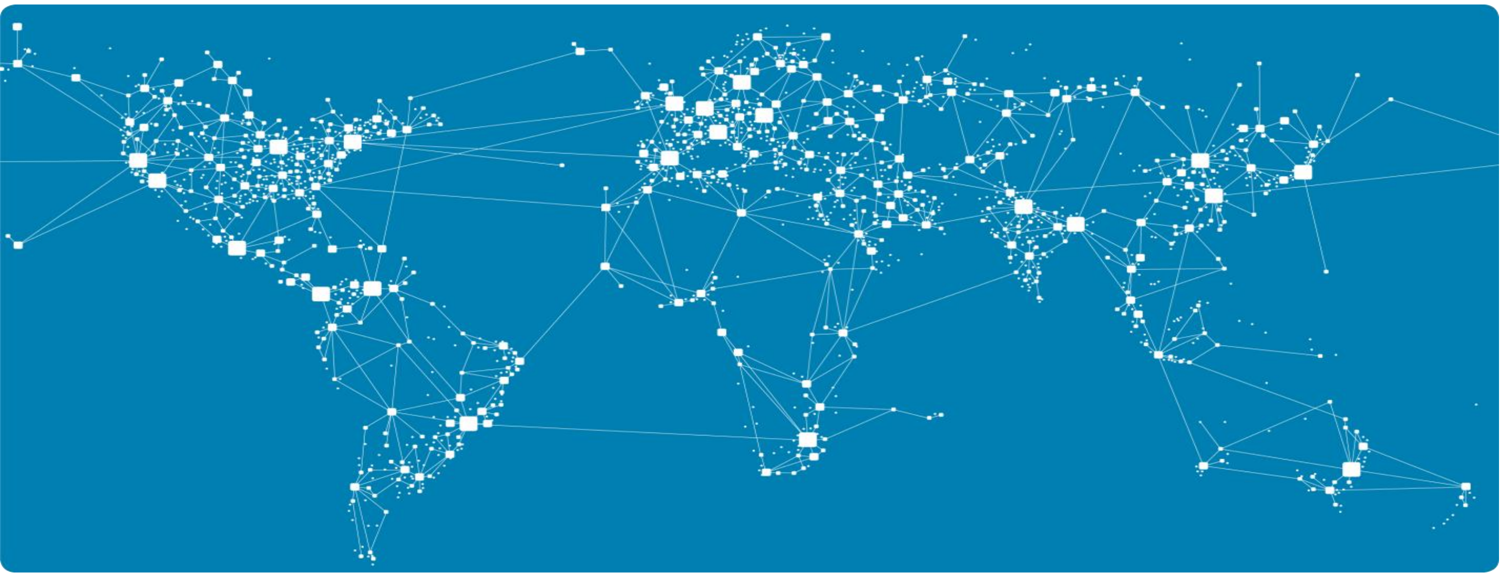


IPLOOK HSS/HLR PRPDUCT INFORMATION

Item No.	IPLOOK HSS/HLR100
Version	V2.0
Release Date	2018-05-09

Contents

1 Description

1.1 Overview

Conform to the 3GPP R10 29.272 and 29.002 protocol specifications, IPLOOK HSS / HLR100 (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.

- BE

  The BE is responsible for storing subscriber's information, with addition, deletion, update and query of subscriber's information to provide effective data management for the FE.

- FE

  The FE is responsible for signaling access and logic processing of service, and obtains data support from the BE. Figure 1-1 shows the networking of the HSS / HLR.

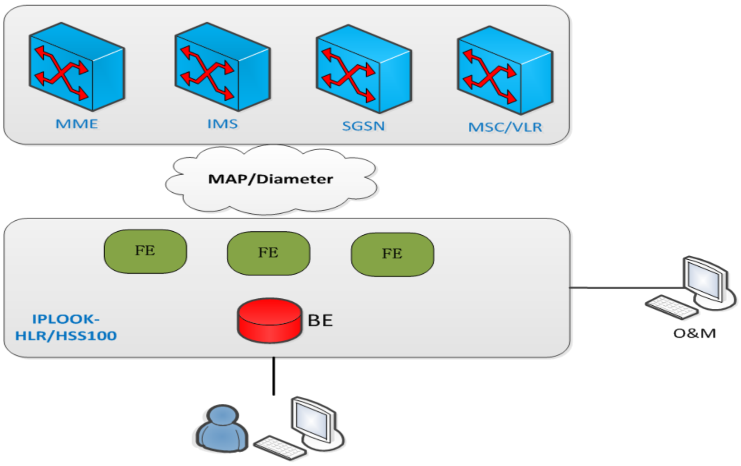


Figure 1-1 SAE-HSS/HLR100

The HSS/HLR user data and service separation has the following advantages:

- Networking is more flexible

  As the BE and FE are deployed separately, they can be deployed in different geographical locations respectively. The operator can deploy the BE and the FE according to the population distribution and the size of the area.

- Avoid the risk of carriers binding equipment vendors

  The BE provides a standard/open access interface of user data for third-party devices to access. In this way, the risk of the operator binding the device vendor avoided.

1.2 Features of IPLOOK HSS/HLR

1.2.1 Distributed Architecture

Distributed Architecture means that multiple same entities within a system perform a specific work in a load-sharing manner. The distributed architecture of HSS/HLR is shown in Figure 1-2.

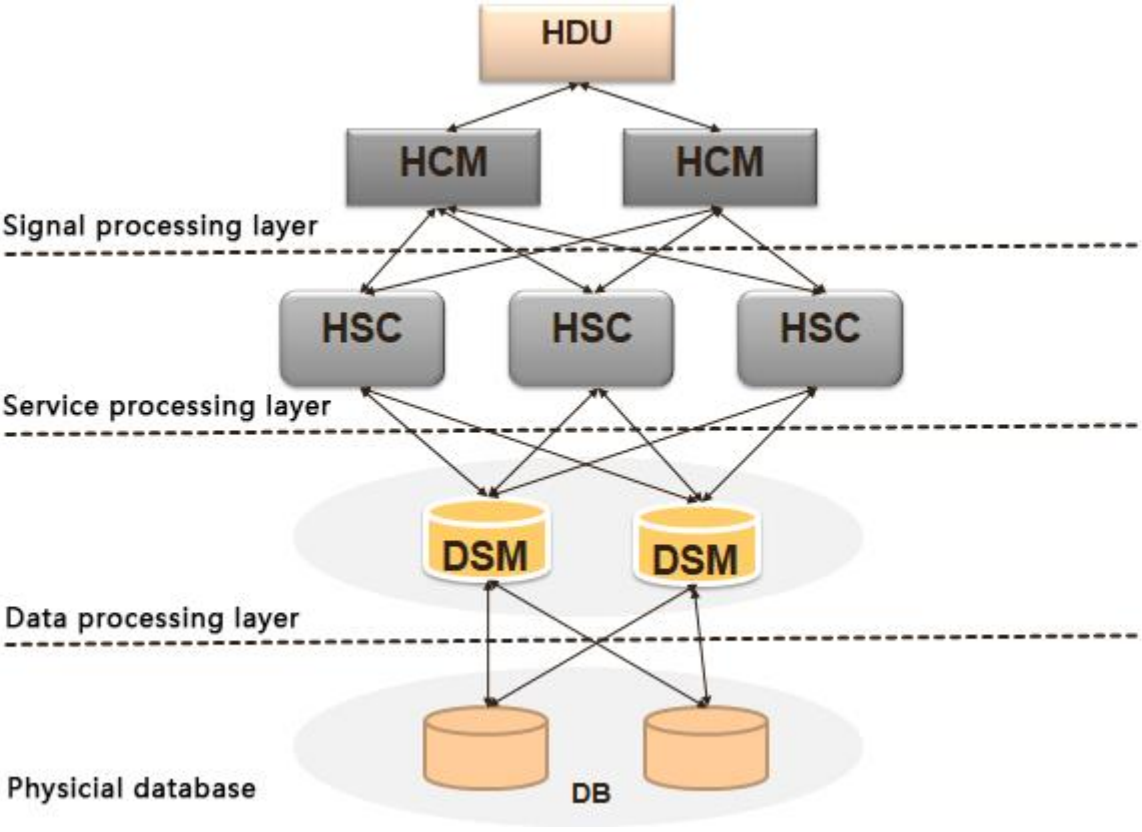


Figure1-2 HSS/HLR Distributed Architecture

HDU: HSS/HLR message distribution module which processes IP/SCTP/TCP data transmission layer;

HCM: HSS/HLR link management, which processes the diameter/MAP application layer protocol;

HSC: HSS/HLR session control module that processes user signaling control logic;

DSM: Data service module and data access middle layer which provide abstract processing of database access;

DB: database

HSS/HLR's distributed architecture has the following advantages:

- Reliability excellence

If any entity in the system faults, its load is automatically balanced to other entities to ensure that the system continues to work.

- Network expansion smoothly

When network expansion is required, you only need to add the corresponding entity. After the new entity runs stably, the system load is automatically balanced to ensure that the entire capacity expansion process has no influence on t the service provided by the system.

1.2.2 Hardware platform

HSS/HLR adopts IA (Intel Architecture) architecture based on high-performance low-power processor and CGL (Carrier Grade Linux) carrier-grade Linux technology

The HSS/HLR hardware adopts a general-purpose server based on the X86 architecture processor and is deployed on Linux operating systems such as RedHat. High reliability is achieved through a distributed architecture.

1.2.3 Data cache management

Subscriber's data is cached in memory. Subscriber's data queries and modifications involved in the service process are completed in memory. External database storage is saved persistently

The advantages of data cache:

- Avoiding the dependence on external storage devices, the failure of external storage devices does not affect the normal process of services.
- Compared with data in hard disk, data cache has the advantages of large throughput and short time-delay, which greatly improves system performance, and the strengths of our system is more significant in the cases whose capacity is fairly bigger.

1.2.4 Multiple level of redundancy

HSS/HLR adopts multiple level backup mechanism and store subscriber's data into different physical storage devices to ensure security, as shown in Figure 1-3.

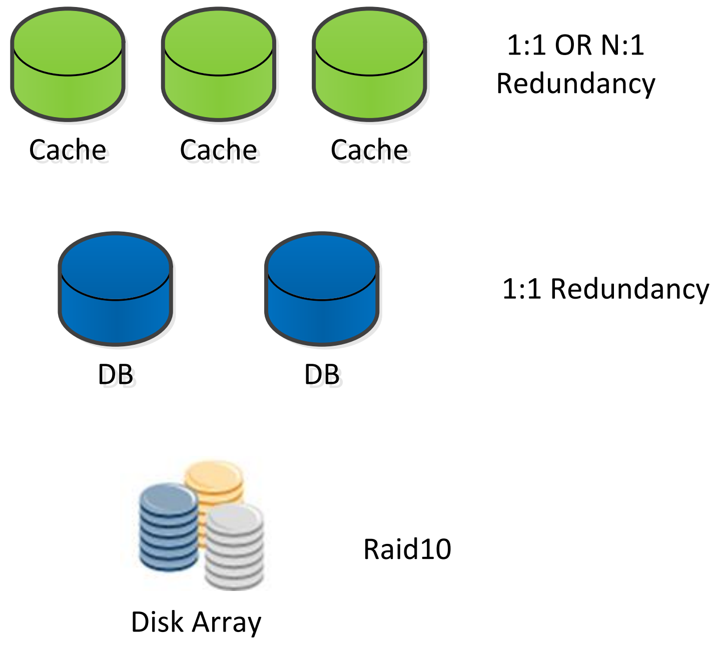


Figure 1-3 diagram of multi-level backup mechanism

- 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.

1.2.5 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.

1.2.6 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.

2 Functions

2.1 Basic subscirber's data management

IK-HSS/HLR store data of the subscribers from CS domain and the PS domain. The data mainly includes:

1) Subscriber's info

- IMSI
- MSISDN
- Status

2) Supplementary services info

- Forwarding info
- Call barring info

3) GPRS，UMTS and EPS subscription info

- Provide up to 10 APN subscription data to one user

4) ODB info

5) Roaming restriction info

6) CAMEL2 subscription info

7) ARD info

- Restrict users from accessing 2G, 3G or 4G networks, and can subscribe ARD information based on number

8) User hierarchical access information, including 2 eMLPP parameters：

- maximum entitled priority
- default priority

9) ADD info

10) HSPA QoS Profile info, which support R7 QoS Profile (from 16Mbps to 256Mbps).

2.2 Authentication

IK-HSS/HLR 100 combine the functions of the AuC Authentication function

2.2.1 GSM/UMTS authentication

IK-HSS/HLR 100 provide authentication parameters to the VLR/SGSN according to the request of the VLR/SGSN, and 1~5 sets of authentication triplet/Quintet are sent each time. After the authentication parameters are sent to the VLR/SGSN, the HLR deletes the old authentication parameters. IK-HSS/HLR 100 has the function of converting quintet authentication parameters into triplet authentication parameters.

1） The authentication algorithm supports multiple algorithms of the 2G system and various algorithms of the 3G system, including the comp128-1 algorithm, the comp128-3 algorithm, and the MILENAGE algorithm (including f0, f1, f1*, f2, f3, f4, f5, f5). *, c1, c2, c3 function)

2） Storage of authentication data: a UMTS user or a GSM user is supported, storing the IMSI/KI/Ver of each user for the GSM user, and storing the IMSI, K, AMF, SQN, OP or OPC of each user for the UMTS user.

3） Generate and transmit authentication triplet and quintet: According to the user type(UMTS user or GSM user) and the MAP protocol version supported by the VLR/SGSN currently accessed by the user, the AUC generates a triplet authentication vector or quintet. Ang HSS/HLR can provide 1~5 groups of authentication quintuet/triplet each time according to the VLR/SGSN request and its own configuration.

4） Conversion between quintet and triplet: If the UMTS user accesses from the 2G VLR/SGSN, the AUC uses the conversion algorithms c1, c2, c3 to achieve the conversion between 3G authentication quintet and 2G authentication triplet.

5） Support authentication resynchronization: AUC supports authentication resynchronization algorithms f5*, f1*. When it finds that the SQN in the USIM card is incorrect, the authentication resynchronization process is initiated, requesting to generate a new authentication vector.

2.2.2 **EPS authentication function**

The IK HSS/HLR 100 can provide one or more sets of authentication parameters to the MME according to the MME’s request, and supports related process of authentication service .

The IK HSS/HLR 100 is responsible for generating the key and authentication vector associated with the user authentication. In addition to the related parameters of authentication vector, namely RAND, MAC, XRES, KASME (for EPS AKA) or CK/IK (for UMTS AKA), all generated and stored parameters in the IK HSS/HLR 100 are not transmitted outside. The safety parameters involved in IK HSS/HLR 100 are: K, r1-r5, c1-c5, AMF, SQN, RAND, OPc, CK, IK, KASME, AK, SN ID, AUTN, XRES.

2.3 Mobility management and roaming functions

2.3.1 GSM/UMTS Mobility management

✓ Support mobile management MAP interface, including location update and location deletion.

- The HSS/HLR can cooperate with the VLR/SGSN to complete the location registration function and initiate a deregistration to the previous VLR/SGSN.
- When the HSS/HLR receives the PURGE request message from the VLR/SGSN, the mobile station is set to the PURGE state.

2.3.2 LTE Mobility management

- □ Store the IP address of MME currently serving the user, and store related parameters like the network capability of the MME.
- □ Be able to complete the location registration notification initiated by the MME, the location registration status of the user and the update of the current serving MME’s IP address .
- When the following conditions occur, the HSS should initiate a logout to the original MME and carry the relevant logout type: attaching to the network for the first time, moving to the new MME; the network forcibly changing the registration status or MME’s address of the user; the user is deleted.
- When receiving the request from the MME to delete the UE, the HSS shall be able to set the “UE Clear” mark for the UE.
- □ Support configuring reachability management functions in user subscription data; notifying the corresponding MME.
- Save the service platform information of the reachability information of the application user, and notify the corresponding service platform of the user reachability information.

2.4 ODB and roaming restriction function

The IK-HSS/HLR 100 supports the following ODB features:

- □Block all outgoing calls
- □Block all international calls
- □Block all international calls except those belonging to the PLMN country
- When the roaming out of the home PLMN country, the call is blocked
- □Block supplementary service access
- □Block all incoming calls
- When in roaming out of the home PLMN country, the inbound call is blocked
- Blocking services out of the home PLMN
- □Block SMS service
- □Blocking the outgoing call and access of a specified user
- □ODB block call forwarding
- □ODB blocking PS service

When the ODB information changes (adds, modifies or deletes), the HSS/HLR updates the corresponding subscription information and sends the ODB information to the VLR/SGSN in the ISD message.

2.5 Restriction based on accessing type

Restriction based on accessing type, that is, limit the type of users. Accessing type mainly include:

- ✓ UTRAN(Universal Terrestrial Radio Access Network)
- ✓ 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-Access(Handover-To-Non General Packet Radio Service-Access)。

2.6 Call session management

Routing the callee’s call session and obtain the roaming number in circuit domain.

When the MS is callee, the IK-HSS/HLR requests the callee’s VLR to allocate the MSRN according to the request of the GMSC or the MSC, and then sends the MSRN to the requesting MSC.That is, supporting to provide routing information for each call session.

2.7 Supplementary services function

HSS/HLR can cooperate with MS to complete the activation, deactivation, registration, deletion, password modification and other procedures of supplementary services.

2.8 Online charging /hot billing function

When the real-time charging of the PS domain is performed by the OCS, or when the user is hot-charged, the Subscribed Charging Characteristic fields in the user subscription data is used to identify the user as an online charging user or a hot charging user to trigger the corresponding online charging process or hot billing for users in the PS domain.

2.9 Restore function

After the IK-HSS/HLR is restarted, on the basis of the previous backup, the corresponding recovery procedure is executed to obtain the correct mobile location and supplementary service information, and notify the affected user of the current MME, SGSN and MSC.

3 Product Architecture

3.1 Hardware platform

3.1.1 Product appearance

The HSS/HLR deployment adopts a X86 physical server or a cloud platform such as vmware/OpenStack. The number of servers and cloud platform resources required for HSS/HLR deployment are determined by the user scale and the capacity requirements of the customers. For details, please refer to Section 7.1: “Performance Indexes” chapter.

Figure 3-4 Product appearance

Hardware specifications：

CPU:2 x Intel E5-2650 v3 10 cores，2.3GHz（Or later version）

MEM:32G RAM

HDD: 2 x 500G HDD Raid 1

NIC: 6 x 1GE NIC

Size:444 x 684 x 87.3 mm（Vary with brand）

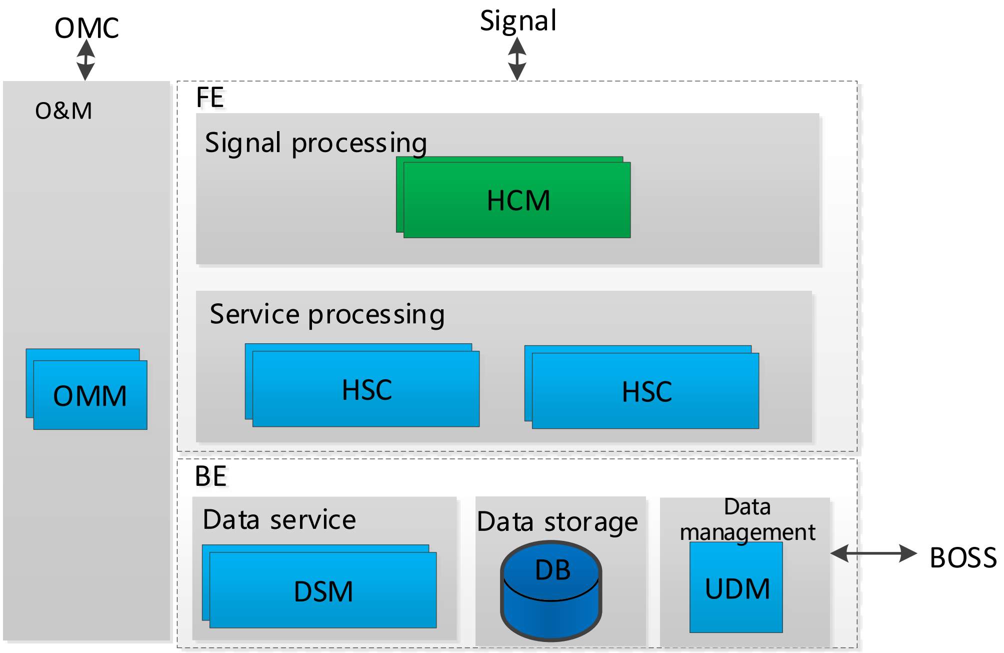
Temperature：-40~+85°C

Operation System：CentOS 7.4

3.2 Software architecture

The software architecture of HSS/HLR is shown in Figure 3-5. It is divided into six logical functional layers: signaling processing, service processing, subscriber’s data management, data service, data storage and O&M.

图 3-5 HSS/HLR software architecture



HCM：HSS/HLR link management module

HSC：HSS/HLR session control module

DSM：HSS/HLR data service module

UDM：User data management module

OMM：Operation and Maintenance module

3.2.1 Signal Processing subsystem

The signal processing is responsible for establishing a connection with other network devices and performing signal service processing. The functions are as following:

- Responsible for message processing at the IP/SCTP (TCP) and TCAP/MAP protocol layers.
- Receiving a Diameter message from the MME, unpacking the Diameter message, and forwarding the message to the HSC.
- Receiving a MAP message from the VLR/SGSN, unpacking the MAP message, and forwarding the message to the HSC.

- Distribute Diameter/MAP messages according to the load of the HSC module to achieve load sharing.

3.2.2 Service processing subsystem

The main function of service processing subsystem：

- To achieve user service processing logic.
- To support GSM/UMTS AKA authentication process and EPS AKA authentication process.
- To support application layer coding and decoding of messages.
- To support the management of user data.

3.2.3 Data service subsystem

It's main functions are as following：

- Data caching function

  Complete the caching function of user subscription data and parameter dynamic data in service processing. Sustainable storage for dynamic data.
- Backup for HSC modules

  To support HSC module registration and data backup function to achieve high reliability of HSC.

3.2.4 Data storage subsystem

The data storage subsystem consists of the MySql database platform and disk arrays, providing persistent storage of data and third-tier backup and recovery. The data storage subsystem is only used as a device for data persistent storage, and does no matter with service processing.

3.2.5 Data management subsystem

The data management subsystem primarily provides an interface to the service delivery system. Completing the interaction with the BSS/OSS system.

3.2.6 Operation and maintenance subsystem

OMM is a operation and maintenance system. The introduction of it is described in 4 Operation & Maintenance.

4 Operation & Maintenance

4.1 The architecture of O&M subsystem

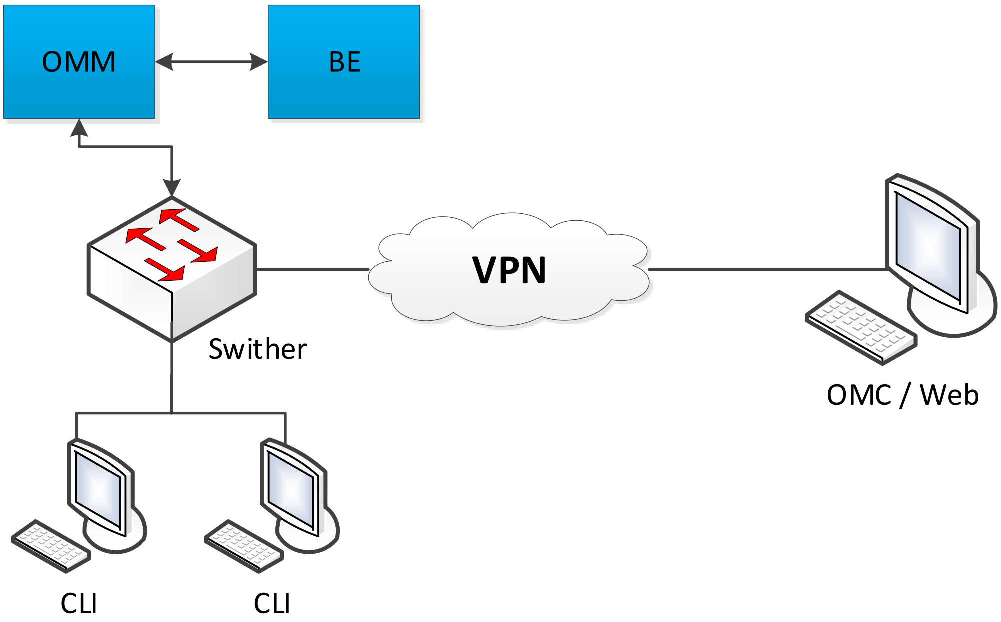
Based on the Client/Server architecture, the operation and maintenance subsystem provides a GUI operation and maintenance subsystem and a Web UI performance measurement system to support customized human-machine interfaces.

The operation and maintenance subsystem supports three modes of operation:

- Performing operations on the local maintenance terminal.
- 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.

Operation & Maintenance subsystem's diagram is as figure 4-1

Figure 4-1 Architecture of O&M subsystem



Oi&M subsystem works in client/server mode

4.2 Basic functions of O&M subsystem

4.2.1 Configuration management

There are two ways of configuration . One is to use a SNMP-based configuration system, providing users with a set of methods for operation and query. OMC can monitor and manage this product in all aspects. The other is a local command line system.

The relational database is used to manage the configuration, and provides database operations such as adding, deleting, modifying, querying, storing, backing up, restoring, etc., and can effectively manage various configuration data (such as hardware data, signaling data, module data, etc.).

4.2.2 Fault management

Alarm management

- Real-time detection and reporting of alarms such as faults or abnormalities of the device.
- To support store alarm information, query alarm history records, and set alarm processing modes.
- To display alarm handling suggestions on the alarm console to facilitate rapid location and processing of device faults.

4.2.3 Performance measurement

The performance measurement system can feed back various measurement indexes of the system in a variety of ways.

4.2.4 Security management

O&M system is a multi-user system. In order to ensure that multiple users can use the system safely and conveniently, the system adopts rights management.

4.2.5 Remote maintenance

Main functions of remote maintenance：

- The remote maintenance is safe and convenient, and the system software is characterized with its anti-virus, anti-hacking and anti-illegal attacks service.
- To provide remote maintenance capabilities.

5 Interface and Protocol

5.1 Interfaces

5.1.1 Interfaces

IK-HSS/HLR 100 provides an open, standard protocol interface for interaction or interworking with multiple devices. Figure 5-1 shows the interface between the IK-HSS/HLR 100 and each NE.

Figure 5-1 IK-HSS/HLR 100’s interfaces in the mobile communication network

Name	NEs	Protocol	Bear	Physical interface
S6a	MME	Diameter	IP	GE
Cx	IMS	Diameter	IP	GE
C	GMSC	MAP	IP	GE
D	MSC/VLR	MAP	IP	GE
Gr	SGSN	MAP	IP	GE
Northbound	BSS, OSS	MML，SOAP，RESTful	IP	GE

5.2 Signal and protocol

The main protocols supported by HSS/HLR are shown in Table 5-2

Table 5-2 HSS/HLR

Name of protocol	Description	The main standard it conform to
Diameter	To complete EPS (Evolved Packet switched system) user subscription data and authentication vector delivery, TA management and update.	IETF，RFC3588，Diameter Base Protocol
MAP	Application layer protocol	3GPP 29.002
TCAP	Transaction Capabilities Application protocol	ITU-T Q.771~Q.775
M3UA	MTP3 user application	ITU-T Q.711~Q.716
SCCP	network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities in Signaling System 7 telecommunications networks.	IETF, RFC4666
NTP	Network Time Protocol， which is used to support the time synchronization between the OMM of the HSS/HLR and the OMC network management system, so that the time of the entire network device keeps synchronized.	IETF, RFC1305, Network Time Protocol (NTP)

6 Design for reliability

6.1 Distributed design of software

The software are distributed architecture. As a result, single point failure can be avoided, and system reliability is also enhanced, which will ensure uninterrupted operation.

6.2 Load-sharing automatically

The software automatically balance the load of the same type of module to ensure that the same type of FE signaling processing unit and BE storage unit work under the same load to improve the stability of the system, thereby improving the reliability of the system.

6.3 Automatic fault detection and self-recovery capabilities

The techniques for fault detection and self-recovery：

- Automatic detection of hardware and software failures
- When the hardware or software of important components fails, the system will generate an alarm and execute a fault handler to eliminate the fault.
- For major faults that cannot be eliminated, manually switch to the backup system to take over the faulty hardware and software work without affecting system service processing.

6.4 Memory data management technology

All the user data is saved in the memory. The hard disk storage is only used as a mechanism for the permanent backup. Therefore, the fault of external storage device does not affect the normal service.

6.5 User data backup and recovery

Adopting automatic and multi-level backup techniques to ensure the reliability

Providing three levels of data backup and recovery mechanism. Storing user data into several physical node to improve the reliability:

- □ User data is stored in cache
- □ User data is backed up to the local hard disk from memory.
- □ User data is backed up from memory to disk array.

There are three ways to recover data:

- □ Recover data from the in-memory cache.
- □ Recover data from the local hard disk.
- □ Recover data from the disk array.

7 Technical Index

7.1 Performance index

HSS/HLR’s performance indexes are shown in figure7-1

Figure7-1 HSS/HLR Performance Indexes

Parameter	Index
Max number of subscribers	10 Million
Bearer of network	IP
Max number of diameter signal links(Single FE)	20
Max number of SCCP links(Single FE)	50
Max processing speed of signal simultaneously	500/S

In the fundamental configuration, the hardware specification of Section 3.1.1 is adopted, and the FE signaling processing unit and the BE storage unit are independently deployed by two servers to support 500K users.

For millions of users and above, the FE unit and BE unit are overlaid to support larger capacity.

7.2 Reliability index

As is show in diagram 7-2

说明

The following index are based on disaster-tolerant mode

Parameters	Index
Returning rate of systems	≤0.3％
Availability	≥99.9999%
Fault detect rate	＞95%
Mean time to restore（MTTR）	＜1h
Mean service disruption time annually	＜30sec
The period from power on to operation	≤8min
Success rate of switcing to redundancy components	＞95%
Single board switch time	≤10sec

8 Abbreviations

3

3GPP	3rd Generation Partnership Project

A

AAA	Authentication, Authorization and Accounting
AC	Authentication Center

B

BE	Back End
BMC	Baseboard Management Controller

C

CGL	Carrier Grade Linux
CPU	Central Processing Unit

CS	Circuit Switched Domain
D	
DCI	DS Call Interface
DSU	Data Service Unit
DRU	Data Routing Unit
E	
EMC	Electromagnetic Compatibility
ETS	European Telecommunication Standards
ETSI	European Telecommunications Standards Institute
F	
FC	Fiber Channel
FCC	Federal Communications Commission
FCP	Fiber Channel Protocol
FE	Front End
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
GSM	Global System for Mobile communications
GUI	Graphic User Interface

H

HCF	HSS Control Function
HLR	Home Location Register
HMF	HSS Management Function
HSF	HSS Signaling Function
HSS	Home Subscriber Server

I

IA	Intel Architecture
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force;
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector

L

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMT	Local Maintenance Terminal

LTE	Long Term Evolution
M	
MCI	Message Call Interface
MME	Mobility Management Entity
MML	Man-Machine Language
MRTIE	Maximum Relative Time Interval Error
MSC	Mobile Switching Center
MSISDN	Mobile Station International ISDN Number
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
N	
NE	Network Element
NEBS	Network Equipment Building System
NTP	Network Time Protocol
O	
OM	Operation and Maintenance
OMU	Operation and Maintenance Unit
OPEX	OPeration EXpenditure
OSTA	Open Standards Telecom Architecture

P

PCI	Peripheral Component Interconnect

Q

QoS	Quality of Service

R

RAID	Redundant Array of Independent Disks
RFC	Remote Feature Control
PGW	Provisioning Gateway

S

SAE	System Architecture Evolution
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDM	Subrack Data Module
SIGTRAN	Signaling Transport
SMB	Sub-miniature B
SMM	Shelf Management Module
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SVGA	Super Video Graphics Array
SWI	Switch Interface Unit

SWP	Sliding Window Protocol
SWU	Switching Unit
T	
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
U	
UDP	User Datagram Protocol
UI	Unit Interval
UMTS	Universal Mobile Telecommunications System
UPB	Universal Process Blade
USB	Universal Serial Bus
USCDB	Unified Subscriber Center DataBase
USI	Universal Service Interface
V	
VGA	Variable Gain Amplifier
VLR	Visitor Location Register
X	
XML	Extensible Markup Language