGSN / AAA to update the relevant user signing data through the independent user data insertion process.

Distribute relevant user signing data through the location update process:

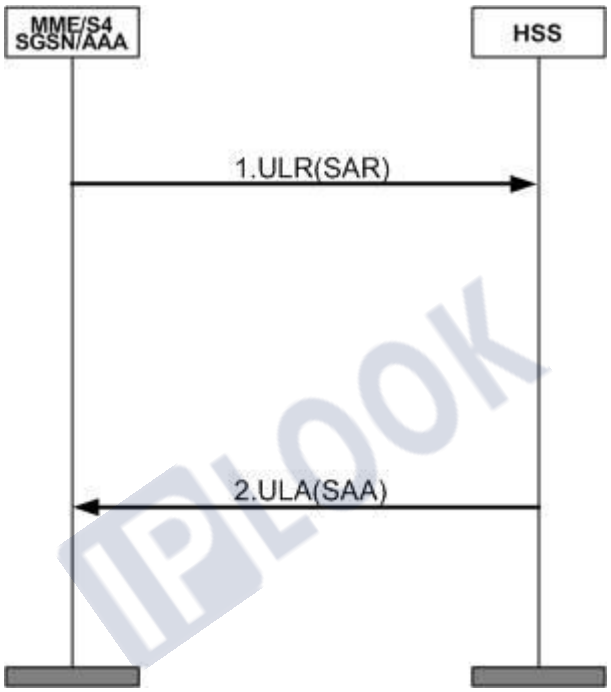


Figure 8 IPLOOK HSS System distribution of relevant user signing data through location update process

1. MME / S4 SGSN / AAA sends a location update request to HSS. The interaction between AAA and HSS is completed through the SAR process (the server assignment request).

2. Return the response message update location answer with successful location update, and bring relevant user data in the response message. The interaction between AAA and HSS is completed through the SAA process (the server assignment answer).

Issue relevant user signing data through the independent user data insertion process:

1. HSS sends the relevant user signing data to MME / S4 SGSN / AAA through the independent insertion user data process IDR (PPR), in which the interaction between AAA and HSS is completed through the PPR process (the push profile request).
2. MME / S4 SGSN / AAA returns the response message of IDA (PPA) to HSS. The interaction between AAA and HSS is completed through the push profile answer.

3.4 PLMN based roaming restrictions

3.4.1 Definition

Roaming restriction service based on PLMN (public land mobile network) means that the system manages user mobility according to the requirements of operators, networks or users, and restricts users to allow or prohibit access to other operators' networks.

This service is generally used to limit the access range of users to the networks of other operators that have signed roaming agreements with this operator.

3.4.2 Dependency

UE	MME	HSS
√	√	√

3.4.3 Principle description

In S6a / S6d location update process, PLMN based roaming restriction process:

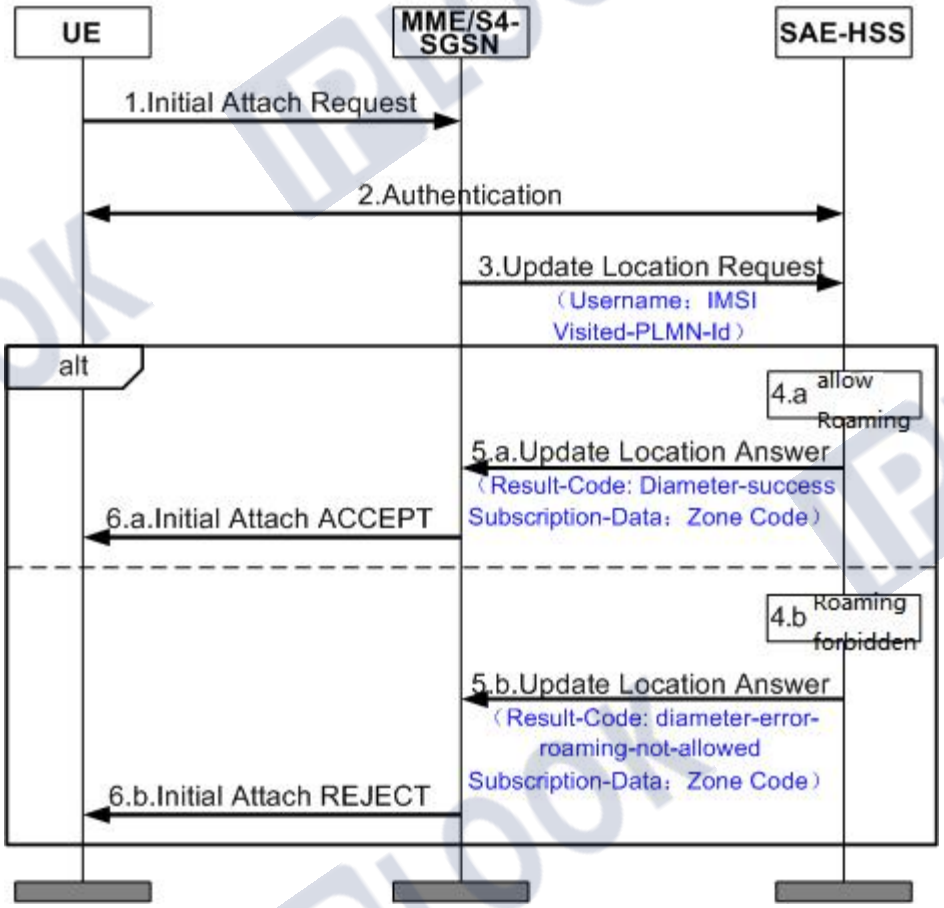


Figure 9 IPLOOK HSS System roaming restriction flow chart based on PLMN

1. When the mobile user leaves the PLMN area to another PLMN area, it will send an initial attach request to MME.

2. MME / S4-SGSN initiates an authentication operation for the user to determine the legitimacy of the user.

3. After successful authentication, MME / S4-SGSN sends a location update request ULR (update location request) to SAE-HSS.

4. SAE-HSS determines whether the user is roaming allowed or roaming prohibited according to the IMSI and visited PLMN ID carried in the location update request message.

5. SAE-HSS returns ULA (update location answer) response message.

a. Roaming is allowed, and the AVP of "result code" carried in the returned ula message is "diameter success".

b. Roaming is prohibited, and the AVP of "result code" carried in the returned ula message is "diameter error roaming not allowed".

6. MME / S4-SGSN returns the initial attach message to the user.

a. Roaming is allowed, and the initial attach accept message is returned to the user. The user's location is updated successfully.

b. Roaming is prohibited, and the initial attach reject message is returned to the user. The user location update fails.

3.5 Equipment status management

3.5.1 Definition

EIR (Equipment Identity Register) is an independent network element device used to store the status information of IMEI (international mobile station equipment identity).The device status management function refers to the function that EIR can detect the legitimacy of the network to the terminal device by checking the status information of the terminal IMEI, so as to control whether the mobile device can access the network.

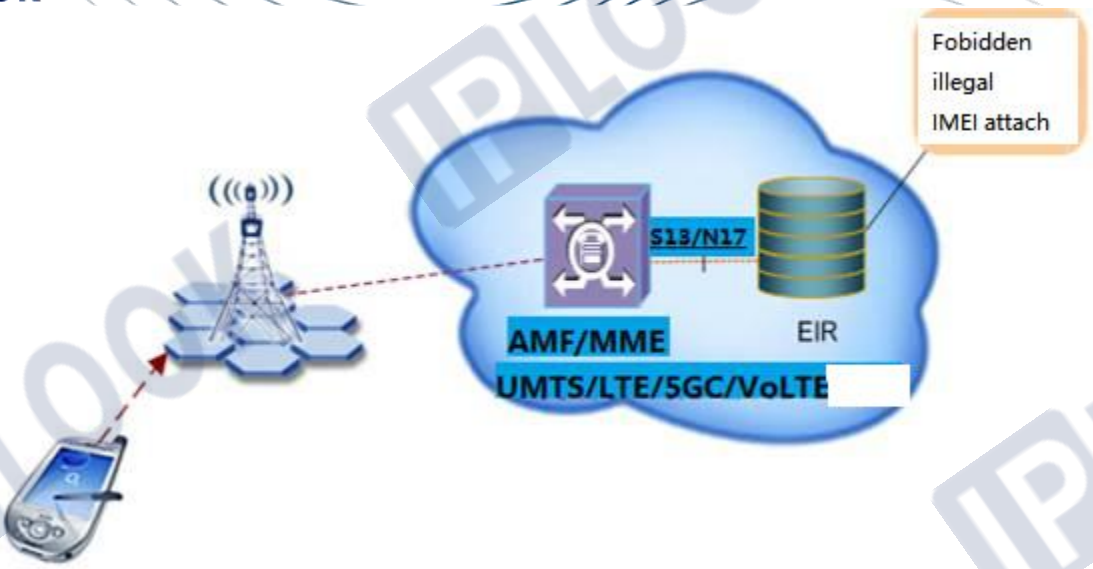


Figure 10 IPLOOK HSS System Schematic diagram of equipment status management function

3.5.2 Application scenario

When the operator needs to restrict the use of mobile devices in a batch of IMEI segments, the status of devices in this IMEI segment can be configured as blacklist status;When the operator allows the mobile equipment in an IMEI section to be available, the equipment status in this IMEI section can be configured as white list status;When the user's mobile equipment is stolen, it can provide the equipment identification IMEI to the corresponding eir business hall and report the loss. Eir can configure the equipment status corresponding to this IMEI to the blacklist status to restrict its access to the network;When the mobile device held by the user is an illegal device (such as a fake machine or an unauthenticated mobile device), EIR can restrict its access to the network.

In addition to the black-and-white list, operators can customize the functions supported by the gray list if necessary.

This function can be applied to LTE network, 5GC network and volte network.

3.5.3 Dependency

UE	MME/AMF
√	√

3.5.4 Description of special effect parameters

category	parameter
Equipment status management parameters	IMEI = international mobile device number
	Status = current status of equipment (white list, blacklist, gray list)

3.5.5 Principle description

3.5.5.1 **IMEI status information**

IMEI number is represented by a 14 digit decimal number, which is used to uniquely identify a mobile device.The EIR stores the IMEI status information of the mobile device, including the following three types:

- White table status: indicates that this mobile device is a legal device, and MME / AMF will allow it to access the network.
- Black table status: indicates that this mobile device is an illegal device, and MME / AMF will deny its access to the network.

- Gray table status: indicates whether the mobile device can access the network, which will be determined by the operator.

According to different application network types, the implementation principle is described according to business process 1 (LTE network and volte network) and business process 2 (5GC network).

3.5.5.2 **Business process 1(LTE Network and volte Network)**

When detecting the legitimacy of the mobile device, MME will obtain the IMEI number from the mobile device and send me identity check req (ECR) message to eir to check the device status. Eir queries the device status information and returns the status information to MME. MME will judge whether the mobile device is legitimate according to the status returned by eir, and then decide whether to allow the mobile device to access the network.

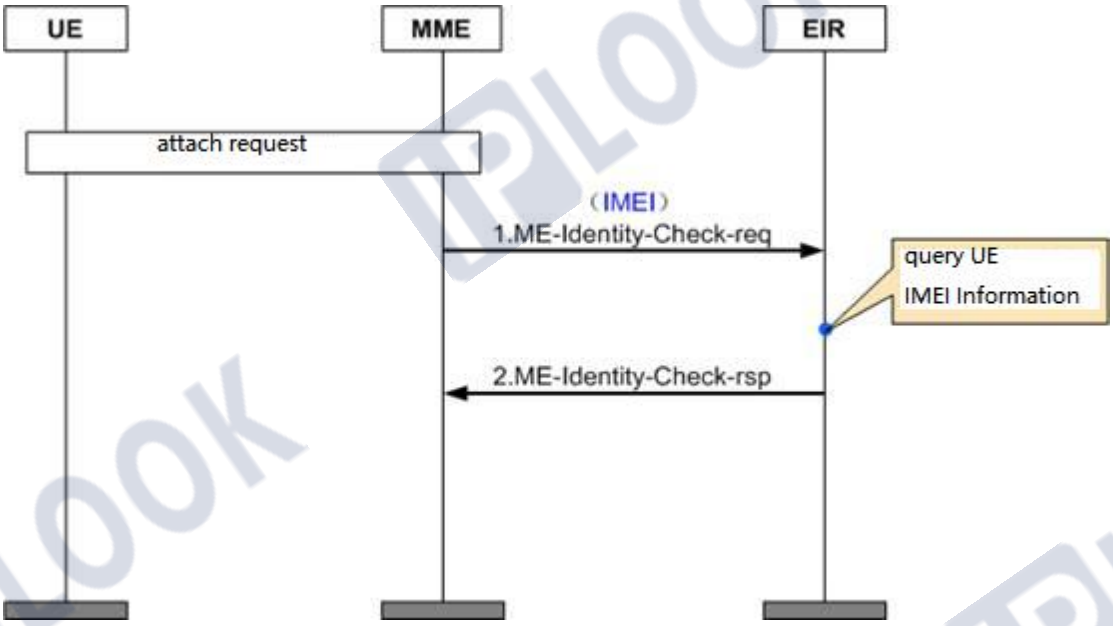


Figure 11 IPLOOK HSS System ECR message interaction diagram

1.After initiating the network access request, MME sends ME-Identity-Check-req message to eir, and carries the IMEI number of the UE in the request message.

2. After receiving the request message, the EIR first looks up the IMEI number. If it exists, set the status information of the IMEI to the status queried in the database. If it does not exist, set the status information of the IMEI to unknown.The IMEI status message of the MS is carried in the me identity check RSP message.

3.5.5.3 **Business process 2(5GC Network)**

When detecting the legitimacy of a mobile device, AMF will obtain the IMEI number from the mobile device and send a GET .equipment-status?pei={pei}&supi={supi} message to 5G-EIR to check the device status. 5g-eir queries the device status information and returns the status information to AMF. AMF judges whether the mobile device is legitimate according to the status returned by EIR,Then decide whether to allow the mobile device to access the network.

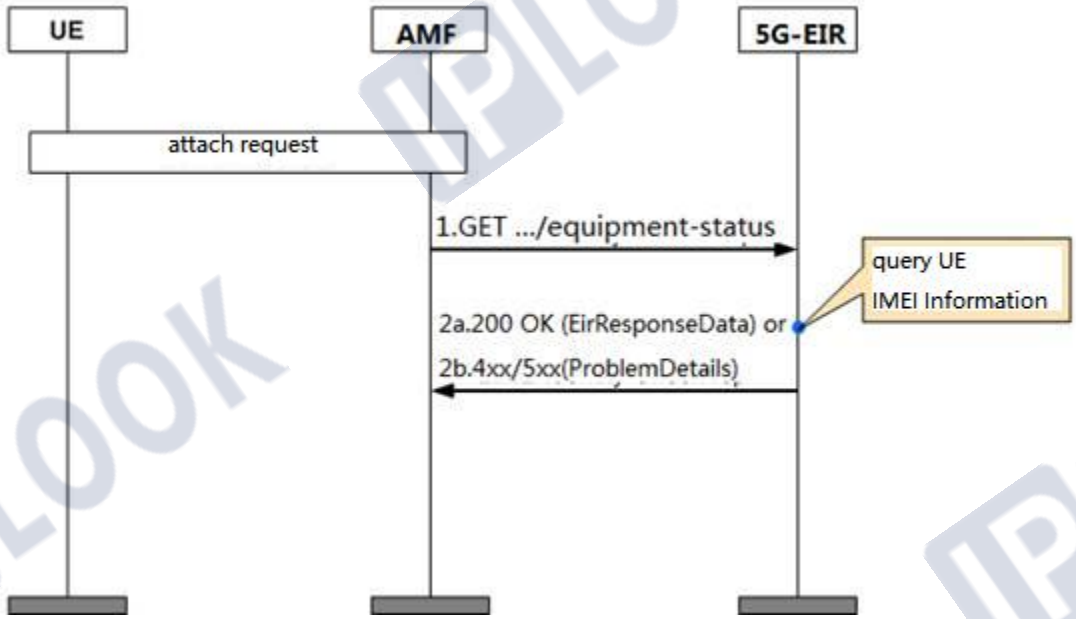


Figure 12 IPLOOK HSS System 5G get device status message interaction diagram

1.After initiating the network access request, AMF sends a GET .equipment-status message to 5G-EIR, and carries the PEI (IMEI or imeisv) number of the UE in the request message.

2a.5G-EIR first looks up the PEI (IMEI or imeisv) number after receiving the request message. If it exists, it returns 200 OK and the status information of the IMEI is the status queried in the database.

2b. If PEI (IMEI or imeisv) does not exist, the message "404 not found" and the "problemdetails" object are carried in the message, and the "detail" in the object is set to "error_equipment_unknown".

3.5.6 Beneficiary

Operators can increase their operating revenue through the equipment status management function.

Through the equipment status management function, operators prohibit illegal terminals (such as cottage machines) from outside the network, which can protect network security and reliability.

By providing equipment status management function, operators can provide security services for end users and attract more users to the network.For example, operators can monitor users' stolen mobile phones through the device status management function to prevent users' mobile phones from being stolen or online information disclosure.When a user's mobile phone is stolen, he can report the loss of the mobile phone IMEI to the business hall, limiting his access to the network, so as to improve the security of the mobile phone.

3.6 Authentication data configurable

3.6.1 Definition

The configurable functions of authentication parameters mainly include supporting the configuration of C1 ~ C5 and R1 ~ R5 parameters

3.6.2 Dependency

UE	MME	HSS
√		√

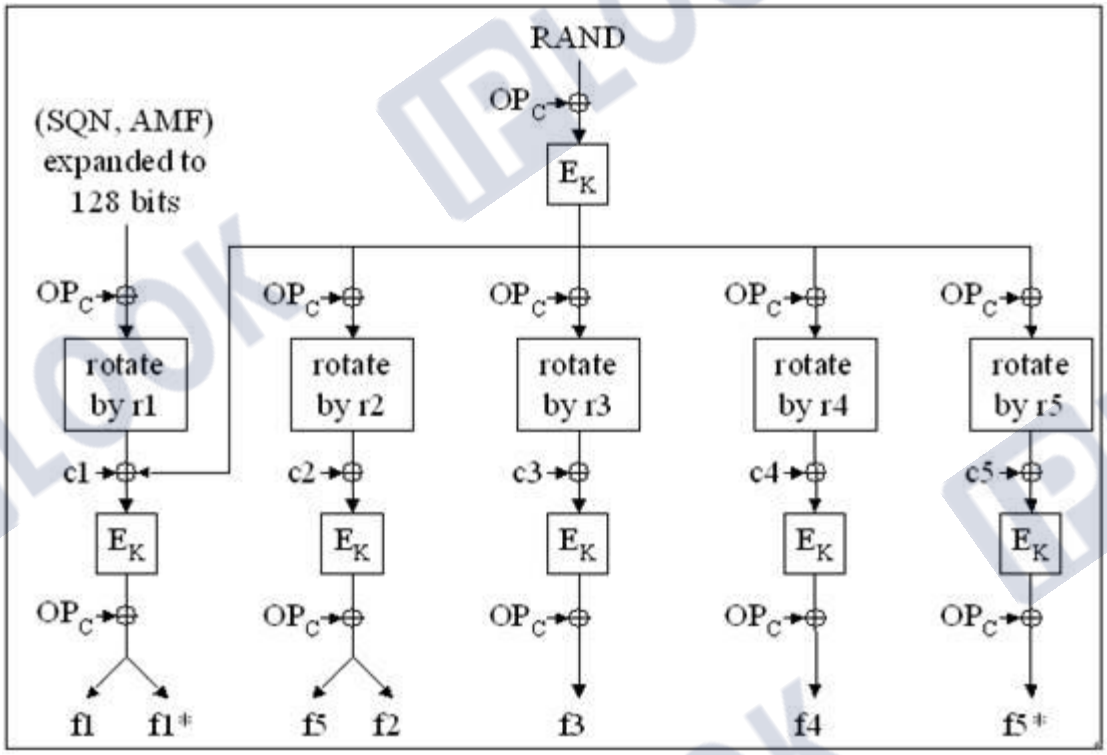
3.6.3 Description of special effect parameters

When some operators have high security requirements, they may use customized C1 ~ C5 and R1 ~ R5 parameters as the input of authentication milenage algorithm to improve the security of users.

3.6.4 Principle description

In the calculation process of milenage algorithm, C1 ~ C5 and R1 ~ R5 parameters will be used. These parameters can be customized by operators to enhance the security of the algorithm.The calculation process of the specific algorithm is shown in the following figure:

Calculation process of f1，f1*，f2，f3，f4，f5 and f5*



3.7 ODB service

3.7.1 definition

ODB (operator determined barring) refers to the blocking determined by the operator, which means that the service capability of the user to access the GSM / UMTS / LTE network is set for the user by the PLMN (public land mobile network) network operator.

3.7.2 Dependency

UE	MME	HSS
√	√	√

3.8 Access type restriction function

3.8.1 Definition

The access type restriction function is a function provided to operators to control the access rights of mobile users to different networks.

Access types can be divided into:

- GERAN(GSM/EDGE Radio Access Network)
- GAN(Generic Access Network)
- I-HSPA-Evolution(Internet High Speed Packet Access-Evolution)
- EUTRAN(Evolved Universal Terrestrial Radio Access Network)
- HO-To-Non3GPP-AccessHO To Non 3rd Generation Partnership Project Access

When a mobile user opens an account, the operator configures the user's ard (access restriction data) data on HSS according to the access type selected by the user, so as to control the mobile user to access different types of networks.

3.8.2 Dependency

UE	MME	HSS
√	√	√

3.8.3 Description of special effect parameters

This feature can be applied to 2G / 3G networks or LTE networks

3.8.4 Principle description

The user accesses the LTE network and checks the ARD function when the location is updated

1.The mobile user sends an initial attach request to the MME.

2.MME initiates an authentication operation for the user to determine the legitimacy of the user.

3.After successful authentication, MME initiates update location to HSS.

4.HSS returns the response message of update location, which contains the ard data of the user.

5.MME determines whether the user is allowed to access the network according to the user's ard data. If it is determined that it is not allowed, it returns the initial attach reject message to the user, and the user's location update fails.

6.If the user allows access, the initial attach accept message is returned to the user, and the user location is updated successfully.

3.9 Roaming restrictions in user area

3.9.1 Definition

EPS (evolved packet system) user area roaming restriction, that is, EPS user roaming is restricted according to the area roaming template or the cell location accessed by the user for the first time.

Zone Code is the roaming area code of the user area planned by the operator. A roaming area template can have up to 20 Zone Codes.

There are two user area roaming restriction schemes provided by EPS HSS, namely static area roaming restriction and dynamic area roaming restriction. The flexible area roaming restriction function can not only realize different roaming experiences of users, but also enable operators to flexibly and efficiently manage user mobility.

Static area roaming limit means that the user has signed up for a fixed area roaming template planned by the operator (the Zone Code list and roaming cell range have been determined at the time of signing up and cannot be changed automatically).EPS HSS sends the Zone Code list signed by the user to the MME where the user is located. After receiving the Zone Code list, MME limits the roaming status of the user according to the Zone Code and roaming restriction policy (blacklist or whitelist) of the roaming area where the user is located.

Dynamic area roaming restriction means that when a user signs up, the range of the roaming area is not determined, but the area centered on the cell (including adjacent cells) is automatically locked as the roaming active area of the user according to the cell location when the user UE (user equipment) first accesses, and a regional subscription Zone Code list is generated at the same time.EPS HSS sends the user area signing code list to the MME where the user is located. After receiving the user area signing code list, MME limits the user's roaming

status according to the user area signing code and roaming restriction policy (blacklist or white list) in the user's roaming area.

3.9.2 Dependency

UE	MME	HSS
√	√	√

3.9.3 Principle description

The specific business implementation is mainly completed by MME, and HSS is only responsible for the storage and distribution of signing information.

·If the user signs up for static area roaming restrictions when he is not on the network, HSS will distribute the list of zone codes signed by the user to MME through the location update process.

·If the user is in the network and signs up for static area roaming restrictions, HSS will send the user's modified zone code list to MME through IDR / IDA message.

·If the user is in the network and signs up for static area roaming restrictions, HSS notifies MME to delete the user's zone code list information through DSR / DSA message.

3.10 General configuration APN function

3.10.1 Definition

When signing an APN (access point name) for a user, the wildcard "*" is used to indicate the universal APN.After signing the universal APN, the user can select the appropriate APN access network according to the actual situation.

3.10.2 Dependency

UE	MME	HSS
√	√	√

3.10.3 Principle description

The specific business implementation is mainly completed by MME, and HSS is only responsible for the storage and distribution of signing information.

3.10.3.1operation flow

- If the user signs up for the general distribution APN when he is not in the network, HSS will issue the general distribution APN signed by the user to MME through the location update process.
- If the user is in the network and signs up for universal APN, HSS sends the universal APN signed by the user to MME through IDR / IDA message.
- If the user is in the network and signs up for universal APN, HSS notifies MME to delete the user's universal APN information through DSR / DSA message.

3.11 Multi HPLMN function

3.11.1 Definition

HPLMN (home public land mobile network) management function is mainly to provide users with operations of adding, deleting, modifying and querying system HPLMN information.

3.11.2 Dependency

UE	MME	HSS
√	√	√

3.11.3 Principle description

The HPLMN function mainly involves four operations: add, delete, modify and query.The message processing mainly involves the processing of location registration messages.When the user signs up for ODB service, compare the VPLMN brought by the message with multiple HPLMN records saved in the database:

·If there is a match, it is considered to be the home domain.

·If none of them match, it is considered a visiting domain (roaming).

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.

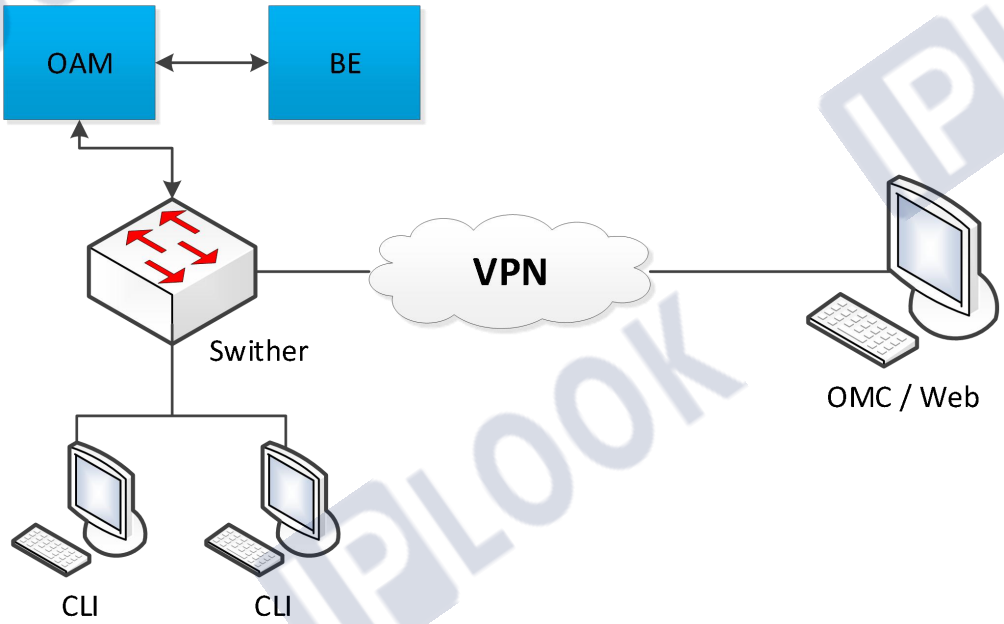
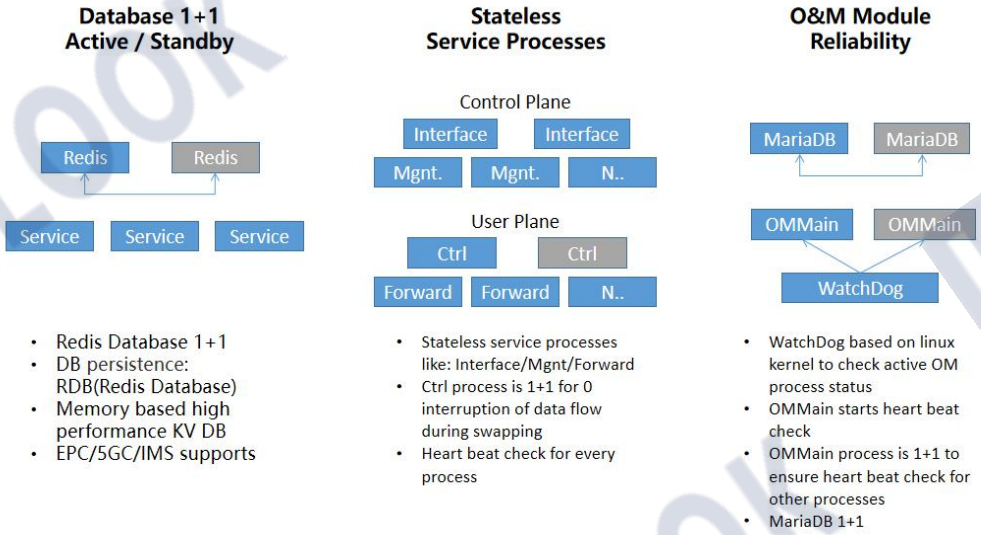


Figure 13 shows the network architecture

5 Reliability design

5.1 Software Reliability

Figure 14 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.

5.2 Network element Reliability

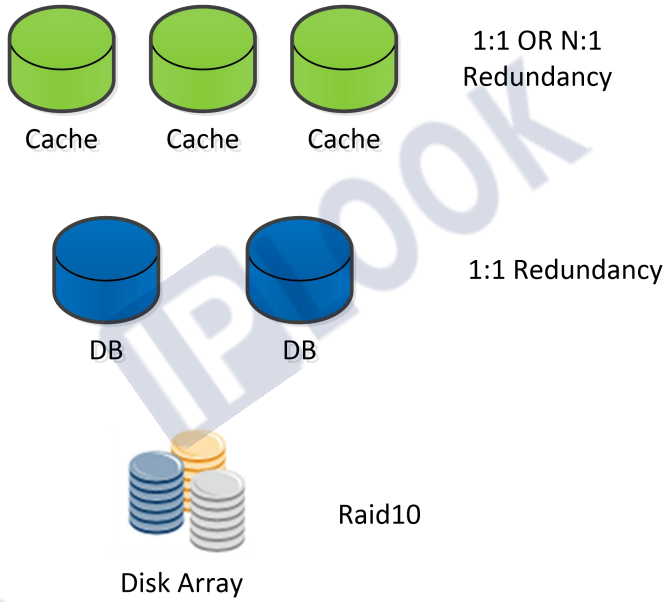
5.2.1 Multiple level of redundancy

At NE level, IPLOOK provides Configuration Data Backup and Recovery.

This feature provides the function for backup and recovery of configuration data in the back end database.

HSS/HLR adopts multiple level backup mechanism and store subscriber's data into different physical storage devices to ensure security, as shown in Figure 15.

Figure 15 OAM redundancy



- Level Ⅰ redundancy

  subscriber's data is cached in different in-memory databases. It can be a 1:1 active/standby mode or an N:1 redundant mode. The data on the Active unit will be synchronized to the standby unit in real time.

- Level Ⅱ redundancy

  The database backup mode adopts 1:1 active/standby

- Level Ⅲ redundancy

  Subscriber's data is saved to the disk array. The disk array hard disk is in RAID 10 mode and hot spares disk mode.

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.

5.2.2 High Capacity and integration

HSS/HLR， different capacity can be supported based on different deployment modes and hardware. It can support half a million users under fundamental conditions. The fundamental is to deploy the FE signaling processing unit and BE storage unit respectively with two general servers. See section 3.11 for general server hardware configuration

For operators over a million subscribers, greater capacity can be achieved by overlaying the FE signaling processing unit and BE storage unit.

5.2.3 Remote disaster-tolerant

HSS/HLR support migrant deployment , and achieve seamless remote disaster-tolerant through completing data synchronization with data replication and consistency verification technology.

Remote disaster-tolerant has following advantages:

- "0" time of fault isolation with high reliability
- With mature IT technology, the cost of disaster recovery system's construction is low.
- Simplify the network, facilitate maintenance, and lower the total cost.

6 Interfaces and Protocols

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

Table 3 3GPP Related Interfaces and Protocols of IPLOOK HSS

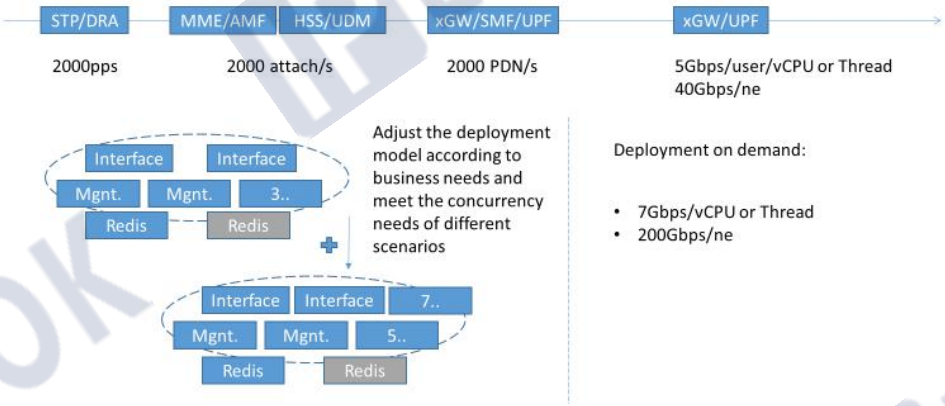
Interface	Description	Protocol	Standard
S6a	Interface between HSS and MME.	Diameter	3GPP TS 29.272
Cx	Interface between IMS and HSS/HLR	Diameter	3GPP TS 29.272
C	Interface between GMSC and HSS/HLR.	MAP	3GPP 29.002
D	Interface between MSC/VLR and HSS/HLR.	MAP	3GPP 29.002

Interface	Description	Protocol	Standard
Gr	Interface betwee SGSN and HSS/HLR	MAP	3GPP TS 29.274
Northbound	Interface between BSS/OSS and HSS/HLR	MML，SOAP，RESTful	

7 Dimension

7.1 Performance

Figure 16 Performance



One HSS 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 4 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
HSS/HLR	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.

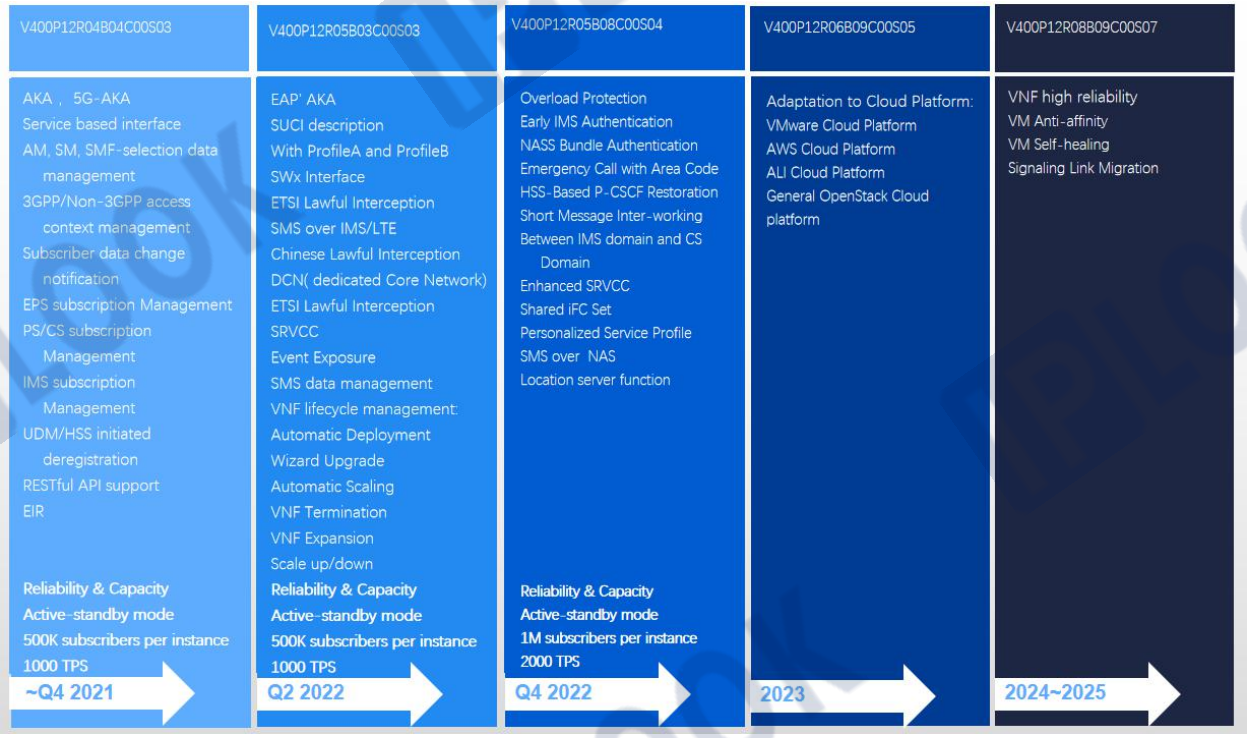
HSS/HLR means they have same dimension methodologies, share same hardware resource requirements.

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


V400P12R04B04C00S03
AKA , 5G-AKA
Service based interface
AM, SM, SMF-selection data management
3GPP/Non-3GPP access context management
Subscriber data change notification
EPS subscription Management
PS/CS subscription Management
IMS subscription Management
UDM/HSS initiated deregistration
RESTful API support
EIR
Reliability & Capacity
Active-standby mode
500K subscribers per instance
1000 TPS
~Q4 2021
V400P12R05B03C00S03
EAP' AKA
SUCI description
With ProfileA and ProfileB
SWx Interface
ETSI Lawful Interception
SMS over IMS/LTE
Chinese Lawful Interception
DCN(dedicated Core Network)
ETSI Lawful Interception
SRVCC
Event Exposure
SMS data management
VNF lifecycle management:
Automatic Deployment
Wizard Upgrade
Automatic Scaling
VNF Termination
VNF Expansion
Scale up/down
Reliability & Capacity
Active-standby mode
500K subscribers per instance
1000 TPS
Q2 2022
V400P12R05B08C00S04
Overload Protection
Early IMS Authentication
NASS Bundle Authentication
Emergency Call with Area Code
HSS-Based P-CSCF Restoration
Short Message Inter-working Between IMS domain and CS Domain
Enhanced SRVCC
Shared iFC Set
Personalized Service Profile
SMS over NAS
Location server function
Reliability & Capacity
Active-standby mode
1M subscribers per instance
2000 TPS
Q4 2022
V400P12R06B09C00S05
Adaptation to Cloud Platform:
VMware Cloud Platform
AWS Cloud Platform
ALI Cloud Platform
General OpenStack Cloud platform
2023
V400P12R08B09C00S07
VNF high reliability
VM Anti-affinity
VM Self-healing
Signaling Link Migration
2024~2025

9 Acronyms and Abbreviations

Table 5 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