KIATEL

KSS200 NGN/IMS Platform
System Description

Ver. 1.4

1397
2018

KIATEL *KSS200* Carrier Grade

NGN/IMS Platform

www.kiatelco.com

About This Manual

This manual applies to KIATEL *KSS200* NGN/IMS Platform and introduces product characteristics, system architecture, interfaces signaling and protocols, OSS-BSS system, services and functions, networking and applications, reliability and security design, technical specifications and environmental requirements of *KSS200*.

Intended Readers

The manual is intended for the following readers:

- NGN/IMS network planning experts
- NGN/IMS network administrators
- NGN/IMS system engineers

Notice

Table of Contents

Preface: An introduction to NGN/IMS

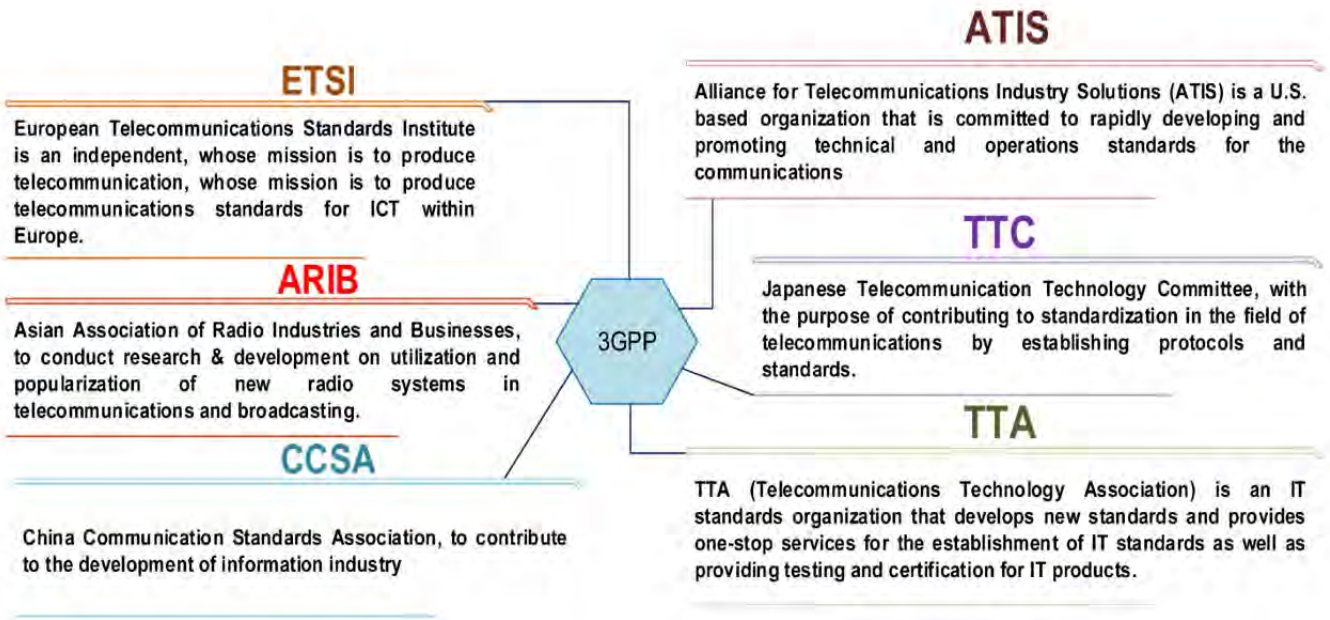
This chapter gives an overview of NGN/IMS, including how it can help telecommunication operators to achieve their goal of delivering advanced and innovative services, with reference to KIATEL experiences in near 30 years network implementation for TCI and private networks.

The main topics discussed are:

- IMS standardization organizations
- IMS and Telecommunications Operators services
- NGN/IMS architecture
- KSS200 NGN/IMS platform layers
- KSS200 NGN/IMS platform Core Functions
- KSS200 NGN/IMS platform Service Layer Interfaces
- Registration and basic call flow in KSS200
- Developing and deploying applications in KSS200
- TISPAN Architecture in KSS200 NGN/IMS Platform

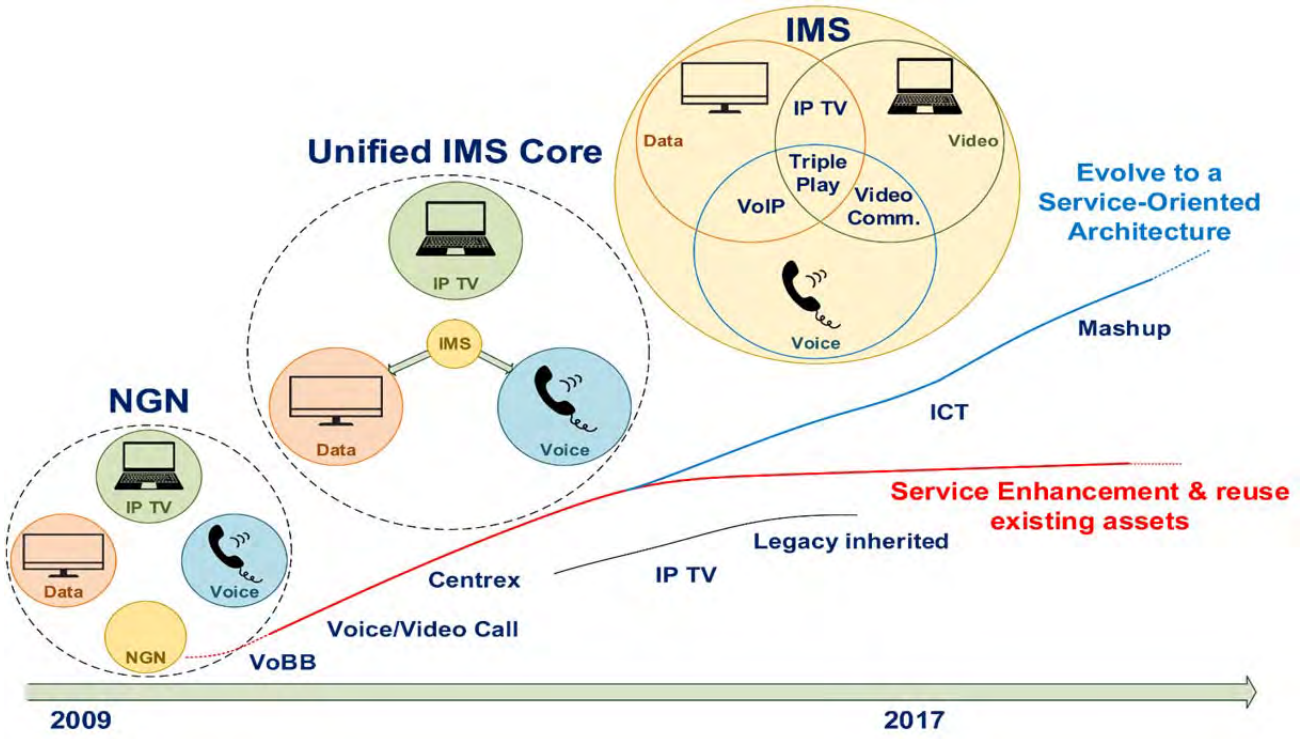
IMS standardization organizations

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in 1998 bringing together a number of telecommunications standardization bodies. Scope of 3GPP was to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile Systems based on GSM, GPRS and EDGE core networks and the radio access technologies. The European Telecommunications Standards Institute (ETSI) is an independent, non-profit organization, whose mission is to produce telecommunications standards for today and for the future is responsible for standardization of Information and Communication Technologies (ICT) within Europe.

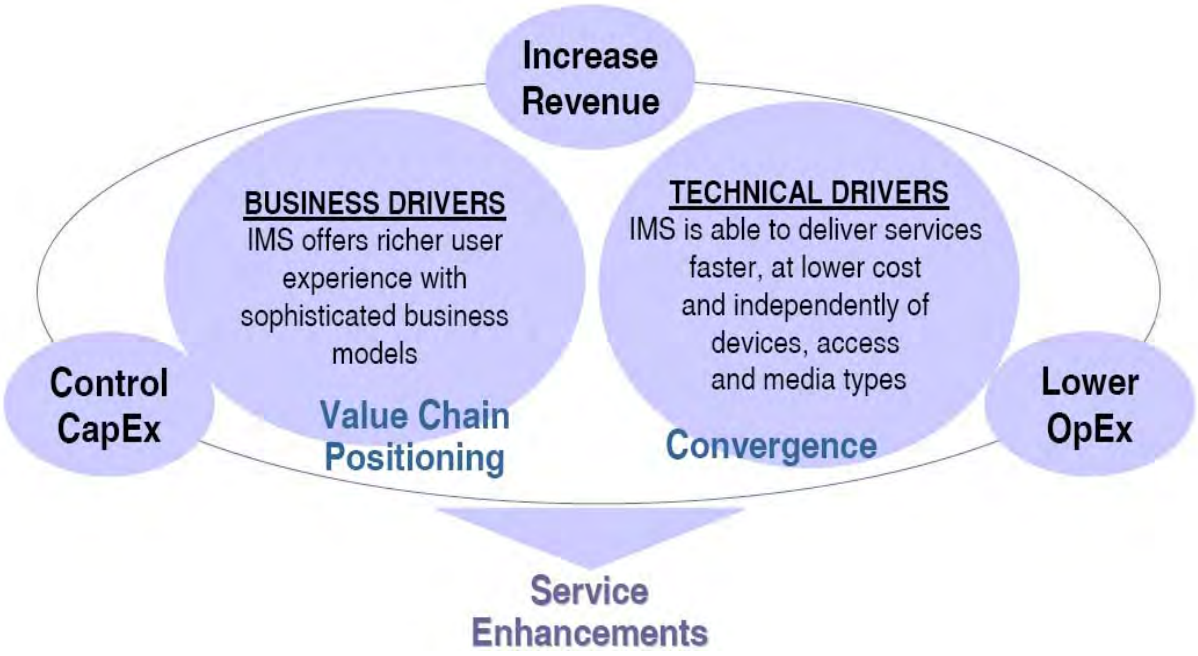


IMS and Telecommunications Operators services

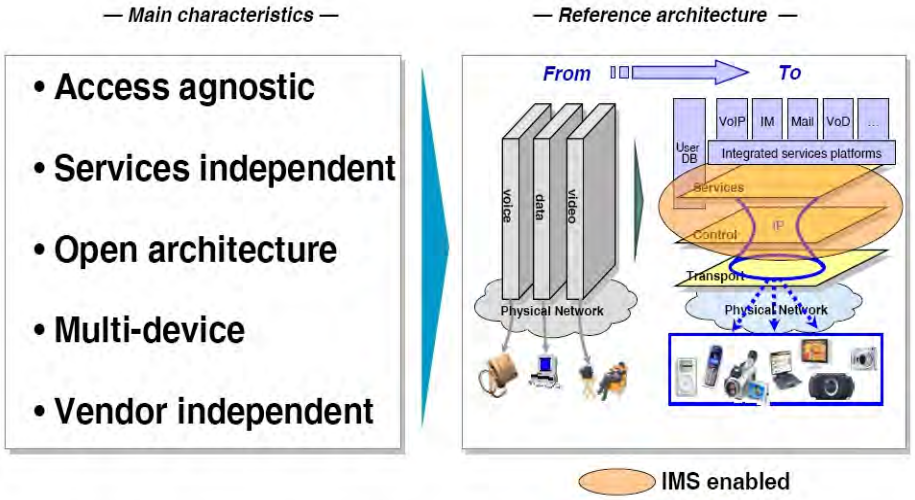
The IP Multimedia Subsystem (IMS) provides unified service architecture for all networks, leveraging the capabilities of IP.



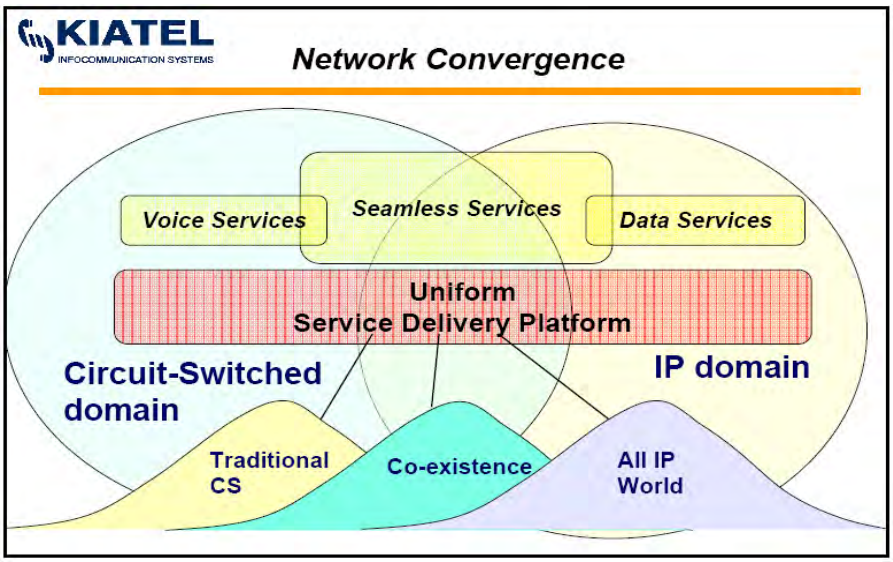
There are both business and technical drivers associated with IMS deployment that will bring benefits in service creation capabilities as well as in cost optimization.



IMS enables a packet-based network to provide multiple services on single Control/Service layers via different access network.



A (controlled) change of paradigm in the network architectures is a clear requirement for achieving the goal of delivering advanced and innovative services in an efficient way.



- services tightly associated with specific terminals and access networks
- layered networks with separated, non-integrated service control layers
- non-uniform user profiling
- IP pervasive but issues in guaranteeing QoS and charging for real-time, integrated services
- IMS introduces a structured, layered architecture with “standardized” interfaces
- clear path for integrating 3G world and “internet”
- ubiquitous access to all services from any device: IMS as access independent and all services developed on IMS are access agnostic
- uniform support for customer profiling, service access control and charging, integration with “legacy” networks

NGN/IMS Architecture

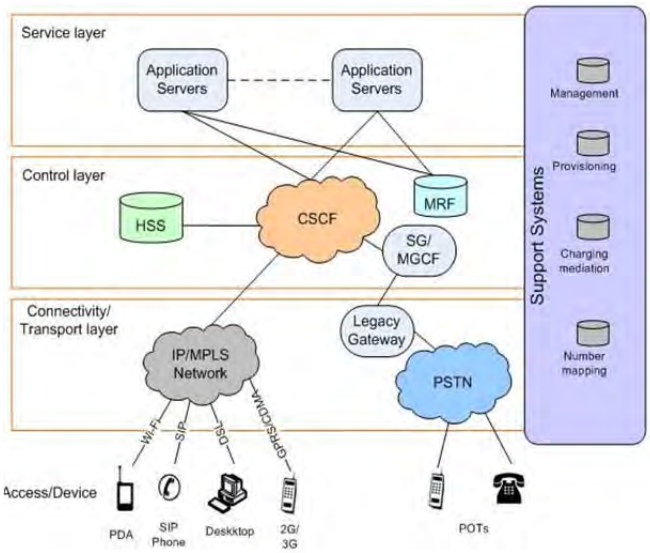
The *KSS200* platform has been based on concepts originally defined and standardized by the 3GPP consortium, thought to provide multimedia services exploiting an ALL-IP domain.

IP transport offers a cheaper and simpler way to carry multimedia sessions, compared to traditional circuit-switched networks. The first step toward the ALL-IP solution is the separation of the Control Layer from the Transport Layer, which can therefore be implemented exploiting the IP network.

IMS steps over redefining and standardizing the Transport Layer, Control Layer and Application Layer to exploit the IP infrastructure.

The *KSS200* platform is therefore an ALL-IP architecture. Moreover, standardization of functions and interfaces allow:

- ✓ Interoperability with other providers
- ✓ Convergence of services
- ✓ Flexibility and extensibility of the solution



KSS200 platform layers

The *KSS200* platform defines elements and functions on three layers:

1- Access and Transport Layer

This layer initiates and terminates the SIP signaling, setting up sessions and providing bearer services including the conversion from analogue or digital formats to packets.

Access and Transport layer also contains all of the media processing facilities including media gateways. These can be used to convert VoIP bearer streams to the PSTN TDM format. They can also be used to provide many media-related services such as conferencing, playing announcements, collecting in-band signaling tones, speech recognition, and speech synthesis.

2- Control Layer

This layer contains what is termed the Call Session Control Function (CSCF) which provides the endpoints for the registration and routing for the SIP signaling messages, enabling them to be routed to the correct application servers. The CSCF also enables QoS to be guaranteed. It achieves this by communicating with the transport and endpoint layer.

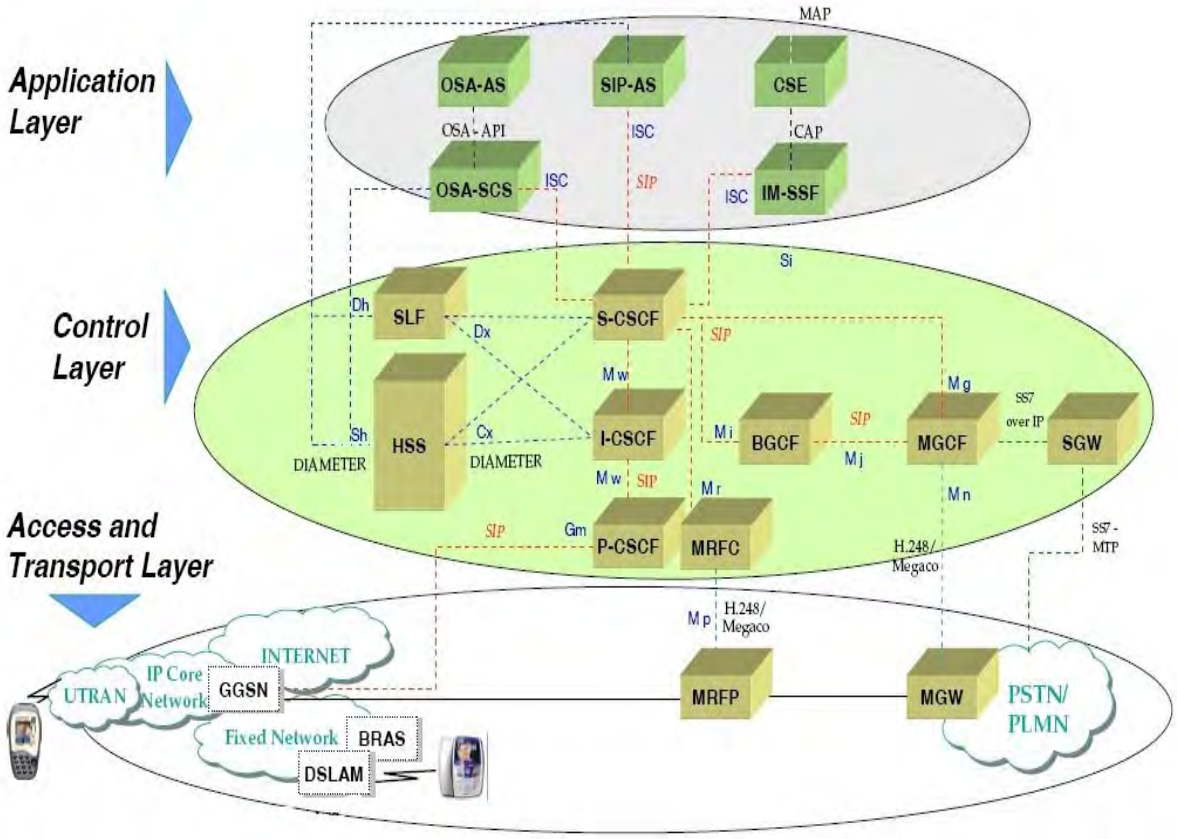
The layer also includes other elements including the Home Subscriber Server (HSS) that maintains the user profiles including their registration details as well as preferences and the like.

It includes the presence server essential to many interactive applications such as PoC. A further element of the session Control Layer is the Media Gateway Control.

3- Application Layer

The control of the end services required by the user is undertaken by the Application Server Layer. The IMS architecture and SIP signaling has been designed to be flexible and in this way it is possible to support a variety of telephony and non-telephony servers concurrently.

Within this layer there is a wide variety of different servers that are supported. This includes a Telephony Application Server (TAS), IP Multimedia - Service Switching Function (IM-SSF), Supplemental Telephony Application Server, Non-Telephony Application Server, Open Service Access - Gateway (OSA-GW), etc.



KSS200 platform Core Functions

KIATEL NGN/IMS core have been developed to play all roles in IMS standardized network. It has needed functions to represent a reliable and fully implementable network.

Main *KSS200* core functions are:

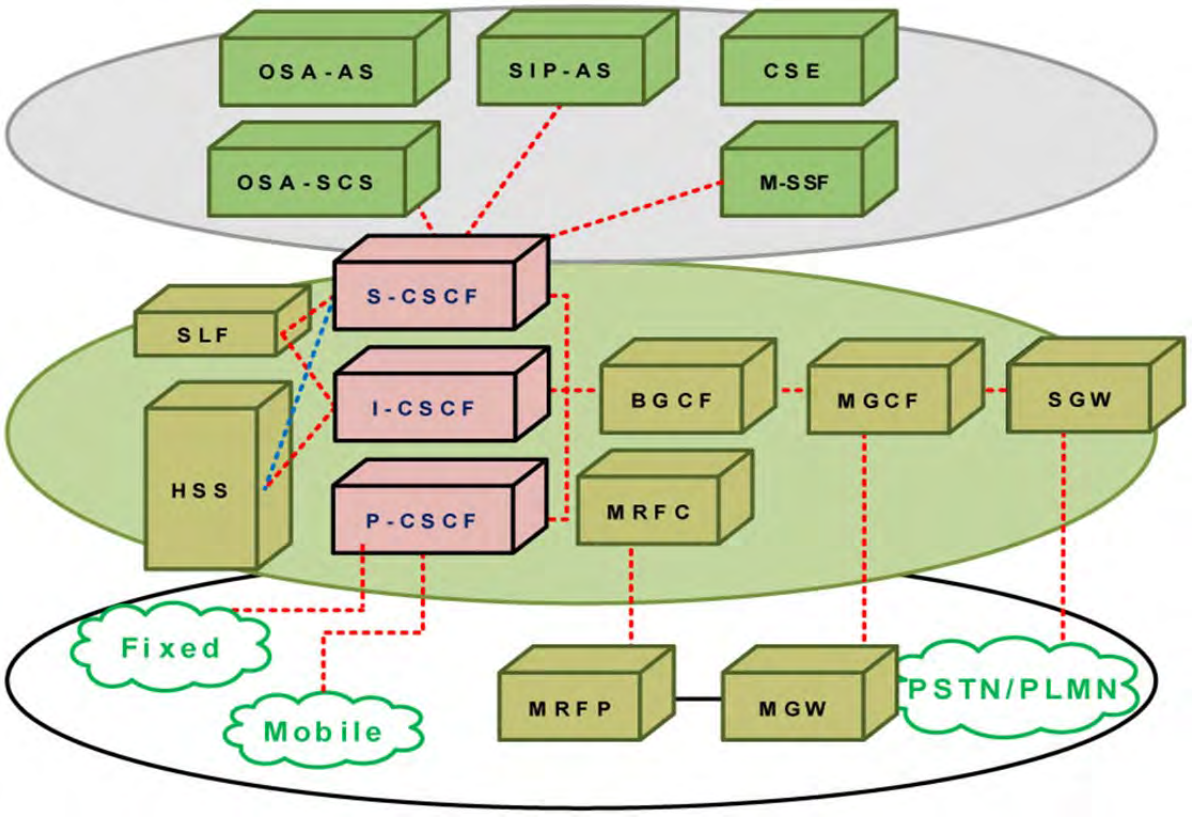
1- Call session control function (CSCF)

Several types of serving modules known as CSCF are used to process SIP signaling packets in the IMS domain:

- Proxy CSCF
- Interrogating CSCF
- Serving CSCF
- The CSCF elements are responsible for SIP session control and implements the logics for the following functions:
- user authentication
- call routing
- controlling the generation of call detail records (CDRs) for accounting purposes

Each network will typically have multiple CSCFs of each type, allowing load sharing and supporting increased reliability through the use of backup servers.

All the CSCF will use the session initiation protocol (SIP) as signaling protocol. Interaction with other domains using different protocols are performed by dedicated elements which allow protocol translation.



➢ Proxy Call Session Control Function(P-CSCF)

A P-CSCF is the first point of contact for the IMS terminal, and performs the following main functionalities:

- forwards the registration requests received from the UE to the I-CSCF

- forwards the SIP messages to the S-CSCF that administrate the user, whose address is defined during the registration

- forwards the request and the answers to the UE

The P-CSCF is assigned to an IMS terminal during registration, assigned either via DHCP, or in the PDP Context, and does not change for the duration of the registration.

- Sits on the path of all signaling messages, and can inspect every message

- Authenticates the user and establishes an IPsec security association with the IMS terminal. This prevents spoofing attacks and replay attacks and protects the privacy of the user.

- Can compress and decompress SIP messages using SigComp, which reduces the round-trip over slow radio links

- May include a PDF (Policy Decision Function), which authorizes media plane resources e.g. quality of service (QoS) over the media plane. It's used for policy control, bandwidth management, etc. The PDF can also be a separate function.

- Can be located either in the visited network (in full IMS networks) or in the home network (when the visited network is not IMS compliant yet).

P-CSCF acts as Session Border Controller in KSS200 platform.

- Interrogating Call Session Control Function (I-CSCF)

I-CSCF is a SIP function located at the edge of an administrative domain.

- Its IP address is published in the DNS of the domain (using NAPTR and SRV type of DNS records), so that remote servers can find it, and use it as a forwarding point (e.g. registering) for SIP packets to this domain.

- I-CSCF queries the HSS using the DIAMETER Cx interface to retrieve the user location (Dx interface is used from I-CSCF to SLF to locate the needed HSS only), and then routes the SIP request to its assigned S-CSCF.

- It can also be used to hide the internal network from the outside world (encrypting part of the SIP message), in which case it's called a THIG (Topology Hiding Inter-network Gateway).

- This "entry point" function is removed from the I-CSCF and is now art of the IBCF (Interconnection Border Control Function). The IBCF is used as gateway to external networks, and provides NAT and Firewall functions (pin holing).

- Serving Call Session Control Function (S-CSCF)

S-CSCF (Serving-CSCF) is the central node of the signaling plane. It is a SIP server always located in the home network. The S-CSCF uses DIAMETER Cx and Dx interfaces to the HSS to download and upload user profiles.

- It has no local storage of the user. All necessary information is loaded from the HSS.

- S-CSCF handles SIP registrations, which allows it to bind the user location (e.g. the IP address of the terminal) and the SIP address.

- It sits on the path of all signaling messages, and can inspect every message.

- It decides to which application server(s) the SIP message will be forwarded, in order to provide their services

- S-CSCF provides routing services, typically using ENUM lookups.

- It enforces the policy of the network operator.

- There can be multiple S-CSCFs in the network for load distribution and high availability reasons. It's the HSS that assigns the S-CSCF to a user, when it's queried by the I-CSCF.

2- Home Subscriber Server (HSS)

The HSS is the database of all subscriber and service data. HSS is the master user database that supports the IMS network entities that handle the call sessions:

- It contains the subscription-related information (user profiles), used by the control layer.

- HSS contains subscription information used by the service layer.

- It provides data used to perform authentication and authorization of the user.

- HSS can provide information about the physical location of user.

The HSS also provides the traditional Home Location Register (HLR) and Authentication Centre (AUC) functions. This allows the user to access the packet and circuit domains of the network initially, via IMSI authentication.

User Profile is composed by:

- User identity

- Allocated S-CSCF name

- Registration information and roaming profile

- Authentication parameters

- Control and service information

3- Subscription Locator Function (SLF)

An SLF is needed to map user addresses when multiple HSSs are used. The Subscription Locator Function (SLF) is used in a IMS network as a resolution mechanism that enables the I-CSCF, the S-CSCF and the AS to find the address of the HSS that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator.

The SLF expose Dx and Dh interfaces, which have the same syntax and semantic of the Cx and Sh interfaces provided by the HSS.

The SLF does not perform any logic on its interfaces, but replies to the requestor with a REDIRECT message, specifying the address of the HSS which is able to fulfill the request received. Both the HSS and the SLF communicate through the DIAMETER protocol.

4- Media Resource Function (MRF)

MRF is a source for network initiated and network managed media streams in the home network.

It is exploited for:

- Playing of announcements (audio/video)

- Multimedia conferencing (e.g. mixing of audio streams)

- Text-to-speech conversion (TTS) and speech recognition.

- Real-time transcoding of multimedia data (i.e. conversion between different codecs)

Each MRF is further divided into:

- An MRFC (Media Resource Function Controller) is a signaling plane node that acts as a SIP

User Agent to the S-CSCF and which controls the MRFP with a H.248 interface.

- An MRFP (Media Resource Function Processor) is a media plane node that implements all media-related functions.

5- Break out Gateway Control Function (BGCF)

The Breakout Gateway Control Function is the IMS element that selects the network in which PSTN breakout has to occur. A BGCF is used for calls from the IMS to a phone in a Circuit Switched Network, such as the PSTN or the PLMN.

BGCF forwards the signaling to the selected PSTN/PLMN network. If the breakout occurs in the same network as the BGCF then the BGCF selects a MGCF (Media Gateway Control Function) that will be responsible for inter-working with the PSTN, and forwards the signaling to MGCF. Otherwise it forwards signaling to BCGF of another operator network. The MGCF then receives the SIP signaling from the BGCF and manages the interworking with the PSTN network.

6- Public Switched Telephone Network (PSTN) Gateway

The interworking with the Circuit Switched network is realized by several components, for signaling, media and control functionalities:

I. SGW (Signaling Gateway)

SGW is the interface with the signaling plane of the Circuit Switched Network (CS). It transforms lower layer protocols as SCTP (which is an IP protocol) into MTP (which is a SS7 protocol), to pass ISUP from the MGCF to the CS network.

II. MGCF (Media Gateway Controller Function)

- Performs call control protocol conversion between SIP and ISUP

- Interfaces the SGW over SCTP

- Controls the MGW resources with a H.248 interface.

III. MGW (Media Gateway)

- Interfaces the media plane of the CS network, by converting between RTP and PCM.

- It can also perform media transcoding, when the codecs used do not match (e.g. IMS might use AMR, PSTN might use G.711).

7- Application Server (AS)

In *KSS200* Application Server host and execute services, and interface with the S-CSCF using SIP. This allows third party providers an easy integration and deployment of their value added services (VAS) to the KIATEL NGN/IMS platform.

Examples of services are:

- Caller ID related services (CLIP, CLIR ...)

- Call waiting, Call hold, Call pick up

- Call forwarding, Call transfer

- Call blocking services, Malicious Caller Identification

- Lawful interception

- Announcements, Digit collection

- Conference call services

- Location based services

- SMS, MMS

- Presence information, instant messaging

- Voice Call Continuity Function (VCC Service) or Fixed-Mobile Convergence

8- IP Multimedia - Service Switching Function (IM-SSF)

The IM-SSF is the node in the IMS domain which provides interworking between the SIP session control and the Intelligent Network of traditional networks.

It allowing service requests to be forwarded to legacy service delivery platforms such as IN-based SCPs. IM-SSF provides intelligent gateway functionality between the SIP-based IMS network and IN systems that use protocols such as CAMEL, INAP, AIN and MAP.

This functionality is critical for the rollout of new, converged offerings, while continuing service to

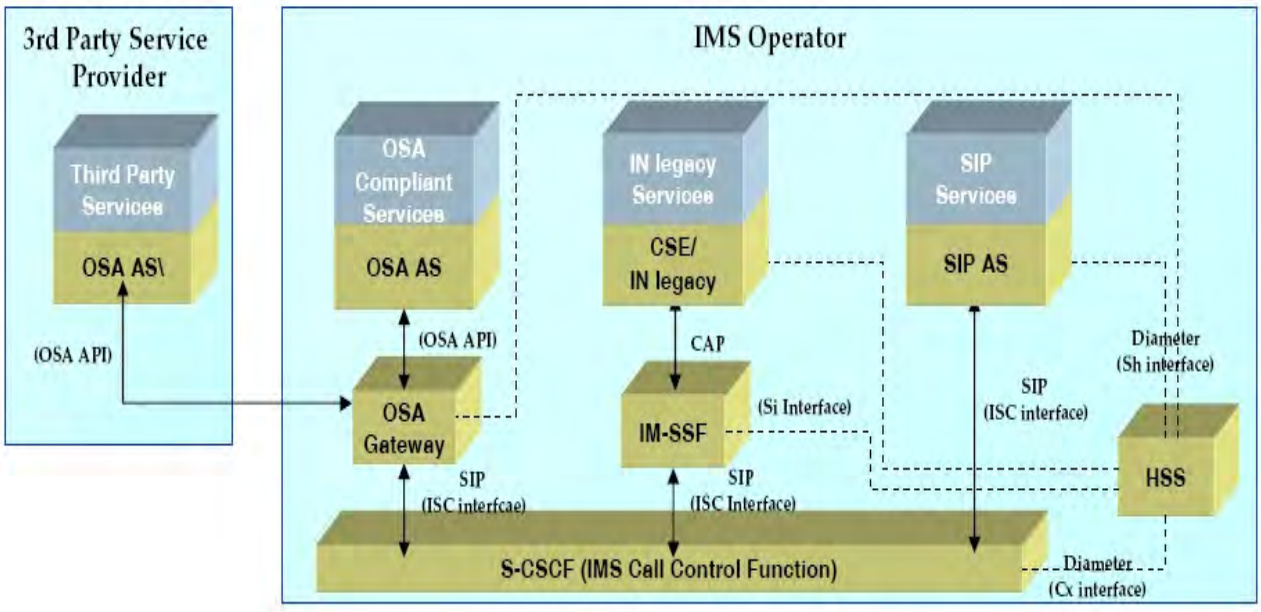
high-value customers.

The IM-SSF also enables access to subscriber information retrieved from the HSS over the Si interface using the MAP protocol.

KSS200 platform Service Layer Interfaces

The *KSS200* NGN/IMS platform control layer implements several interfaces toward the service layer which enables the user to access to service logics implemented by heterogeneous resources and application servers.

Diagram shows elements and interfaces which have been developed for communication between *KSS200* service layers.



- ISC (between S-CSCF and OSA Gateway/IM-SSF/SIP AS) allows receive/notify SIP messages from/to the S-CSCF to realize the service session control.

- Cx between S-CSCF and HSS is used to retrieve/update the subscriber profile data

- Sh between HSS/OSA- Gateway/SIP-AS is used to retrieve/update the subscriber profile data related to the service. The HSS is responsible for policing what information will be provided to each individual application server.

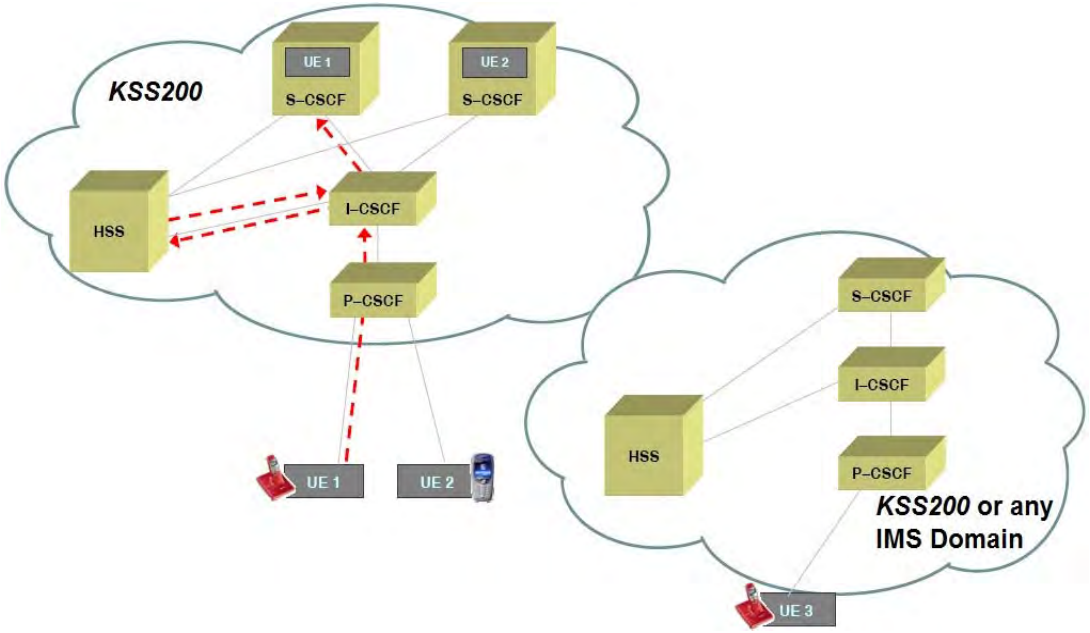
- Si between HSS and IM-SSF is used to retrieve/update the subscriber profile data related to IN services.

Registration and basic call flow in IMS

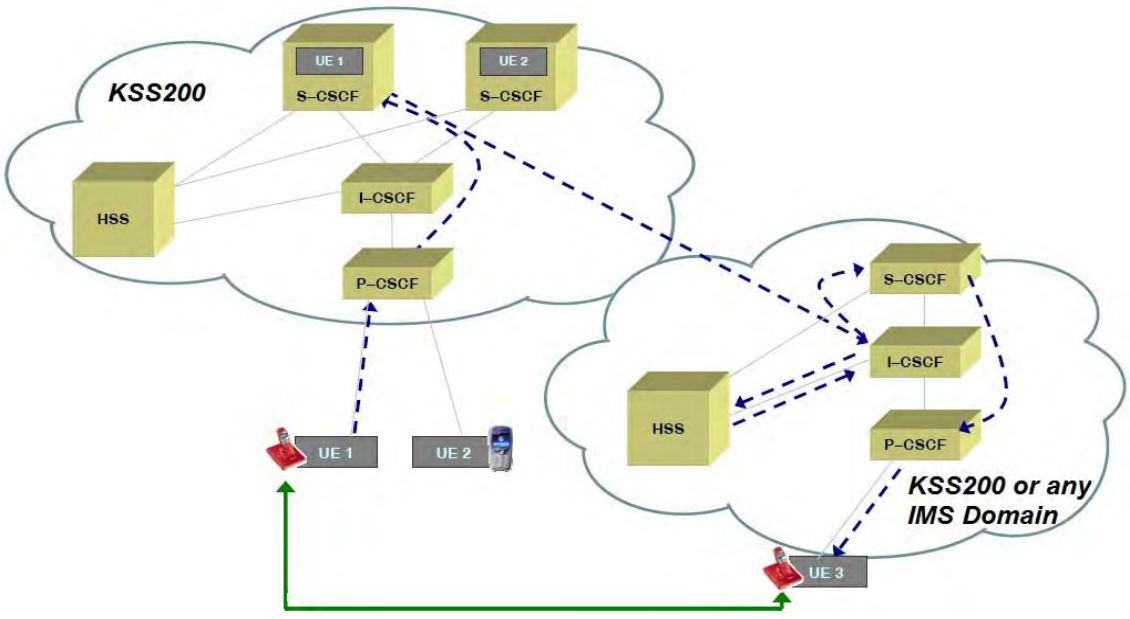
I. Registration

Before starting a multimedia session, the UE must be registered to the system.

The session origination procedures specify the signaling path between the UE initiating a session setup attempt and the Serving-CSCF that is assigned to perform the session origination service. This signaling path is determined at the time of UE registration, and remains fixed for the life of the registration.

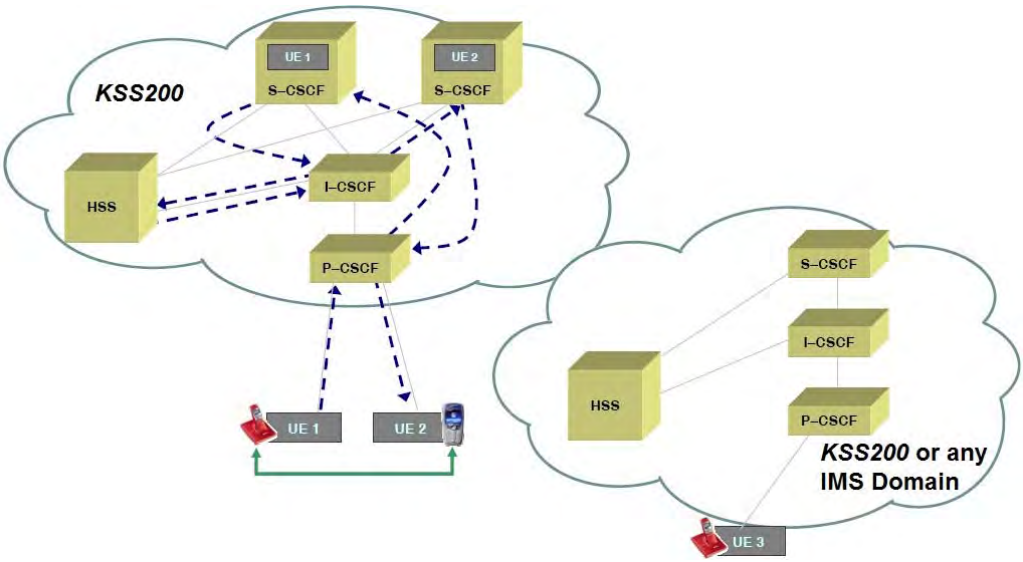


II. Session setup for UEs in different IMS domains



III. Session setup for UEs in same IMS domains

The session origination procedures specify the signaling path between the UE initiating a session setup attempt and the Serving-CSCF that is assigned to perform the session origination service. This signaling path is determined at the time of UE registration, and remains fixed for the life of the registration.



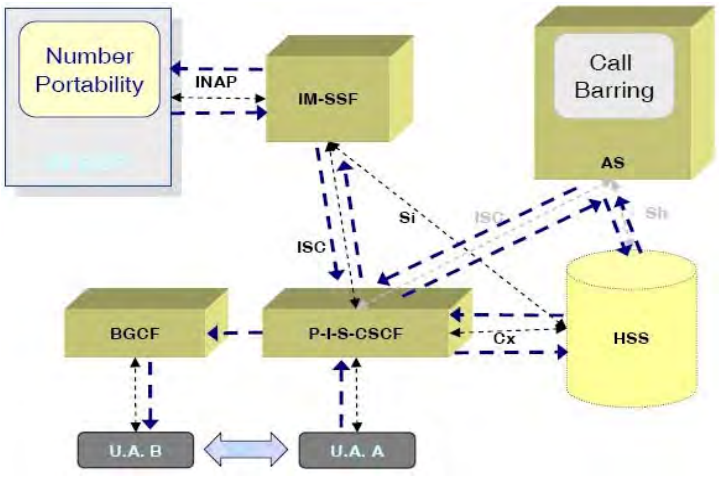
IV. Call flow with services like Call Barring & Number portability

User A initiates a call to a number that has been ported to an external network.

User A has the Call barring service, which prevents him to call 1xx numbers; hence the S-CSCF triggers the Application Server to apply the CB logic. The AS retrieves the profile associated to User A from the HSS, performs the service logic, and sends back the message to the S-CSCF allowing the call. Call control comes back to the CSCF, which interrogates the HSS and recognizes the dialed number has been 'ported' to an external network. The SCSCF forward the request to the IM-SSF to apply the Number Portability service on the Intelligent Network.

The IM-SSF forwards the request to the SCP using INAP, which responds with the new Routing Number of the User B. The IM-SSF responds to the S-CSCF with the new number.

The CSCF completes the signaling phase forwarding the call to the BGCP, and finally to the called party User B.

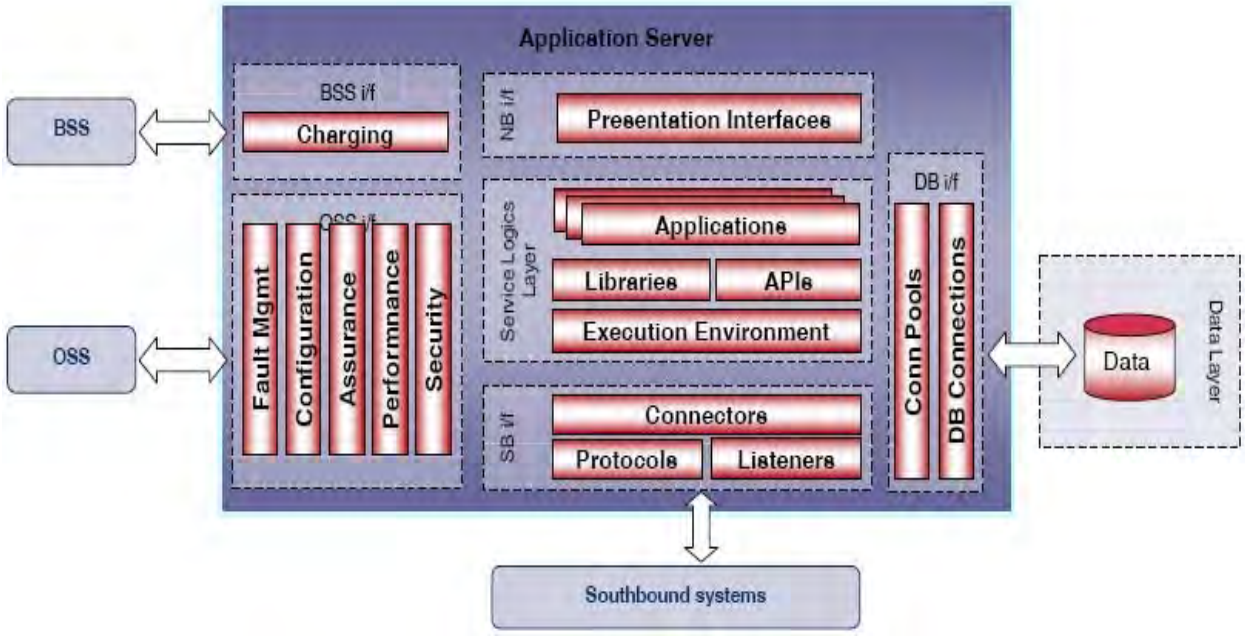


Developing and deploying applications in IMS

I. Applications Container Architectures

In *KSS200* applications deployed on ASs are the basic blocks used to develop services. Services can be provided directly by a single application or can be the result of the orchestration of several applications, eventually hosted on different Application Servers.

Application Servers are the execution environments for applications, providing framework facilities such as protocols and interface support, database connections, security, monitoring and more…



Application Containers can be based on different paradigms, depending on the structure of the application execution environment and on the technique used to convey messages between different components inside the application server.

Two main execution environments types are currently exploited to develop application servers:

Message Driven, Servlet Containers	Event Driven, SLEE
Synchronous execution: Logics are activated by requests received from the network.	**Asynchronous execution:** Requests generate events. Service logics are notified of raised events, and activate services.
Service model: Request/response Direct association between messages and Logics.	**Service model: Publish/subscribe** Requests have not a direct connection with service blocks.
Coarse grained: Does not allow managing same request in different way.	**Fine grained:** Allows more granularities in management of the requests**.**

II. SLEE Container

SLEE (Service Logic Execution Environment) architecture is based on an execution model with application hosted as independent service building blocks (SBB).

Each SBB can be triggered and activated by one or more events, generated inside the SLEE. Interfaces are realized implementing Resource Adaptors, which manage listeners and protocols, and are able to raise specific events when interrogated by network requests.

The SLEE environments manage the entire lifecycle of events, applying subscribe/notify and routing rules between RAs and SBBs.

This kind of service environment has been specifically thought for TelCo operators, as allows following features:

- Modular development of service logics.

- Easy combination of different Service Block to provide convergent services.

- Resource Adapters can be added or extended without modifying the service logics implemented inside SBBs.

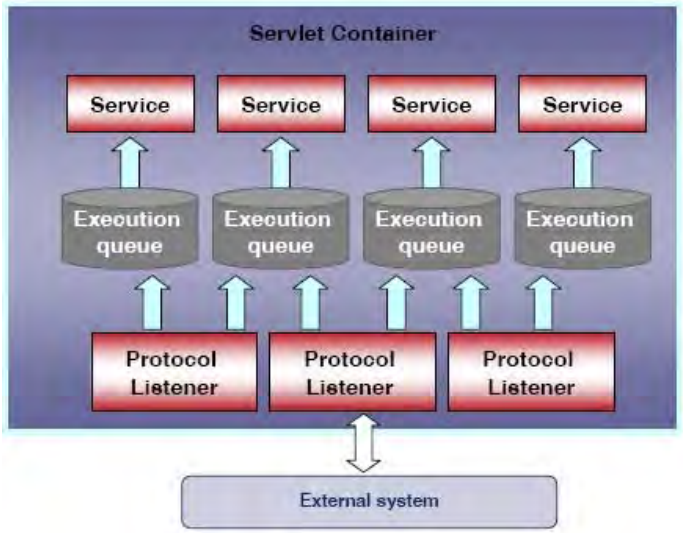
III. Servlet Container

Servlet Containers are execution environments which bind the execution of service logic to the receiving of a particular request.

- Service Logic lifecycle is entirely managed by the environment.

- Requests are associated to service logics depending on the type of message received (servlet model).

- Service Logics are activated synchronously with request elaboration.



- Combination of service logics is managed redirecting messages inside the container.

The servlet paradigm can be used implementing adaptors for several protocols, allowing the development of fast network oriented services:

- Service Logics are directly connected to network messages.

- Can manage queuing, overloading and prioritization of requests.

- Protocols and interfaces can be added implementing new listeners.

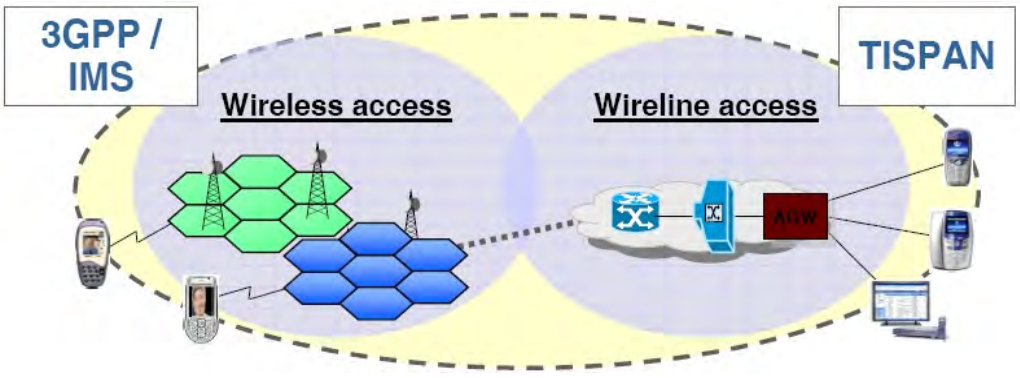
TISPAN Architecture in *KSS200* NGN/IMS Platform

The Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN) is a standardization body of ETSI, specializing in fixed networks and Internet convergence. TISPAN is the ETSI core competence center for fixed networks and for migration from switched circuit networks to packet-based networks with an architecture that can serve in both to create the Next Generation Network.

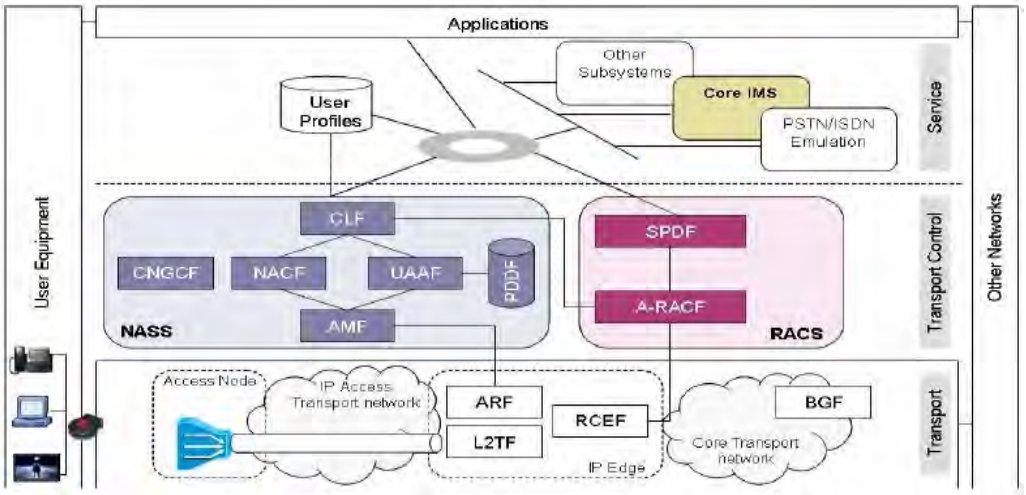
This focus on fixed accesses together with the choice of using the IMS network in the core architecture led to new requirements and to an evolution of the original IMS solution.

TISPAN and 3GPP are now working together to define a harmonized IMS-centric core for both

wireless and wireline networks, enabling new convergent accesses and services.



KIATEL follows this policy to fulfil requirements of future networks and making this convergence achievable. The NGN standard functional architecture, defined by TISPAN, is composed by a "service layer" and a "transport-layer" both based on IP.



This subsystem-oriented architecture enables the addition of new subsystems over the time to cover new demands and service classes. This architecture has been implemented in *KSS200* and ensures that the network resources, applications, and user equipment are common to all subsystems and therefore ensure user, terminal and service mobility to the fullest extent possible, including across administrative boundaries.

KSS200 NGN/IMS platform is based on a subsystem–oriented architecture, enabling the insertion of new subsystems over the time to cover new demands and providing the ability to import/adapt subsystems defined within other standardization bodies.

Components of layers in this platform are:

Transport Layer Components	**Service Layer Components**
IP Connectivity is provided to the user equipment by the Transport Layer.	Core IP Multimedia Subsystem (IMS)
The transport layer comprises a transport control sub layer on top of transfer functions.	PSTN/ISDN Emulation Subsystem (PES)
The transport control sub layer is further divided in two subsystems: • Network Attachment Subsystem (NASS) • Resource and Admission Control Subsystem (RACS).	Other subsystems (e.g. streaming subsystem, content broadcasting subsystem etc.) and applications.
	Common components used by several subsystems, such as: -Charging Functions -User Profile Management -Security Management -Routing Data Bases (e.g. ENUM)

Network Attachment Subsystem (NASS)

NASS is a Transport Control layer element defined by ETSI /TISPAN. NASS system provides integrated and centralized management of user's access to the network. NASS makes possible to expose towards upper-layer systems user's presence information's and at the same time apply policies to control network access based on various users' profiles

NASS functionalities cover:

- Authentication and authorization

- Dynamic or static IP address assignment

- Access devices configuration

- Assignment of the proxy to access to IMS services (i.e. P-CSCF)

- Access parameters management (i.e. QoS, bandwidth)

- Management of network presence towards application layers

- Mobility features

Resource and Admission Control Subsystem (RACS)

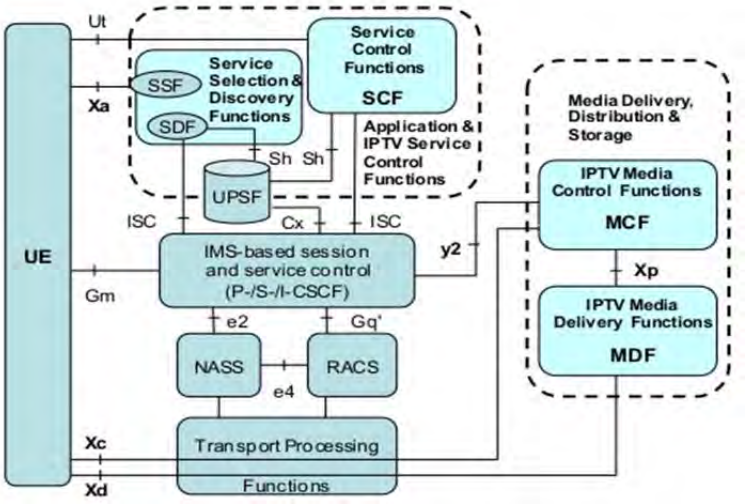
RACS is the TISPAN element in the transport control layer responsible of policy control, resource reservation and admission control.

RACS main functionalities are:

- Admission Control, which enforce limitations to the access to network resources, e.g. applying bandwidth thresholds.

- Resource reservation, which enables the reservation for a given period of the resources needed to provide a service. For example, a voice call will reserve a given bandwidth over the entire circuit before the call is initiated.

- Policy Control, enable enforcement of policies on the resource exploitation.



Chapter 1 System Introduction

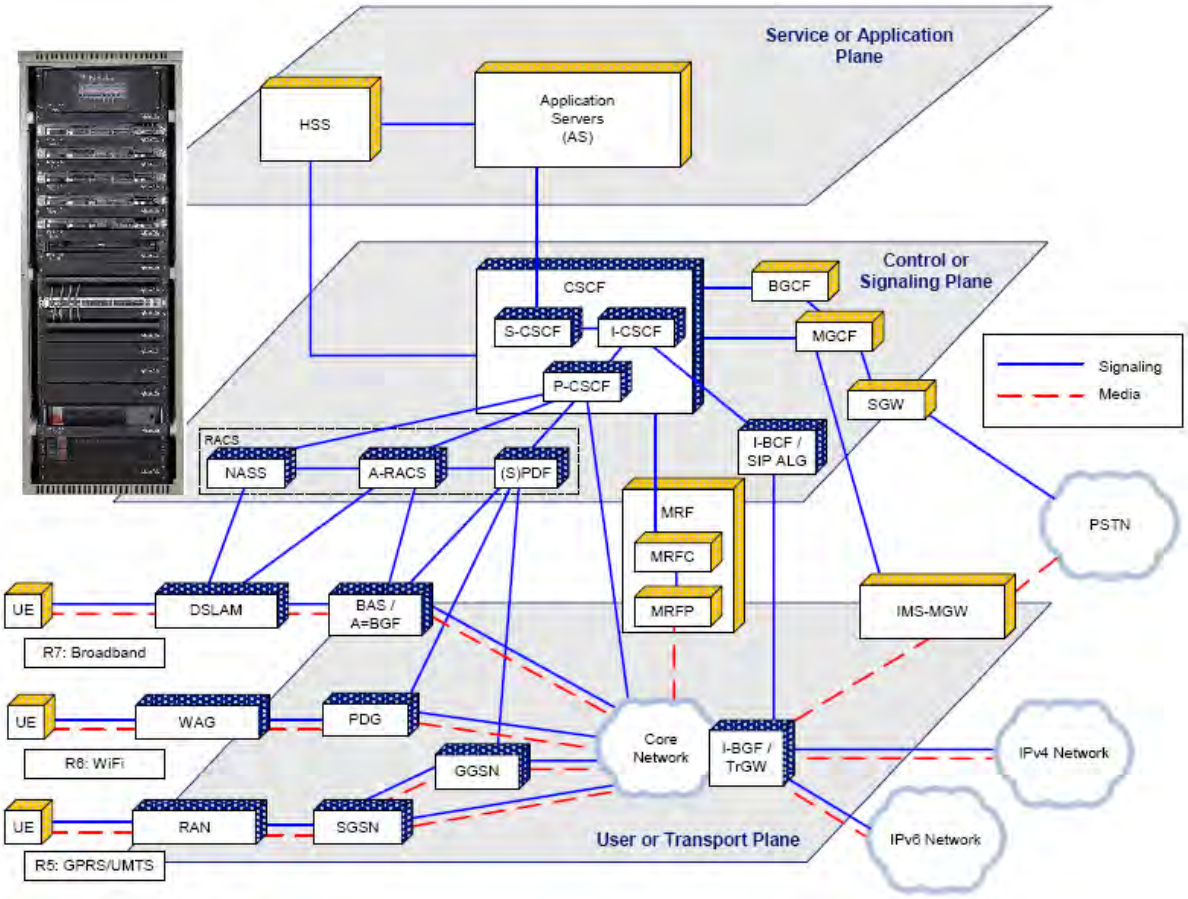
1.1 Introduction to KIATEL NGN/IMS Platform

1.1.1 Overview of KIATEL NGN/IMS Platform

NGN is a service-driven network, which realizes a relatively independent service system by separating service from call control, as well as call control from bearer, thus enabling service independent of network. NGN employs open and integrated network architecture.

With abundant service provisioning capabilities, NGN is able to provide a variety of services, such as voice, data and multimedia services, or integrated services.

Depending on the *KSS200* NGN/IMS platform proposed by KIATEL, NGN comprises three planes, namely edge access, network control and service management. The network architecture is shown in Figure 1-1.



1.1.2 Network Components

I. Edge access layer

Edge access layer is used to connect subscribers and terminals to the network by a variety of means and convert the original information format to the suitable one that can be transferred over the network.

• Integrated Access Device (IAD): It is a type of subscriber access device used in the NGN

architecture. It introduces data, audio, video and other services of the subscribers to the packet-based network. Each IAD provides many subscriber ports.

• IP Access (IPA): It provides subscribers with a diversity of service access, such as analog subscriber access, Integrated Services Digital Network (ISDN) access, V5 access and x Digital Subscriber Line (xDSL) access.

• IP Phone: It is a type of multimedia terminal device supporting the Session Initiation Protocol (SIP) or H323.

• Signaling Gateway (SGW): It is located at the interface layer of the Signaling System No. 7 network and the Internet Protocol (IP) network, achieving the signaling conversion function between the Public Switched Telephone Network (PSTN) and the IP network.

• Trunk Gateway (TGW): It is resident between the circuit switched network and the IP packet switched network. It provides functions of format conversion between Pulse Code Modulation (PCM) signal streams and IP media streams.

• Residential Gateway (RGW): It implements the functions of media stream format conversion and signaling conversion. It can act as a TGW, built-in SGW or IPA. It can connect a variety of devices including PSTN exchange, Private Branch Exchange (PBX), access network, Network Access Server (NAS) and Base Station Controller (BSC).

II. Network control layer

Network control layer is responsible for implementing call control. Its core technology is soft switching, which is used to achieve basic real-time call control and connection control functions.

SoftSwitch is the core equipment of NGN and mainly implements call control, media gateway access control, resource allocation, protocol processing, routing, authentication, and charging functions, and provides subscribers with basic voice services, mobile services, multimedia services and Application Programming Interfaces (APIs).

III. Service management layer

Service management layer is mainly used to provide supplementary value added services and operation support based on established calls.

• OSS-BSS is the acronym of Operation Support System- Business Support System, which includes two parts: Network Management System (NMS) for managing the NGN network elements in a centralized way, and integrated charging system.

• Policy Server: It is used to manage the policies of the users, such as Access Control List (ACL), bandwidth, traffic, and QoS.

• Application Server: It is responsible for generating and managing logics of various value added services and intelligent network services, and providing innovation Platform for developing third-party services by means of open APIs. As a physically separated component, Application Server is independent of the equipment which resident on the network control layer. This contributes to the separation of service from call control and is beneficial to the introduction of new services.

• Location Server: It is used to dynamically manage the routes between the SoftSwitch equipment in NGN, indicate reachability of the destinations of calls, ensure the best efficiency of the call routing table, prevent the routing table from being oversized and impractical, and abate the complexity of routes.

• Diameter Server: It is used to implement AAA services and manage subscriber authentication,

password encryption, service selection and filtering, and call charging in a centralized way.

• Media Resource Server (MRS): It is used to enable the media processing functions in the basic and enhanced services. The functions include service tone provision, conference service, Interactive Voice Response (IVR), recorded announcement and advanced tone service.

• Service Control Point (SCP): It is the core component of the Intelligent Network (IN), and is used to store subscriber data and service logics. According to the call events reported by Service Switching Point (SSP), SCP starts an appropriate service logic, retrieves the service database and the subscriber database based on the started service logic, and then sends proper call control instructions to the corresponding SSP to instruct the SSP how to perform next, thus realizing various intelligent calls. That is the main function of SCP.

1.1.3 *KSS200* Major Technical Features

I. Open and distributed network architecture

KSS200 has an open and distributed network architecture where service is separated from call control and call control is separated from bearer. Thus service is independent of network. Through open protocols and interfaces, a variety of services can be provided flexibly and rapidly, and individual subscribers can customize their own service features without considering the network structure and the terminal type of the bearer services.

II. High-speed and packet switched core bearer

The packet switched core bearer network speeds up the integration of the telecommunication network, computer network and cable TV network. Meanwhile, the high-speed core bearer network supports a diversity of services including voice service, data service and video service.

III. Independent network control layer

The network control layer, that is, SoftSwitch, employs an open and independent control Platform to isolate call control from media gateways. The independent network control layer implements by software the basic call control functions including call routing, management control and signaling interworking, so that service suppliers can customize bearer services and control protocols. The network control layer also provides open APIs to facilitate a third party to provide services in a rapid, flexible and efficient way.

IV. Internetworking and gateways

KSS200 can interwork with PSTN, Public Land Mobile Network (PLMN), 3rd Generation (3G), IN, Internet and other networks by means of access media gateway, trunk media gateway and signaling gateway. The interworking enables NGN to inherit all services from the original networks efficiently.

V. Diversified access modes

Ordinary subscribers can access the network through intelligent packet voice terminals and multimedia terminals. Enterprise users and corporate users can be connected to the network through access media gateways and integrated access devices, which fully meets the requirements of

individual users for voice, data and video services.

1.2 *KSS200* roles in NGN

KIATEL *KSS200* NGN/IMS platform (hereinafter referred to as *KSS200*) adopts advanced software and hardware technologies and owns abundant service provisioning capabilities and powerful networking capabilities. *KSS200* is applicable to the network control and service management layers of the Next Generation Network (NGN).

1.3 Location of *KSS200*

As a large-capacity and high-performance NGN/IMS platform, *KSS200* is applicable to the network control and service management layers of NGN and implements call control and connection management of voice, data and multimedia services as well as applications management based on the IP network.
KSS200 owns abundant service provisioning capabilities and powerful networking capabilities. On the way of the development and integration of the traditional PSTN networks to NGN, *KSS200* can be used as main core for controlling end offices (C5 office), tandem offices, toll offices (C4 office), gateways and so on.

1) *KSS200* is fully compatible with all service capabilities of PSTN exchanges and supports a variety of protocols including Media Gateway Control Protocol (MGCP), H.248(Megaco), V5.2, SS7, SIP and H.323. Traditional PSTN telephone terminals and ISDN terminals (via gateway), MGCP packet terminals, H.248 packet terminals, SIP packet terminals and H.323 packet terminals can be connected to *KSS200* which is capable of a diversity of service provision such as voice, data and multimedia.

2) *KSS200* supports the traditional PSTN signaling, such as Signaling System No. 7 (SS7), R2 signaling and V5.2 protocol. Coordination with SGW, TGW, RGW and other gateways enables *KSS200* to own various access networking capabilities and trunk networking capabilities which the existent PSTN exchanges have.

3) *KSS200* supports black and white lists, authentication, authorization and accounting of users, call interception and so on.
4) *KSS200* supports the Message Transfer Part (MTP) and the Message Transfer Part 3 - User Adaptation Layer (M3UA) signaling which enables *KSS200* to serve as signaling gateway controller.

1.4 *KSS200* Features

1.4.1 Abundant Service Provisioning Capabilities

KSS200 not only supports the various service capabilities in the traditional PSTN and IN, but also provides value added services on the basis of the IMS architecture.
KSS200 has abundant service provisioning capabilities as follows:

1) Completely supports voice service capabilities in TDM switches which enables *KSS200* to provide basic voice services and supplementary services.

2) Proposes an optimized IP Centrex solution and supports IP Centrex subscribers, IP console and wide area Centrex services.

3) Supports the T.38 protocol and provides high-quality IP fax services.

4) Supports multimedia communication protocols including SIP and H.323 to provide videophone, application share, electronic whiteboard and videoconferencing services.

5) In cooperation with SCP intelligent platform, *KSS200* fully supports INAP and the traditional IN services, such as Free Phone (FPH), Account Card Calling (ACC), Virtual Private Network (VPN) and Universal Personal Telecommunication (UPT).

6) *KSS200* provides subscribers with diversified value added services, third-party services or customized services, such as Unified Messaging (UM), Instant Messaging (IM), Click To Dial (CTD), Click To Fax (CTF), and Presence.

7) Supports Internet Personal Number (IPN).

1.4.2 Powerful and Flexible Networking Capabilities

KSS200 provides open and standard protocol interfaces. *KSS200* not only supports a variety of NGN signaling protocols including MGCP, H.248, SIP, SIGTRAN, but also supports a number of traditional PSTN signaling systems such as SS7, R2 and V5.2. *KSS200* has powerful and flexible networking capabilities.

1) Supports both MGCP and H.248 as the media gateway control protocols, is able to interconnect with IADs, AGWs, TGWs and RGWs, and allows access to MGCP packet terminals and H.248 packet terminals.

2) *KSS200* is able to interwork with other IMSs and SIP application servers, and allows SIP packet terminals to access directly.

3) This platform is able to interconnect with traditional VoIP gateways and Multipoint Control Units (MCUs), and allows H.323 packet terminals to access directly.

4) *KSS200* supports V5.2 protocol and R2 signaling. In cooperation with RGW enables the access of PBX, NAS, access network devices and Base Station Controllers.

5) Via SGW, TGW and RGW it supports Telephone User Part (TUP) and ISDN User Part (ISUP) and is able to interconnect with Signaling Points (SPs) and Signaling Transfer Points (STPs) resident in the SS7 network, and provides SS7 trunks to interconnect with PSTN exchanges.

6) *KSS200* (Via SGW and RGW) supports Signaling Connection Control Part (SCCP), Transaction Capabilities Application Part (TCAP), and INAP and provides Service Switching Function (SSF).

7) This system supports M2UA, M3UA and MTP protocols Via SGW and RGW.

8) *KSS200* supports Simple Traversal of UDP through Network Address Translators (STUN). This is a Network Address Translation (NAT) protocol which enables enterprise networks to pass through NAT devices such as firewalls and access the IMS.

9) Supports the Simple Network Management Protocol (SNMP) and Man Machine Language (MML) interfaces to access the network management center.

10) Supports the File Transfer Protocol (FTP) and the File Transfer Access and Management Protocol (FTAM) to access the billing center.

1.4.3 Large Capacity and High Integration

As advanced hardware and software design technologies are employed, *KSS200* not only has modularized hardware architecture, but also owns a high processing capability and a large capacity on the carrier grade level.

1) The Busy Hour Call Attempt (BHCA) value of Main Core Server (MCS) and its redundant (BCS) independently are at least 1.4M.

2) *KSS200* represents 200,000 concurrent calls for 2,000,000 registered users.

3) *KSS200* is also characterized by high integration and has been configured in only 1 cabinet. The operation power consumption of the system is less than 1.5kW.

1.4.4 High Reliability

For the purpose of guaranteeing the high reliability of the system, a number of protective measures are taken in the hardware design, software design, system overload control and charging system of *KSS200*.Furthermore *KSS200* can work in a Multi Homing topology.

1) Hardware design: adopts active/hot standby mode, load sharing and redundancy configuration for the servers and optimizes fault detection and isolation techniques of the servers and the system to improve the maintainability of the whole system.

2) Software design: adopts hierarchical modularized architecture with protective performance, error tolerance capability and fault monitoring function.

3) System overload control: provides multi-level overload restrictions, dynamic resource allocation and traffic control to fully ensure the reliability of the system.

4) Charging system: OSS-BSS software developed by KIATEL is employed as *KSS200* charging system. OSS-BSS is configured with Hot RAID5 hard disk array to implement dual backup and mass storage of bill data.
Depending on a reliable prediction method, the Mean Time Between Failures (MTBF) of *KSS200* is at least 35 years and the interruption time of the system is lower than 0.6 minute yearly.

1.4.5 High Security

NGN is an open and distributed network where open protocols and interfaces enable it to interwork with various NGN network components. Networking applications over NGN are very flexible. However, this openness also results in inevitable network security issues as IP network is characterized by seamless connection.
For the purpose of ensuring the security of the network and all authorized subscribers, *KSS200* is structured with a perfect security design against malicious attack, illegal registration, anonymous

calling, wiretapping, stealing accounts and other illegal acts.

1) Security in the aspect of networking applications
• Protocol interfaces that are not in use can be closed.
• Supports the complete Internet Protocol Security extensions (IPSec) protocol to prevent the system from being attacked by means of Denial of Service (DoS).

2) Security in the aspect of protocols and communications supports the security of the protocols and the encryption processing of the protocol packets, including MGCP, H.248, SIP and H.323.

3) Security in the aspect of data

• Supports the real-time data backup mechanism between the active (MCS) and redundant (BCS) servers.

• Supports the mechanism of automatically backing up the information of the Main Data Base Server (MDBS) to the Backup Data Base Server (BDBS).

• Supports the automatic backup mechanism of the bills in OSS-BSS & Billing Server (BOBS).

4) Security in the aspect of subscribers

• Supports certification and authentication on all the devices attempting to access *KSS200*.

• Supports encryption and ciphering of certification information.

5) Security in the aspect of operations and maintenance

• Supports login security management pertaining to both account and workstation IP address.

• Supports multi-level user authority management.

1.4.6 Smooth Expansion Capability

KSS200 is designed with a smooth expansion capability in the aspects of hardware design and system processing capability, with the potential expansion requirements of the customers taken into account.

1) Hardware design: The *KSS200* platform has a modular structure. By expansion of servers in the mode of building blocks (servers are interconnected through network switch), many core and data base servers can be configured freely and the customers' requirements for smooth expansion can be satisfied.

2) System processing capability: The BHCA value of *KSS200* is at least 1.4M. Enough space is reserved for future service expansion, so increasing service or expansion requirements of the customers can be satisfied.

1.4.7 Optimized Charging Capabilities and Bill Management Functions

KSS200 has optimized charging capabilities and not only supports to charge voice, data and multimedia services with several charging modes and bill types, but also provides optimized bill management functions. The main characteristics are as follows:

1) Supports multiple charging modes based on call duration, bearer capability, time segment, time category, or chargeable party (calling, called or third party).

2) Supports charging of supplementary services.

3) Supports charging of prepaid card.

4) Supports to charge Centrex groups.

5) Supports quota restricted calling and timed restriction.

6) Supports a variety of bill types, such as detailed bill, subscriber charging meter bill, trunk charging meter bill, charging meter statistical bill, trunk occupation duration statistical bill, alarm bill, failure bill, complaint bill and intelligent bill.

7) Supports bill restricted calling functions.

8) Supports to store bills depending on respective modules, services and time.

9) Supports the automatic backup, dumping, sorting and format conversion functions of bills.

10) Supports standard FTP and FTAM charging interfaces.

1.4.8 Excellent Traffic Measurement Functions

KSS200 provides excellent traffic measurement (traffic statistics) functions and supports multiple measurement indices and flexible measurement tasks. *KSS200* adopts lists and graphics to display the performance data in real time, for the purpose of fully reflecting the traffic loading information and running and operation of the equipment.

1) *KSS200* has traffic measurement and record functions. Many statistical tasks can be registered and conducted at the same time regarding requirements of the customer.

2) The traffic measurement item can be scheduled and the testing time can be preset, so that the measurement can be started and stopped at the specified date and time automatically. The scheduled measurement item can also be cancelled.

3) For the scheduled traffic measurement item, the system supports more than 12 statistical durations every day. The statistical tasks can be automatically output to different terminals and the network management center.

4) Several traffic measurement items can be combined according to your requirements. Items can be measured individually or together at a time.

5) One statistical task has up to 48 measurement items.

6) A maximum of 1000 measured objects can be supported, such as destination signaling code and media gateway status.

1.4.9 Convenient and Practical Operation and Maintenance

KSS200 provides convenient and practical operation and maintenance functions as follows:

1) Flexible and diversified management modes. *KSS200* adopts a Web based system access,

providing multiple maintenance modes such as Graphical User Interface (GUI) and MML command line. *KSS200* supports simultaneous access to the equipment by multiple local and remote clients. The related network management network can be constructed flexibly depending on the factors including the network structure, the management requirements and the investment scale.

2) Visualized graphical user interface. *KSS200* provides operation and maintenance interfaces by using the OSS-BSS. Therefore many MML characteristics and GUI advantages are reserved: it is visualized, simple and quick to operate, easy to access NMS, easy to memorize. In addition, vivid graphic network component topology view and equipment panel view are provided, thus visualized operation is provided.

3) Optimized call tracing, signaling tracing, interface tracing and message interpretation functions. Signaling analysis tool software which is independently developed by KIATEL is built in to offer customers with powerful fault analysis and location capabilities.

4) Real-time fault management capability. The system receives and displays network equipment fault report in real time, so that the maintenance personnel can diagnose the fault source rapidly and precisely and take proper measures to recover the system from the abnormal service.

5) Online software patching, online debugging, remote maintenance and dynamic data setting.

Chapter 2 System Architecture

2.1 *KSS200* Mechanical structure

KSS200 is composed of servers, network switches, supervisory terminal and power supply which have been installed in one 42U, 19" standard rack for each home. Figure 2-1 shows the mechanical structure of *KSS200*.

2.2 *KSS200* Hardware Structure

KSS200 NGN/IMS Platform (hereinafter referred to as *KSS200*) is composed of Core Servers, Database Servers and OSS-BSS Server. These 5 servers along with 2 layer 3 network switches and needed accessories are installed in a 36U, 19-inch standard cabinet.

An inverter capable to supply 3KVA power in 220 VAC has been provided in system and devices are supplied through cabinet PDB.

Servers are connected to the supervisory console through an 8 ports KVM switch. One or more Operation and Management Computers (OMC) can be connected to the system directly or through the Web.

The hardware structure of *KSS200* is illustrated in Figure 2-1.

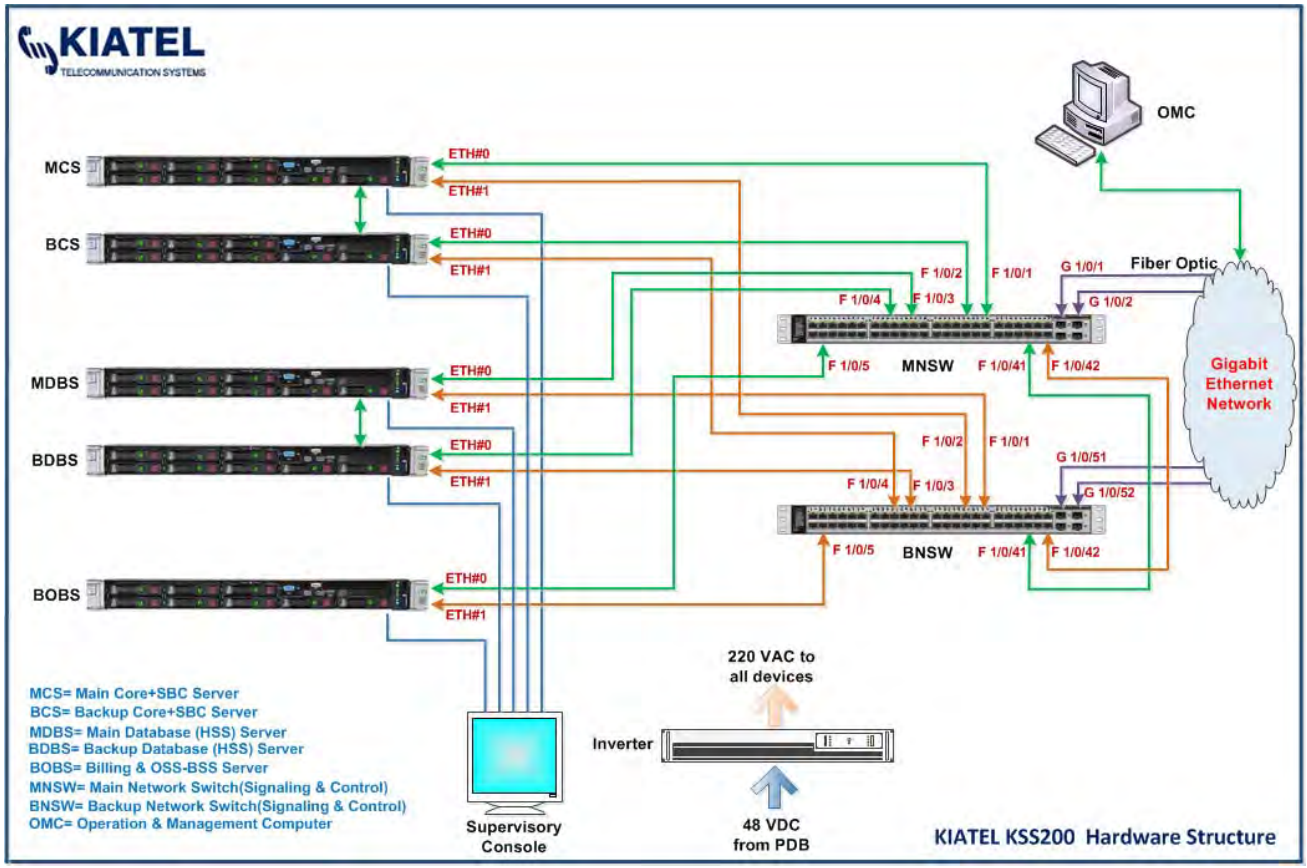


Figure 2-1 Hardware structure of *KSS200*

2.2.1 Devices Interconnections

The servers communicate with each other and the network through two 3 layers switches. Each server is connected to both switches with CAT6 cables.

The communication between the servers and the OMC is achieved through the two switches.

All Ethernet ports mapping is shown in above figure.

2.2.2 System Capacity

In an actual deployment, the capacity of the system depends on the type and configuration of the servers. At maximum, 2 million registered subscribers and 200,000 concurrent calls can be achieved.

2.2.3 Cabinet Features

KSS200 adopts 36U, 19-inch standard cabinet. One cabinet can accommodate a maximum of 36 standard 19-inch frames. Cabinet is assembled with electrolytic zinc-coated cold-rolled steel sheet and screws, featuring light weight, simple structure and high versatility. The cabinet surface and doors color is RAL-9002, cabinet frame color is RAL-7032 and front panels color is RAL-9005. The front/back doors of the cabinet are single-door mode and front door has a transparent window. The side panels are just hung on the cabinet, thus facilitating installation. The cabinet adopts bottom-to-top ventilation mode so that it has excellent heat dissipation and dust-proof functions.

Dimensions of a cabinet: 1750 mm (height) x 650 mm (width) x 1000 mm (depth)

Height of available space of a cabinet: 36 U (1 U = 44.45 mm)

Weight: 85 kg as an empty cabinet, or 175 kg with full configuration

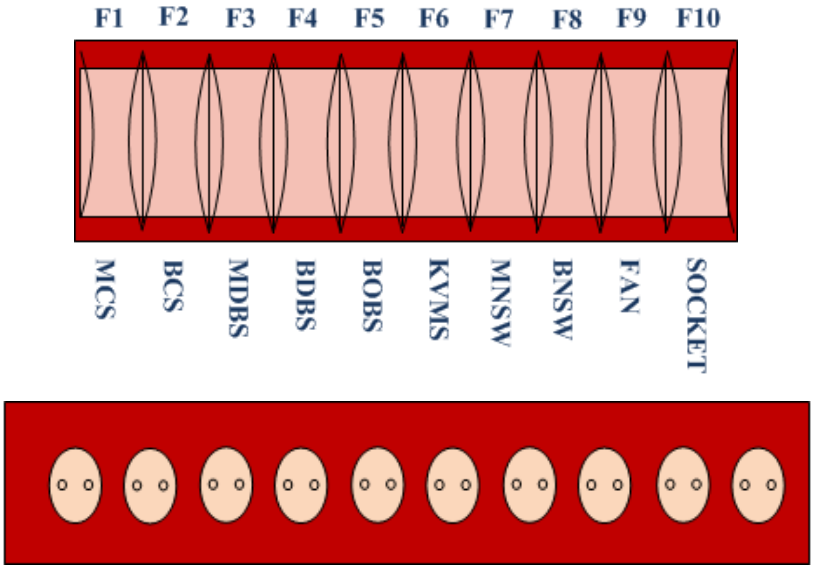
2.2.4 Cabinet Accessories

- **Power Distribution Board**

The power distribution board (PDB) is installed at the top of cabinet, which complies with the international and domestic standards. Its height is 3 U and its depth is 110 mm. A 220VAC power bus is connected to the power distribution board and all devices are supplied through appropriate rated MCBs. There is a socket panel in cabinet which can be used for testing and maintenance activities.

The front view of power distribution board and socket panel is shown in Figure 2-2.

Figure 2-2 Front view of power distribution board and socket panel



Power distribution board MCBs are D type AC and ratings are from 6 to 10 Amps. A technical specification of used MCBs is attached to this document as Enclosure A.

- **Power Supply**

The power supply of system is a 48VDC/220VAC-3KVA inverter which is installed at the bottom of cabinet. It is complies with the international and domestic standards. Its height is 2 U and its depth is 440 mm. A 48VDC power bus is connected to the power supply through a 60 Amps DC MCB in site MPDB. Output of the power supply passes through device MCB and is connected to power distribution board MCBs.

The front and rear view of the power supply are shown in Figures 2-3 and 2-4.

Figure 2-3 Front view of power Supply

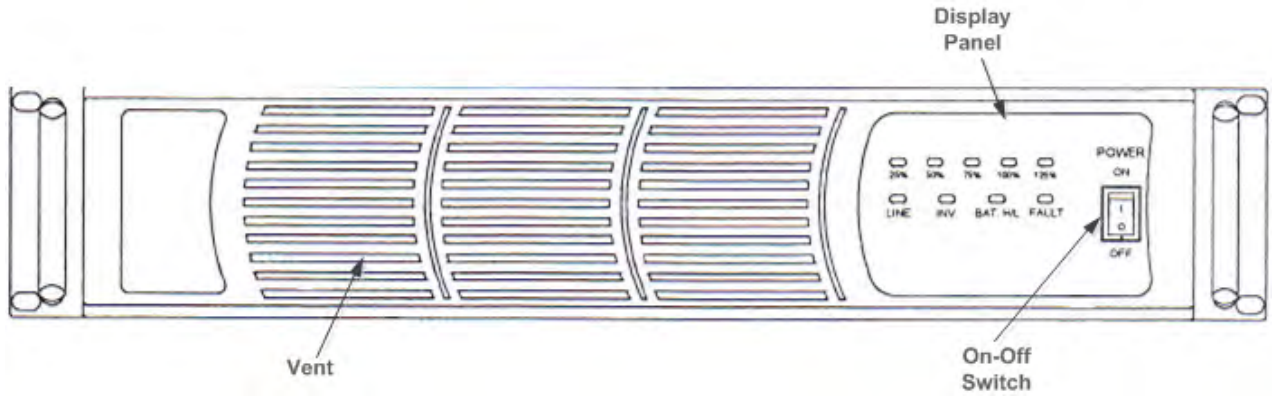
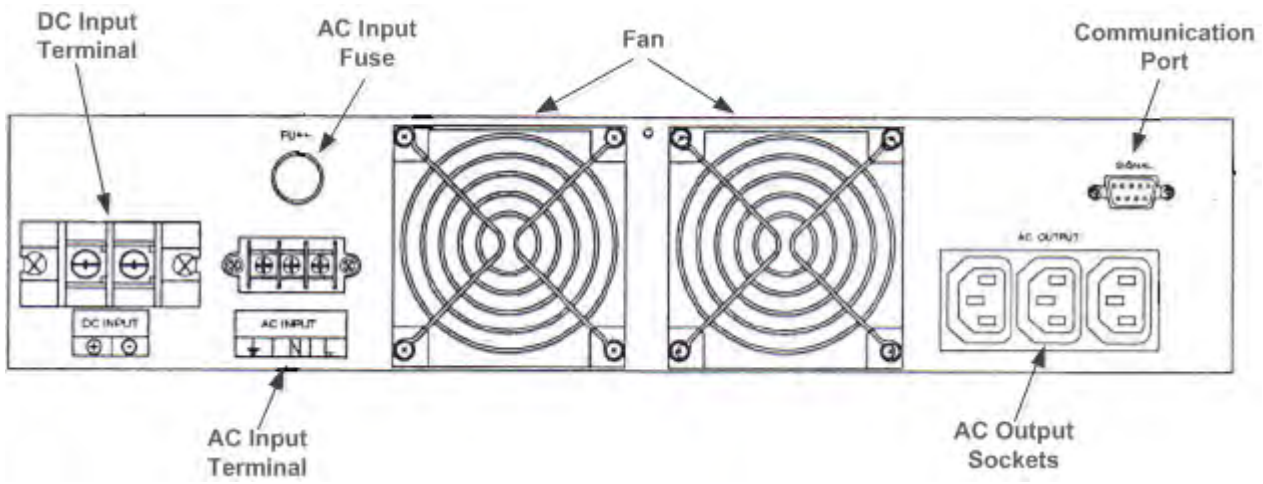


Figure 2-4 Rear view of power Supply



There are nine indicators on the front panel of the power Supply. The On/Off switch on the front panel is used to put device in service.
In the rear panel there are input and output terminal blocks and monitor ports. As can be seen there is AC input terminal in rear panel which shows the device may be used as UPS.
A technical specification of power supply is attached to this document as Enclosure B.

- **Fan Box**

A fan box is installed at the top of system cabinet. It consists of two 12cm high performance fans and is designed for heat dissipation purposes.

A speed adjustment technique is used in the fans. On the premise of normal heat dissipation and reliable running, the rotate speed of the fans can be controlled. The fans are hot-swappable. The running state of the fans can be known by observing the indicators. The fan box can be maintained through a remote network management terminal.

2.2.5 Cabinet Main Devices

➢ **Network switches**

In *KSS200* cabinet, two WS-C3750-48T-S layer 3 network switches interconnects servers, communicate with gateways, achieves redundancy for servers and provides reliability and main/backup configuration functions.
Switches are enterprise-class lines of stackable and standalone type. These switches provide high availability, scalability, security, energy efficiency and ease of operation with innovative features.

Some of the main features are:

- Four optional uplink network modules with GE or 10GE ports
- Media Access Control Security (MACsec) hardware-based encryption
- Flexible NetFlow and switch-to-switch hardware encryption with the Service Module uplink
- Open Shortest Path First (OSPF) for routed access in IP Base image
- IPv4 and IPv6 routing, Multicast routing, advanced quality of service (QoS), and security features in hardware
- USB Type-A and Type-B ports for storage and console respectively and an out-of-band Ethernet management port
- Cisco StackPower technology: An innovative feature and industry first for sharing power among stack members
- Cisco StackWise Plus technology for ease of use and resiliency with 64 Gbps of throughput

KSS200 switches have three feature sets available as follows:

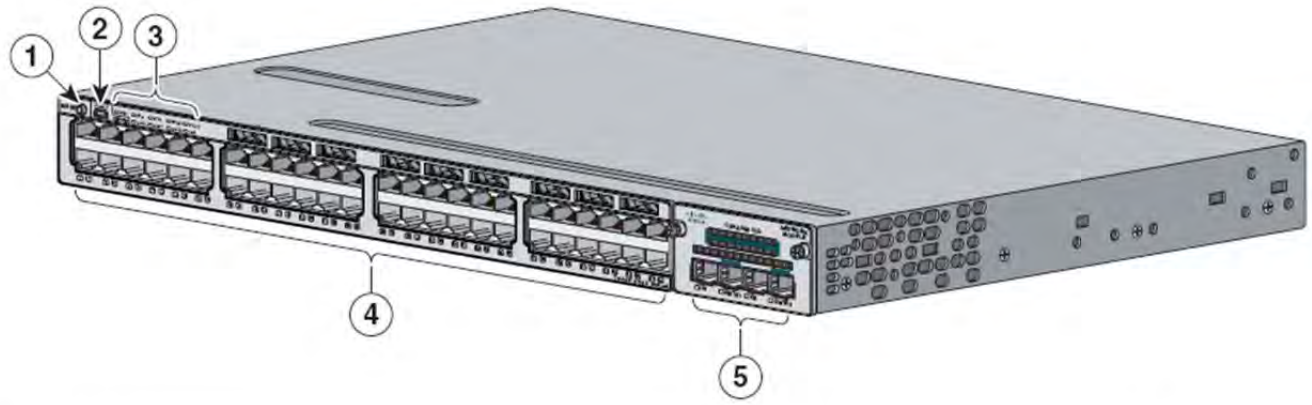
– LAN Base: enterprise access Layer 2 switching features
– IP Base: baseline enterprise access Layer 3 switching features
– IP Services: advanced Layer 3 switching (IPv4 and IPv6) features

The LAN Base feature set includes comprehensive Layer 2 features, with up-to 255 VLANs. The IP Base feature set provides baseline enterprise services in addition to all LAN Base features, with 1K VLANs. IP Base also includes the support for routed access, MACsec and the new Cisco Service Module. The IP Services feature set provides full enterprise services that include advanced Layer 3 features such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Protocol Independent Multicast (PIM), and IPv6 routing

such as OSPFv3 and EIGRPv6. All software feature sets support advanced security, QoS, and management features.

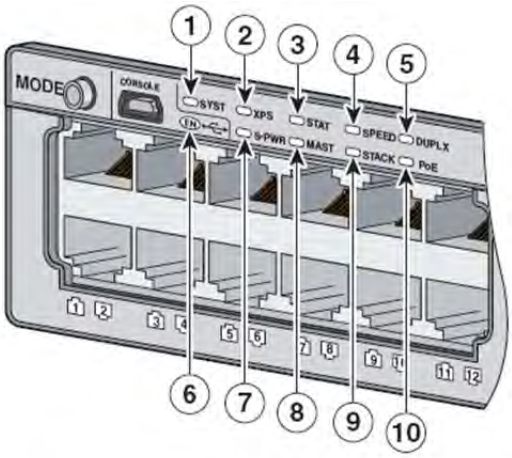
The front, rear and LED panel view of network switch are shown in Figures 2-5 to 2-7.

Figure 2-5 Front view of Network Switch



1	Mode button	4	10/100/1000 ports
2	USB Type-B console port	5	Network Module
3	Status LEDs		

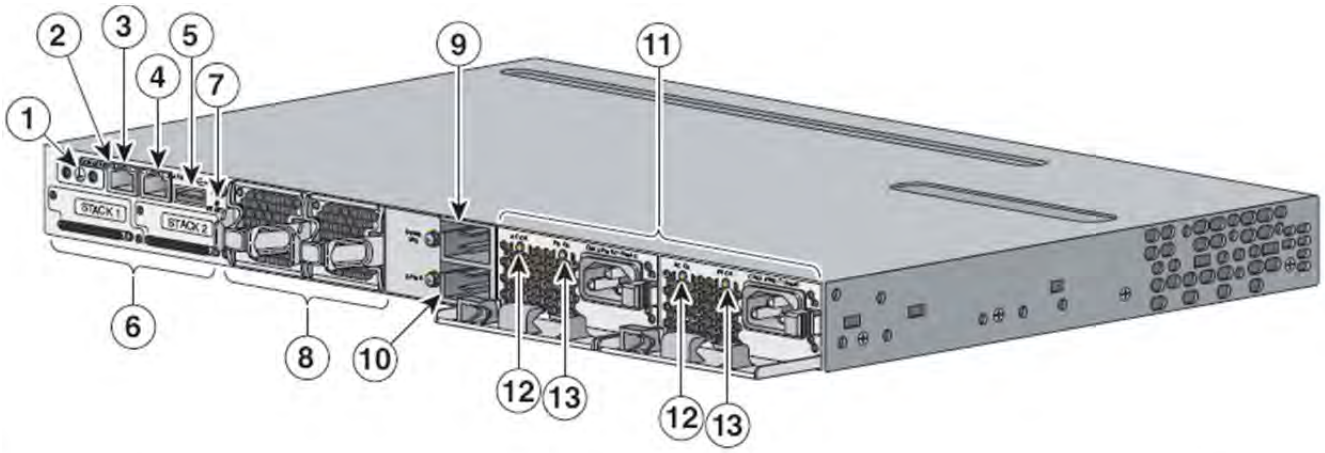
Figure 2-6 LED Panel view of Network Switch



1	System LED	6	USB console port LED
2	XPS[1] LED	7	S-PWR (StackPower) LED[2]
3	Status LED	8	Master LED[2]
4	Speed LED	9	Stack LED[2]
5	Duplex LED	10	PoE LED[3]

1. XPS = Expandable power system.

Figure 2-7 Rear view of Network Switch



1	Ground connector	**8**	Fan modules
2	RJ-45 console port LED	**9**	StackPower or XPS 2200 connector
3	RJ-45 console port	**10**	StackPower connector
4	RJ-45 10/100 management port	**11**	Power supply modules (AC power supply modules shown)
5	USB Type A connector	**12**	AC power (input) status LED
6	Stack cable connectors	**13**	Power supply (output) status LED
7	Reset button		

As mentioned above, switches implement redundancy of servers and are in main/backup configuration as well. Thus any device has a backup and all connections are dual.

The Redundancy (Resiliency) scenario in *KSS200* is Main/ Hot Backup. Hot backup, also known as dynamic or online backup, is a backup performed on system and subscribers data while the database is actively online and accessible to them.

Resiliency is a planned part of system architecture and is usually associated with other disaster planning and system disaster-recovery considerations such as data protection.

KSS200 resiliency is achieved through the use of redundant servers and network switches. When one device fails or experiences a disruption, the redundant device takes over seamlessly and continues to support services to the subscribers. Ideally, subscribers of a resilient system never know that a disruption has even occurred.

If a server's fails, the backup server keeps running until a technician can replace the failed one.

A hot backup is the standard way of doing most database backups. Main/Hot backup scenario can provide a convenient solution in multi-server systems because they do not require downtime, as cold backup do.

Below table shows technical specifications of network switch.

Feature	Specification
Type	IP Base
Number of Electrical Ports	48
Number of SFP Uplinks	4
Switching Fabric	160 Gbps
DRAM	256 MB
Flash	64 MB
Total VLANs	1005
VLAN IDs	4K
Forwarding Rate	101.2 mpps
Connectors	- 1000BASE-T ports: RJ-45 connectors, Cat-5E UTP cabling - 1000BASE-T SFP-based ports: RJ-45 connectors, Cat-5E UTP cabling - 100BASE-FX, 1000BASE-SX, -LX/LH, -ZX, -BX10, DWDM and CWDM SFP Transceivers - 10GBASE-SR, LR, LRM, CX1 SFP+ Transceivers
Power Consumption	120W
Relative Humidity	5% to 95%, noncondensing
Operating Environment and Altitude	-5ºC to +40ºC, up to 3000 m
Mean Time Between Failure (MTBF), Hours	171,846
Weight	7.5 Kg
Dimensions (H x W x D),cm	4.45 x 44.5 x 46.0

- **Servers**

KSS200 uses 5 servers to implement IMS platform for at least 2 million subscribers. There are two servers as core in main/hot backup configuration. Also, two servers handle system and subscribers database and are in main/hot backup configuration as well. The fifth server is assigned for OSS-BSS tasks and services.

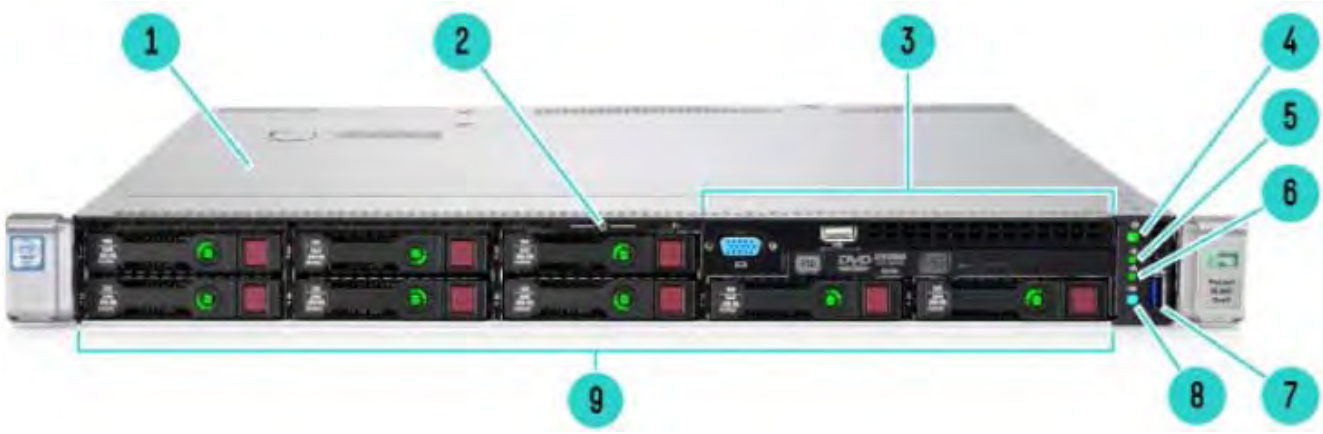
The servers which have been used in *KSS200* are HPE ProLiant DL360 Gen9 type. This is new Hewlett Packard Enterprise leading server for dense general-purpose computing; the HPE ProLiant DL360 Gen9 Server delivers increased performance with the best memory and I/O expandability packed in a 1U dense rack design. Reliability, serviceability and always on availability make it ideal for the most space constrained server workloads.

Each server would be configured according to assigned tasks. The table in next page shows typical servers specifications for a system with 2 million subscribers and completes redundancy.

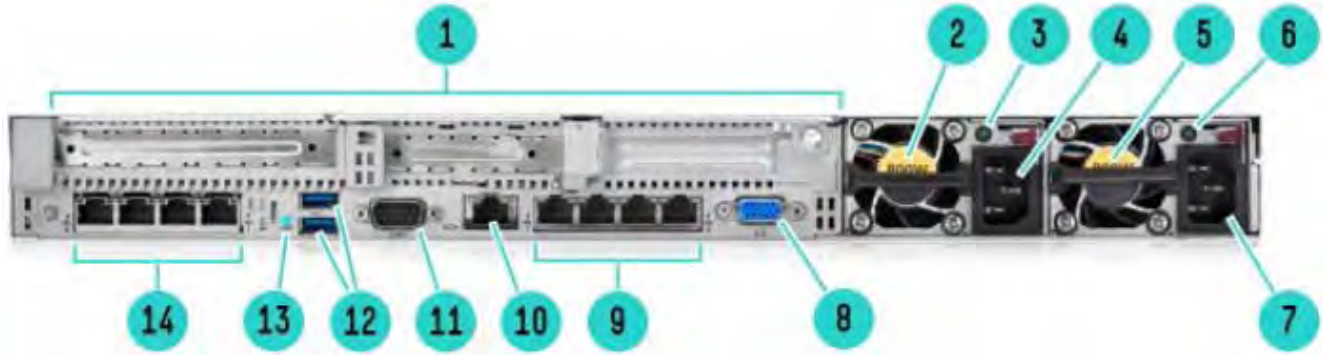
Below table shows each server main configuration.

Item	Device	Specification									
		Qty.	Sub Unit	Model	Qty.	Sub Unit	Model	Qty.	Sub Unit	Model	Qty.
1	Core Server-1	1	CPU	Xeon E5-2620 V3	2	RAM	16GB DDR4-2133	2	HDD	146GB SAS 15K	2
2	Core Server-2	1	CPU	Xeon E5-2620 V3	2	RAM	16GB DDR4-2133	2	HDD	146GB SAS 15K	2
3	Data Base Server-1	1	CPU	Xeon E5-2620 V3	2	RAM	16GB DDR4-2133	4	HDD	600GB SAS 15K	4
4	Data Base Server-2	1	CPU	Xeon E5-2620 V3	2	RAM	16GB DDR4-2133	4	HDD	600GB SAS 15K	4
5	OSS-BSS & Billing Server	1	CPU	Xeon E5-2620 V3	2	RAM	16GB DDR4-2133	4	HDD	600GB SAS 15K	4

Figures 2-8 and 2-9 show servers front and rear panels.



1. Access Panel	6. NIC Status LED
2. Serial Label Pull Tab	7. USB 3.0 Connector
3. HPE Universal Media Bay or NVMe	8. Unit Identification Button & LED
4. Power On/Standby button and system power	9. SAS/SATA/SSD/NVMe Drive Bays
5. Health LED	



1. PCIe 3.0 Slots 1-3	8. Video Connector
2. HPE Flexible Slot Power Supply Bay 2	9. Embedded 4x1GbE Network Adapter
3. Power Supply 2 Status LED	10. Dedicated iLO 4 connector
4. Power Supply 2 C13 Connection	11. Serial Port Connector (Optional)
5. HPE Flexible Slot Power Supply Bay 1	12. USB 3.0 Connectors (2)
6. Power Supply 1 Status LED	13. Unit Identification LED
7. Power Supply 1 C13 Connection	14. FlexibleLOM bay (Optional)

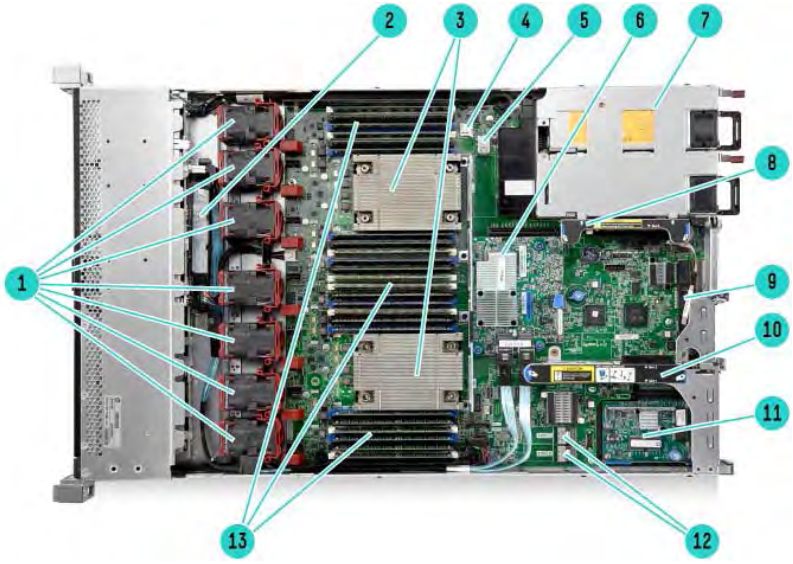
All *KSS200* system servers use HP SAS (Serial Attached SCSI) 15K SFF hard drives which are high-performance, enterprise class type. SAS hard drives combine faster data transfer rates with better error detection and recovery, as well as having higher reliability specifications. SAS based hard drives are ideal for projects requiring transactional applications and performance oriented requirements where throughput and reliability are critical.

SAS 15K SFF hard drives which are used in *KSS200* offer sustained performance of 260 MB/s to 175 MB/s (outer to inner diameter). They are full Enterprise class drives with the industry's highest reliability of 2.0M hours MTBF. These drives offer the highest performance available today.

Benefits of using this type of drive are:

- Higher hard drive performance and reliability compared to typical SATA drives
- "Star" topology (point-to-point, no hubs). Each device gets full bus bandwidth.
- Minimum device arbitration overhead True full duplex communications, transfers both read and write data simultaneously on 1 port.

Figure 2-10 shows internal parts of servers.



1. 5 Standard Fans Ship for 1P and 7 Standard Fans Ship for 2P	8. Secondary PCIe 3.0 riser for PCIe slot 3 (requires CPU 2)
2. HPE Smart Storage Battery (Optional)	9. Embedded 4x1Gbe NIC
3. 2 Processors with HPE Smart Socket Guide	10. Primary PCIe 3.0 riser for PCIe slots 1 & 2
4. MicroSD card slot	11. FlexibleLOM Bay (Optional)
5. Dual Internal USB 3.0 connector	12. Embedded SATA Controller ports
6. HPE Flexible Smart Array or Smart HBA (Optional)	13. DDR4 DIMM slots. Shown fully populated in 24 slots (12 per processor)
7. 2 HPE Flexible Slot Power supplies	

All *KSS200* system servers are equipped with two Intel XEON E5-2620 v3 processors.

This new generation of processors enables powerful, agile telecom systems by supporting a Software-Defined Infrastructure (SDI) to address the imminent need of greater flexibility with higher levels of automation and orchestration. In addition, the Intel Xeon Processor E5-2620 v3 delivers significant benefits in performance, power efficiency, virtualization, and security and adds 50 percent more cores and cache3 over the previous generation and includes numerous other hardware enhancements, such as Intel Advanced Vector Extensions 2 (Intel AVX2) and Intel Quick Path Interconnect link (QPI).

These innovations deliver up to 2.2X the performance over the previous generation to significantly boost output across a broad set of workloads. The Intel Xeon Processor E5-2620 v3 also delivers an increase in virtualization density of up to 1.6X compared to the previous generation, 4 building on an ever more important capability in the system.

With up to 6 cores per socket, 15 MB of last-level cache (LLC) and next generation DDR4-1866 memory support, this processor delivers significant performance improvements in workloads. Fused Multiply-Add (FMA) instructions in this processor doubles the floating point operations (Flops) from first generation Intel AVX, and doubles the width of vector integer instructions to 256 bits, expanding the benefits of Intel AVX2 into enterprise computing.

Trustable and Secure Data protection in telecom systems is critical for operators. Intel's hardware-enhanced security technologies on the Intel Xeon Processor E5-2620 v3 better protect data and platforms through workload isolation, security policy enforcement, and faster data encryption.

Intel Data Protection Technology with Intel Advanced Encryption Standard New Instructions (Intel AES-NI) accelerates data encryption and decryption up to 2X faster than previous generation. With many workloads, Intel AES-NI encryption and decryption is practically transparent to system resources. Combined with Intel Data Protection technology with Intel Secure Key random number generation, this processor provides even stronger data protection.

Intel Platform Protection Technology with Intel OS Guard and BIOS Guard traps external calls trying to hijack System Management Mode (SMM) code in the OS, and provides workstation BIOS protection during FLASH updates via protected agent authentication.

Memory modules in *KSS200* are DRAM type memory. The quality and reliability of DRAM are more important as telecom system trends such as call processing, cloud computing and use of large database applications have all increased the need for higher capacity memory with greater uptime.

KSS200 uses HPE DDR4 16MB-1866 modules in memory stacks. This type of memory is powered

by Hewlett Packard Enterprise SmartMemory technology which enables the reliability of system. Because the memory is authenticated, it can enable extended memory performance features through the system ROM.

- **Supervisory Console**

KIATEL provides a supervisory console including monitor, mouse and keyboard with 8 ports KVM switch in *KSS200* cabinet. This console allows access to servers from a single keyboard, video, and mouse and is equipped with a 17" LED-backlit LCD monitor and touchpad in a 1U rack-mount sliding housing.

2.3 *KSS200* Software Architecture

The software architecture of *KSS200* is functionally composed of modules as shown in Figure 2-11. This architecture can handle all standardized IMS platform functions.

Figure 2-11 Software architecture of *KSS200*

Below table shows *KSS200* software modules.

Module Name	Sub Module Name	Server Placement
CSCF (Call Session Control Function)	I-CSCF	MCS (Main Core Server) BCS (Backup Core Server)
	P-CSCF	
	S-CSCF	
MGC (Media Gateway Control)	AGCF	
	MGCF	
CORE	BGCF	
KDSF (KIATEL Dual Homing Synchronization Function)		
KRSF (KIATEL Redundancy Synchronization Function)		
SLF (Subscriber Location Function)		
MRF (Multimedia Resource Function)	MRFC	
	MRFP	
LIXPF (Lawful Interception X Protocol Function)		
CORE MONITORING (System Monitoring SNMP Module)		
DIAMETER		
RADIUS		
KSSM (KIATEL Special Security Module)	IBCF	
	IBGF	
DIAMETER		MDBS (Main Database Server) BDBS (Backup Database Server)
HSS (Home Subscriber Server)	CX/DX Handler	
	Sh A(Sh Reference Point Administration)	
	S/SPM	
	DBIM	
KSSM	DBAM	
MySQL		
OSS-BSS	Operation Support Service	BOBS (Billing & OSS-BSS Server)
	Business Support Service	
WEB SERVICE		
SNMP		

2-3-1- KCL Operating System

KIATEL develops an operating system in basis of LINUX OS. This OS has mainly customized for *KSS200* NGN/IMS core and has many advantages over other operating systems. All software modules in *KSS200* are running on this OS.

Among various versions of LINUX, KIATEL did choose Debian operating system. The reasons are:

✓ Upgradability

Debian is not exactly a rolling release, but a live system can be upgraded to next stable release, using apt-get package manager. This is a well-documented procedure. Usually, there is no need to reboot or switch into single-user mode.

Common system updates of running release are very safe using just a single command: apt-get update && apt-get -V upgrade. Updates can be automated, but this is not recommended. Excellent tools are available to notify admin when new updates are available and when reboot is required. Reboot is mainly required when kernel is updated. Debian Kernel updates are not so often, so system reboot is rarely required and it can be scheduled.

✓ Security

Packages have been tested thoroughly before each Debian release. This is mainly the reason why packages are not of latest version. Releases occur every 2-3 years. Debian community is very responsive to bug fixing. Security is one of the most important Debian features.

✓ Stability

Debian is one of the oldest distributions (active for more than 18 years). Stability is synonym with Debian. Any package has been tested thoroughly before included in a Debian stable release.

2-3-2- Call/Session Control Function (CSCF) Module

KSS200 provides a control plane using Call Session Control Function (CSCF) by means of the SIP. User data is managed by the Home Subscriber Server (HSS) and the Authentication Center (AuC). As IMS standards define the *KSS200* represents three types of CSCF modules. First one is the proxy-CSCF (P-CSCF), the first hop in network that redirects SIP messages from user terminal to user terminal. It also establishes an IPSEC security association with the user terminal. The confidentiality and integrity keys, CK and IK respectively, are derived as a result of the authentication performed with the HSS and conveyed to P-CSCF using signaling. I-CSCF is an interrogating-CSCF located at core software that locates a module able to manage user originated SIP messages. Finally, the S-CSCF, a serving-CSCF, authenticates users retrieving authentication vectors from the HSS. IMS authentication is based on HTTP Digest Authentication, using AKAv1-MD5 as algorithm, which requires exchanging four messages (2 Round Trip Times-RTT) between the users.

The *KSS200* registration protocol is as follows:

- In the step 1, the user terminal is registered with system and has discovered a P-CSCF.
- In step 2, the user terminal uses the UICC to obtain subscriber information as the registration URI (to locate network), the public/private identity and the Contact Address to build a SIP

REGISTER message. Moreover, the user terminal includes a Security Client header indicating which IPSEC algorithms supports.

- In step 3, the user terminal sends the aforementioned REGISTER message to the P-CSCF which inserts a P-Visited-Network identifier in the REGISTER message. The P-CSCF reads and removes the Security Client header and redirects the REGISTER message to the discovered I-CSCF module. I-CSCF locates an appropriate S-CSCF to handle user terminal's messages by sending UAR as step 4.
- In step 4, a Diameter User-Authentication Request (UAR) is sending to the HSS. The REGISTER message reaches the S-CSCF at step 5. The S-CSCF downloads authentication vectors for the subscriber from the HSS. Those vectors are quintuplets containing parameters for authentication and key derivation using AKA as a random challenge (RAND), an authentication token (AUTN), the expected user terminal response (XRES), an integrity key (IK) and a confidentiality key (CK). AUTN is derived by the HSS using the long-term secret it shares with the user terminal (KI) and a sequence number (SQN).
- The step 5 finishes with the S-CSCF building a 401 unauthorized message adding a WWW Authenticate header containing AUTN and RAND. The S-CSCF includes also CK and IK in the message to be consumed by P-CSCF. Finally, the S-CSCF sends this message back to the user terminal.
- In step 6, the 401 unauthorized messages reach the P-CSCF at visited network. The P-CSCF extracts and removes CK and IK from the message (the user terminal can derive CK and IK from AUTN and RAND using the UICC) and adds a Security-Server header selecting one IPSEC algorithm from those proposed by the client in step 2.
- In step 7, the user terminal receives the 401 unauthorized message and uses the UICC to calculate a response to the challenge (RES), CK and IK from AUTN and RAND. Then the user terminal establishes a security association with P-CSCF using CK/IK and composes a new REGISTER message containing RES and a Security-Verify header. Then it forwards the message to the P-CSCF over the brand new IPSEC security association.
- In step 8 the P-CSCF, upon the reception of the message over a protected channel (CK and IK), implicitly authenticates the user terminal. Then, it redirects the message to the I-CSCF.
- In step 9 the message is forwarded to the S-CSCF.
- Finally, in step 10, the S-CSCF receives the REGISTER message and checks if RES matches XRES to legitimate the subscriber. If the user is successfully authenticated, the S-CSCF builds a 200 OK message and sends it back to the user terminal finishing the IMS registration process.

The Call Session Control Function (CSCF) is a central component to signaling and control within the *KSS200*. The CSCF is responsible for all signaling via SIP between the access layer, control layer and the application layer of IMS.

2-3-3- Core and Gateway control

This module consists of 3 control functions.

- **SGCF module**

The SGCF (Signaling Gateway Control Function) is used for sending signaling messages between SS7 nodes, which communicate with the help of different transports and protocols. The signaling messages include information regarding call establishment, location, address conversion, billing, short messages and other services. The transport conversion is usually from SS7 to IP. Processing of

layer 3 and higher protocols required for service features including MTP3, M3UA, TUP, ISUP, SCCP and TCAP provides by this module.

- **MGCF module**

The MGCF (Media Gateway Control Function) facilitates call control, interfacing the PS (Packet Switching) domain to the CS (Circuit Switching) domain when interworking between the IMS and PSTN is required. From a control perspective, the MGCF has the same responsibilities as a regular telephony exchange, with the addition of protocol conversion in order to switch between SIP or H.248 and ISUP signaling. The MGCF can control one or more media gateway and can be used in conjunction with BGCF for calls breaking out to the PSTN/PLMN.

- **BGCF module**

The BGCF (Breakout Gateway Control Function) is used for calls from the IMS to a phone in the PSTN or the PLMN. BGCF forwards the signaling to the selected PSTN/PLMN network. If the breakout occurs in the same network as the BGCF then the BGCF selects a MGCF (Media Gateway Control Function) that will be responsible for inter-working with the PSTN, and forwards the signaling to MGCF. Otherwise it forwards signaling to BCGF of another operator network The MGCF then receives the SIP signaling from the BGCF and manages the interworking with the PSTN network.

2-3-4- KIATEL Dual Homing Synchronization Function (KDSF)

Dual Homing is necessary in IMS which is based on IP network, so the system can be deployed to a wider area than PSTN and cover more subscribers. If the system is crashed in a disaster, the impact will be very severe. Dual Homing is the solution for recovering the services shortly during a disaster. That is, two systems will be running in the IMS. In case a system fails, its service will be taken over by its Dual Homing system instantly so that services will be recovered immediately.

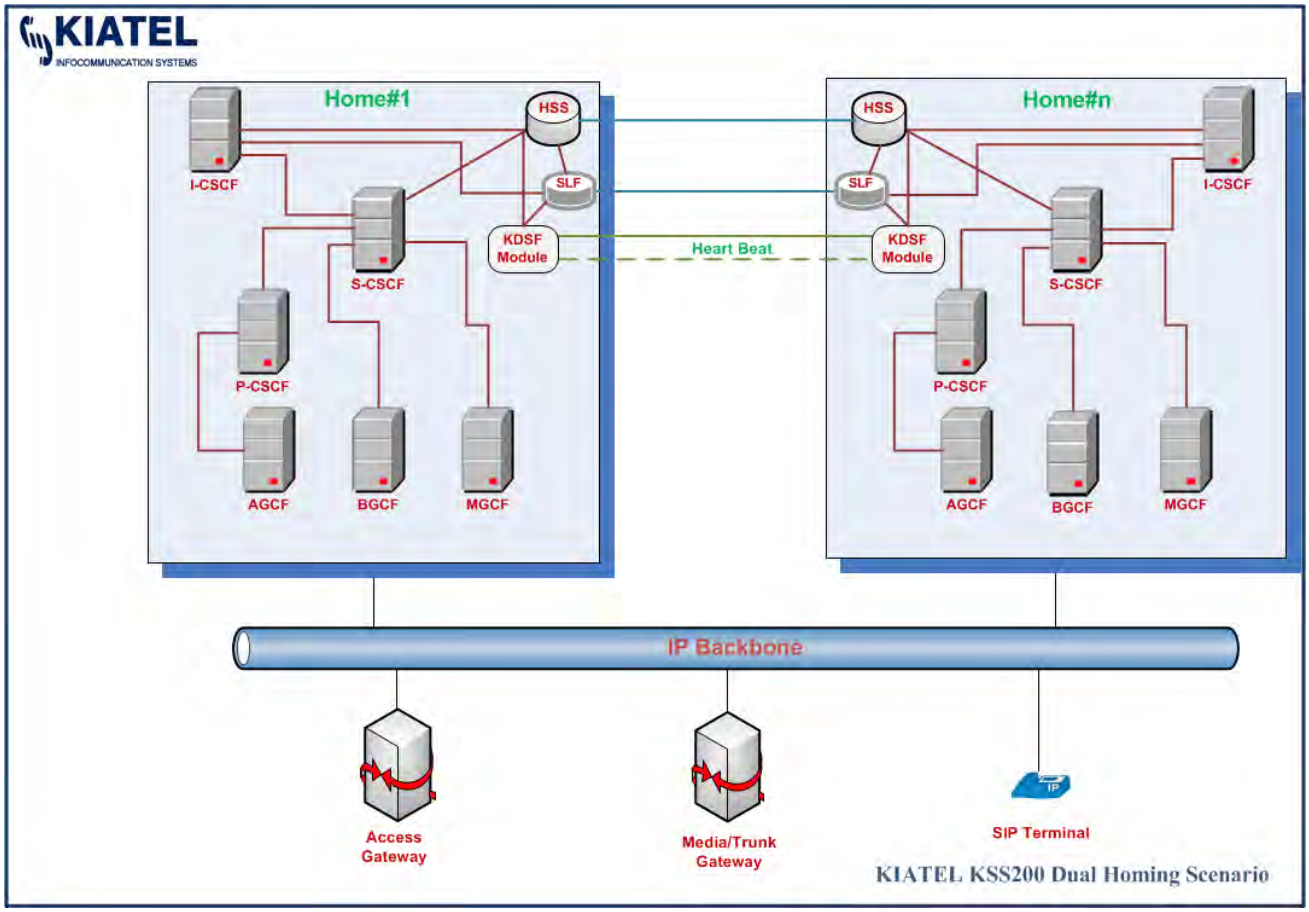
KIATEL Dual Homing Synchronization Function (KDSF**)** is the heart beat of *KSS200* NGN/IMS platform dual homing solution. IP address of Home#1 and Home#2 is different. All gateways are registered to both homes in the normal condition. KDFS configures registration data to both Home#1 and Home#2.

Key Points of Dual Homing switchover will be initialized by registration timeout. The synchronization of procedure is supported by the KDFS. The switchover will happen only when heartbeat between two systems is broken AND the registration has been timed out. Dual homing switchover can be done manually also. In this case switchover command is sent through SNMP.

The concept of KDFS is a kind of handshaking used by each home for detecting the state of the other home. It's a private protocol encrypted using special algorithm which sends directly by a home. The number of heartbeat timeout is configurable. The state of each home is configured on the gateways. In a dual homing topology, each gateway is configured with information of two homes. One home is set to master and another one set to slave. Similarly, gateways also need to be configured as master in one home and slave in another home.

Call during switchover is implemented on the gateway. Every call passing the gateway will be continued (intra-office call, an outgoing call, or an incoming one). As the gateways are registered

with the both homes, no information on call statuses are discarded, so the held calls will not be released and no charging information defected.



2-3-5- KIATEL Redundancy Synchronization Function (KRSF)

KSS200 is a Carrier Grade system which must be available and in service for 99.99999 percent of times. To achieve this goal, KIATEL has used redundant servers in each home to ensure that systems continue without service interruption.

The *KSS200* implements 1+1 redundancy scenario under management of KRSF. This is a form of redundancy that ensures system availability in the event of server's failure. Each server has at least one independent backup. The level of redundancy is referred to as Main/Backup with active-active servers and under management of KRFS each server participates within the system during normal operation. In this scenario the backup server will remain active in the operation even if all other servers are fully functional. Therefore the system will be able to perform in the event that one server is faulted and recover from a single server failure. Thus failover does not actually occur as the backup servers are already active within the system.

2-3-6- Subscriber Location Function (SLF)

KSS200 uses Diameter for access to the HSS. The HSS is used to obtain subscriber data and, when there are a large number of subscribers, they may be partitioned across multiple HSS instances deployed in a network. The 3GPP defines the Subscriber Location Function (SLF) entity to be used to select the correct HSS instance. The 3GPP defines the Diameter Routing Agent (DRA) entity to be used to select the correct instance.

The Diameter Solution Suite (DSS) can be deployed in the IMS to act as a SLF or DRA or both. All

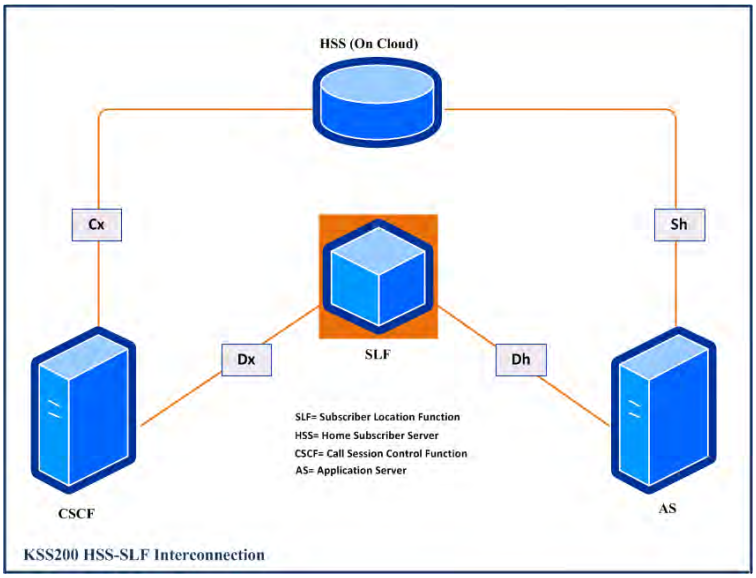
elements connect to the DSS and all Diameter traffic passes through the DSS. The DSS examines the Diameter messages and performs load balancing and binding across the multiple instances of the HSS. The DSS may be deployed in a distributed or centralized configuration and optionally in a dual home redundant configuration for disaster recovery. This results in a more efficient network that is easier to manage.

The Diameter Solution Suite (DSS) can be deployed at the core of the IMS in a highly scalable, highly available and redundant configuration where all Diameter signaling passes through the DRA resulting in a hub rather than a mesh network.
In dual home scenarios where there are multiple systems, the DSS is deployed at the edge of the network and performs the Diameter Edge Agent (DEA) role, passing all Diameters signaling through the DSS while performing routing and security functions.
The DSS detects congestion and can throttle the Diameter signaling passing through the network. The DSS sees all Diameter traffic and can be configured to detect overload and perform overload control on a global or per server basis.
When there are untrusted elements, the DSS provides security at the edge of network, including DoS, DDoS, NAT with topology hiding and IPsec and TLS for protocols.
When there are multiple Diameter servers, the DSS selects and distributes across the multiple server instances and sends all messages in a session to the same server. The DSS can act as a proxy or redirect, e.g., the DSS performs the role of a Subscriber Location Function (SLF) for an HSS or a Diameter Routing Agent (DRA) for a PCRF.

2-3-7- HSS (Home Subscriber Server)

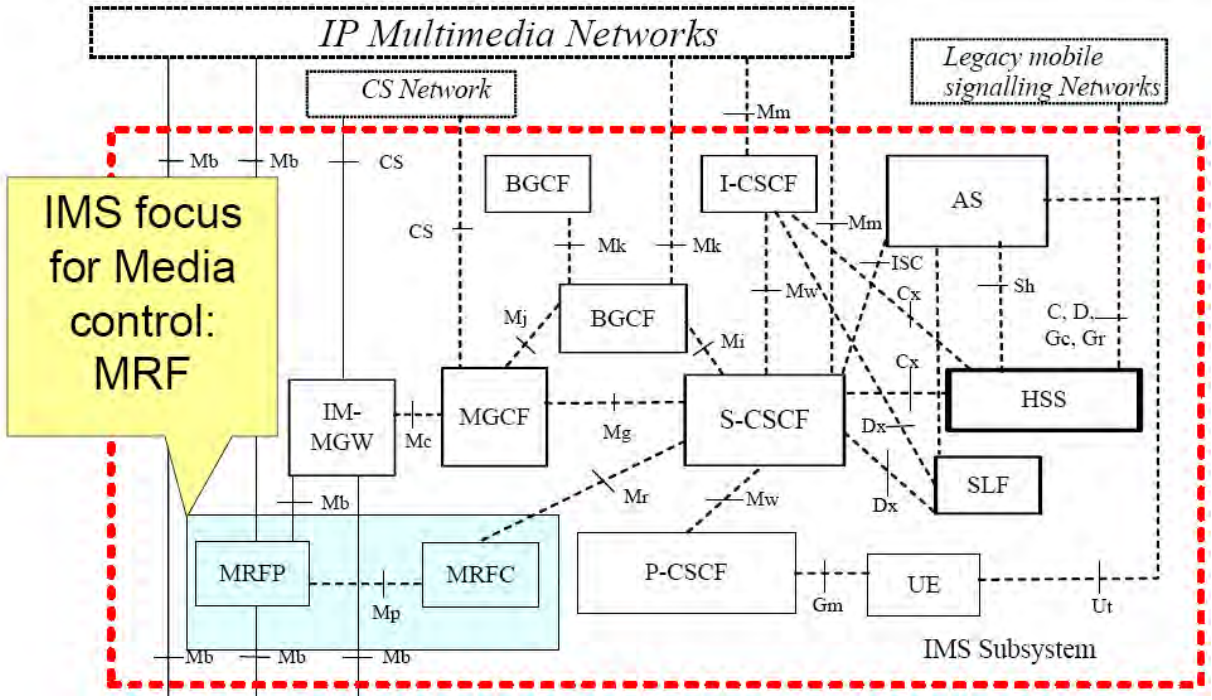
The HSS is a cloud-based database in *KSS200* that holds both static and dynamic data elements related to subscribers. The HSS provides user profile information to the core during user terminal attach and registration. On registration process, I-CSCF interrogates the HSS to determine which suitable S-CSCF to route the request for registration. For mobile terminating calls, it interrogates the HSS to determine which S-CSCF the user is registered on. The S-CSCF acts as SIP registrar for user terminals that the HSS and I-CSCF assign to it. It queries the HSS for the applicable subscriber profiles and handles calls involving these end points once they have been registered.
HSS uses following interfaces:

- S6a Interface (HSS – MME) - The interface enables the transfer of subscription and authentication data for authenticating/authorizing user access. The protocol used on the S6a interface is Diameter.
- Cx Interface (I/S-CSCF – HSS) - The Cx interface is between the I/S CSCF and HSS to enable IMS registration and passing of subscriber data to the S-CSCF. The protocol used on the Cx interface is Diameter.
- Sh Interface (VoLTE AS – HSS)- The Sh interface is between the VoLTE Application Server and HSS to enable service and subscriber related information to be passed to the Application Server or stored in the HSS. The protocol used on the Sh interface is Diameter.



2-3-8- MRF (Media Resource Function)

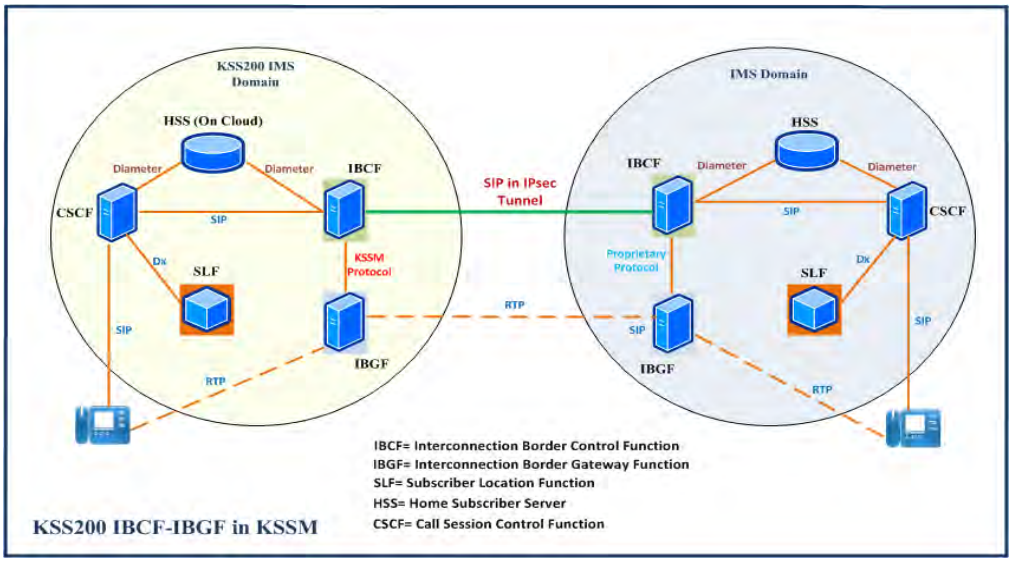
MRF (Media Resource Functions) is a solution that provides multimedia services to IMS subscribers. MRF is composed of MRFC (Media Resource Function Control) that controls the media resource and MRFP (Media Resource Function Processor) that processes all media (voice/video).It provides intelligence service free call, real-time limitation, and prepaid phone to *KSS200* subscribers within SIP/IMS network. It also provides media transcoding and voice and video conferencing functions as well as sound source, balance info, DTMF collection, voice recording.
Figure 2-5 shows MRF implementation in KSS200 NGN/IMS platform.



2-3-9- KIATEL special security module (KSSM)

The KSSM (KIATEL Special Security Module) has been provided for this issue and composes a part of *KSS200* software.

This module consists of Interconnection Border Control Function (IBCF) which acts as a border controller for interworking with IP network and processes issues related to interlock and security for interworking with other IMS networks, Interconnection Border Gateway Function (IBGF) that provides media relay between terminals in the network of a service provider and Special Processing Function (SPF).



With the fundamental role of providing secure, scalable, centralized service delivery, KIATEL has defined an innovative approach based on a distributed signaling / media architecture. Meanwhile KSSM has extended security function to incorporate all IMS core functions such as the Proxy Call Session Control Function (P-CSCF) and Interrogating Call Session Control Function (I-CSCF).

Signaling & Control		Media
P-CSCF	I-CSCF	
User terminal authentication, authorization and registration	SIP security	Media flow firewalling, filtering, bandwidth control and steering
SIP security	SIP message forwarding, routing and load-balancing	Media flow security
SIP encryption	SIP message manipulation and normalization	Media flow encryption
SIP message forwarding and routing	NAT and firewall traversal	Media flow interworking (SRTP-RTP, MSRP-MSRPS, IPv6-IPv4)
SIP message manipulation and normalization	IPv6-IPv4 interworking	Lawful intercept (media)
NAT and firewall traversal	Lawful intercept (signaling)	Transcoding
IPv6-IPv4 interworking (IMS-ALG)		
Lawful intercept (signaling)		

As all IMS engineers know, the security threats to any IMS platform include the following:

(1) Detection Threat

Through scanning the network, hackers can identify easy-to-attack devices without hassle.

(2) DDoS Attack

Distributed Denial of Service (DDoS) is the most dangerous attack to the current IP network. It can cause any high-performance system to crash.

(3) Interrupting and Taking over Equipment

This attack belongs to the broker attack. Usually, it illegally accesses the special devices (by means like illegally adding a route into the routing table) along with detection.

(4) Illegal Service Use and Service Fraud

This means the unauthorized use of network resources.

(5) Zero Day Attack

It attacks the network on some special day.

(6) Stealing Private Information from Host or Access Terminal (AT).

It is the behavior of collecting private information from the AT by spy software and malicious programs, including transferring personal information, eavesdropping SIP calls, and recording and reporting service use ratios.

The KSSM improves the security mechanism in IMS and establishes a new security system. It realizes the prevention, monitoring and control of attacks.

– **KSSM Inherits IMS's Security System**

The KSSM inherits all the security characteristics of the IMS, such as authentication, encryption and the protection algorithm for data integrity.

Therefore, it has the same algorithms with the IMS in legality checking for SIP users and the data privacy and integrity. Moreover, the algorithms have considered the support to the non-SIP applications.

– **KSSM Authentication Algorithm**

There is 2 step initial access authentication, IP mobile service authentication and SIP application authentication in the KSSM system. Moreover, the authentication is necessary for secure communications between users. The KSSM has different authentication algorithms for integrated devices and non-integrated devices.

For integrated devices, the KSSM employs 3GPP2 Authentication and Key Agreement/IP Security (AKA/IPSec) to SIP application, while using specific authentication protocols to non-SIP application, such as Transport Layer Security (TLS).

For non-integrated devices, it uses 3GPP2 AKA/IPSec or TLS to SIP application, while also adopting specific authentication protocols to non-SIP application such as TLS.

– **KSSM Security System Enhancement**

As it has been standardized in IMS, the KSSM enhances the integrated security and unified security management, device admission control and security policies.

– **Integrated Security and Unified Security Management**

Since the *KSS200* has to handle network traffic at Gigabit rates, it integrates security mechanism into every module of the system to avoid the network "bottleneck". The modules dispersed in different locations can work under unified security policies defined by the system manager. In this way, unified security management in the entire network is fulfilled. For instance, the system manager can use the integrated security mechanism to distribute the security policies like the traffic standard to every module, identify, distinguish and trace any abnormal behavior through local and remote measurements and then quickly block the spread of viruses. This unified integrated security mechanism greatly improves the security of the entire system.

– **Device admission control**

Device admission control is a kind of network behavior that decides if the terminal is allowed to access the network. Moreover, it determines the service levels for the accessed terminals according to their security postures.

The KSSM classifies terminals into three types: the voice-only closing terminal, the advanced terminal supporting voice and data, and the personal computer with EV-DO ability. The last two are Intelligent Agent Technology (IAT) terminals, and are the major objects of device admission control of the KSSM.

Device admission control is a major part for security enhancement. The access control measures, such as authorization and encryption, are used to implement device admission control in the KSSM network. Moreover, the KSSM has a new function of security agent that can verify the security status of the AT and determine the security level for its access.

The security agent runs in the IAT is called Posture Agent (PA). This agent in the IAT is an important part for device admission control. It collects the posture information about the AT (including if the version of the operating system is authorized, and whether it has patched correctly), and sends the results to the Security Management (SM).

In an initial IAT access, the SM checks the information report of the device posture sent by the PA and, according to the related security policies, decides an initial policy corresponding to the IP gateway: a limited or a full access. If it is a limited access, the related security policies will download to the Bearer Management (BM) so that the devices connect to the SIP service port for emergency call handling on a specific Application Manager (AM) only through the BM. Moreover, Web traffic will be transferred to the update server that asks users to download the updated software.

The benefits of the device admission control based on the PA are the following:

- It ensures the consistency of security policies between user equipment and the network, and prevents worms, viruses, and spy and malicious software in advance. It helps operators pay more attention to the precaution rather than be busy in handling security events, which greatly improves the security of the network.

- It offers a measure for checking and controlling the AT connected to the network with no need to consider the specific access modes. This improves the adaptation capability and scalability of the network.
- It refuses incompatible and uncontrollable terminal devices, avoiding any impact on network availability.
- It can reduce the operational payment caused by the identification and repair of incompatible, unmanageable and infected systems.
- It protects vulnerable, incompatible and uncontrollable terminal devices from attacks, which also improves the availability of the network.

– **MSA**

The Mobile Security Agent (MSA), which lies on the modules like the AM and BM, cooperates with the PA to implement the function of device admission control. Moreover, it can monitor equipment status according to the requirements of the SM, assist the SM in checking and removing threat of "Zero Day", and reduce the maintenance cost in system attack repair, which is very important when multiple access modes exist in the network (like Wi-Fi and broadband access). With the capability of reverse firewall, the MSA can analyze the behavior during checking threats rather than only relying on users' signature, which is very important for preventing the "Zero Day" attack.

The MSA has all the functions the PA has. In addition, it has the following functions:

- Host intrusion prevention
- Blocking the spy ware
- Preventing buffer overflow attack
- Providing capability of distributed reverse firewall
- Stopping malicious mobile code intrusion
- Ensuring the integrity of the operating system
- Auditing the log
- Enhancing QoS application

– **KSSM security policies**

The KSSM security policies are those that the system manager asks to run automatically when a security event happens in the network. The security policies play an important role in the KSSM. By them, the SM can implement security management, DDoS prevention, access control, intrusion prevention, authorization and device admission control.

According to system manager decision, the KSSM fulfills multi-level policy control. The system manager distributes security policies to related modules, implementing the unified security management in the entire network.

– **Precaution of DDoS**

The KSSM employs the self-learning algorithm to prevent DDoS. The algorithm can learn the traffic model to adapt itself to a special network condition. For example, it can learn SIP behavior to determine a proper traffic threshold. The KSSM can distinguish legal, suspected and malicious traffic, and only legal traffic is allowed to pass.

The function of DDoS precaution usually runs in an unremarkable background model. When the system is suspected to be attacked, the traffic diversion mechanism will be activated to redirect traffic to the protection system for analysis and control, and then return legitimate traffic to the network.

– **Security Log and Report**

All the KSSM sub-modules, including AM, BM, IP gateway and AP support standard registration and report of security events. The warning of security events will be sent to the security incident management subsystem to conduct persistent storage, analysis and auditing. The subsystem, as a log collection station, employs near real-time transmission to implement real-time monitoring of security operations.

The KSSM log transmission is based on the IP Flow Information Export (IPFIX) protocol, Security Device Event Exchange (SDEE) protocol, Simple Network Management Protocol version 3 (SNMPv3) and Syslog protocol.

In the IMS, the network security is divided into intra-domain security and cross-domain security. The former is further subdivided into access security and core network security. The KSSM improves the access security by introducing the mechanisms such as PA, MSA, two-way firewall and IDS/IPS, while it employs the policy-based centralized security management mechanism that makes every module in the control of the system manager and greatly enhances the core network security.

2-3-10- Lawful Interception X Protocol Function (LIXPF)

This function manages the interface between *KSS200* core, LIG and LEA.

2-3-11- Diameter

Diameter is the protocol used in *KSS200* for AAA (Authentication, Authorization, and Accounting). It is intended to work both in home IMS network and in roaming situations between home and visited IMS networks.
Diameter base protocol must be used in conjunction with Diameter applications (also called Diameter interfaces) which complement the base protocol functionality. The base protocol contains the basic functionality and is implemented in all Diameter nodes, independently of any particular application. Applications are extensions to the basic functionality that are tailored for a particular usage of Diameter in a particular environment.
The *KSS200* Diameter architecture consists of a number of entities:

- Diameter Node: A host process that implements the Diameter protocol.
- Diameter Peer: A diameter node that has a direct transport connection with another diameter node.
- Client: A Diameter Client is a device at the edge of the network that performs access control. Examples of Diameter clients are MME (Mobility Management Entity), PCEF (Policy and Charging Enforcement Function) in EPS architecture.

Server: A Diameter Server is one that handles authentication, authorization, and accounting requests for a particular realm. Example of Diameter server is HSS (Home Subscriber Server) and PCRF (Policy and Charging Rules Function) in EPS architecture.

- Agent: A Diameter Agent is a Diameter node that provides relay, proxy, redirect or translation services.
- Relay Agent: Relay Agents are Diameter agents that accept requests and route messages to other Diameter nodes based on information found in the messages (e.g., Destination-Realm). This routing decision is performed using the Realm Routing Table, which informs about the next hop for a given destination-Realm. Relays dot not perform any application level processing. Relay Agents modify Diameter messages by inserting and removing routing information, but do not modify any other portion of a message. Relays should not maintain session state but must maintain transaction state.
- Proxy Agent: Similarly to relays, proxy agents route Diameter messages using the Diameter Routing Table. Proxies may maintain session state and must maintain transaction state. Since enforcing policies requires an understanding of the service being provided, Proxies must only advertise the Diameter applications they support. Example of Proxy agent is the Diameter Routing Agent (DRA).
- Redirect Agent: Redirect Agents do not relay messages, and only return an answer with the information necessary for direct communication with destination. Redirect Agents do not modify messages. Since redirect agents do not receive answer messages, they cannot maintain session state. Further, since redirect agents never relay requests, they are not required to maintain transaction state. Since redirect agents do not perform any application level processing, they provide relaying services for all Diameter applications, and therefore must advertise the Relay Application Identifier. Example of Redirect agent is the SLF (Subscription Locator Function).
- Translation Agent: A Translation Agent translates between two protocols, such as RADIUS and Diameter or MAP and Diameter. In this case, the translation agent supports a RADIUS to Diameter migration, allowing server conversions to Diameter, for example, while permitting the NASes to be converted at a slower pace. Example of Translation agent is one which translates S6 Diameter Interface into Cx MAP interface because an HLR is deployed in Evolved Packet System instead of HSS.

In *KSS200* Diameter Relays and Redirect Agents are protocols transparent and transparently support the Diameter base protocol, which includes accounting and all Diameter applications. Also Diameter proxies support the base protocol, which includes accounting. In addition, they fully support each Diameter application that is needed to implement proxied services.

2-3-12- MySQL Database Management

The *KSS200* uses MySQL database management system. A database is a structured collection of system, subscribers and network data. Since servers handling large amounts of data, database management systems play a central role in computing, as standalone utilities, or as parts of other applications. MySQL is a relational database and stores data in separate tables rather than putting all the data in one big storeroom. The database structures are organized into physical files optimized for speed. The logical model, with objects such as databases, tables, views, rows, and columns, offers a flexible programming environment. By set up rules, it's possible to govern the relationships between different data fields, such as one-to-one, one-to-many, unique, required or optional, and"

pointers" between different tables. The database enforces these rules, so that with a well-designed database, system application never sees inconsistent, duplicate, orphan, out-of-date, or missing data. In *KSS200* MySQL runs on MDBS & BDBS.

2-3-13- Operation & Business Support System (OSS-BSS)

Operation and Business Support System (OMC & OSS-BSS) refers to the solution has been developed by KIATEL. The purpose of OSS-BSS is to ensure the normal running and operation of the system as well as attainment marketing purposes so as to provide high-quality telecommunication services for users.

KSS200 provides MML-based man machine operation environments in a graphic way where a number of OSS-BSS functions can be achieved. The OSS-BSS functions include maintenance management, data management, alarm management, charging and bill management, trace management, signaling analysis, traffic measurement, environment and power supply monitoring.

Here we explain topics of this system and detailed description have been provided in an independent document.

I. Maintenance management

Maintenance management provides multiple maintenance control methods such as query, display, switchover, reset, isolation, block and activation. By using these maintenance control methods, efficient management and maintenance operations can be performed on the hardware components, system resources, signaling links, clock links and physical ports of the *KSS200* as well as the gateways and terminals under its control.

II. Data management

Data management provides multiple database operation methods such as addition, deletion, modification, query, storage, backup and restoration. By using these database operation methods, efficient management and maintenance can be performed on the various data (including equipment data, gateway data, signaling data, routing data, charging data and subscriber data) which runs on the *KSS200*.

III. Alarm management

Alarm management receives and handles the variety of alarm information generated by the system. Depending on the category and severity level of the alarms, the appropriate alarm terminal device such as the alarm box or the alarm station will be driven to produce different audible and visual signals. Moreover, the corresponding alarm message will be interpreted and then transmitted to the network management center through the network management interface. In addition, alarm management also has the functions to store the alarm information, query the alarm history and set the alarm processing mode.

IV. Charging and bill management

Charging and bill management provides functions to manage and operate the bill information which is stored in the bill server hard disks. The functions include updating the host charging meters, getting bills from the host, querying the bills, backing up the bills, converting the bill format, sending the bills to the billing center.

V. Trace management

Trace management provides functions such as connection tracing, signaling tracing, interface tracing and message interpretation. By using these functions, a real-time and dynamic trace can be conducted on the connection process, state transition, resource occupancy, telephone number information transfer and control information streams relating to the terminal users, trunk circuits, signaling links and interface protocols. The tracing information can be preserved for future reference. In this way, powerful fault analysis and location capabilities can be provided for users.

VI. Signaling analysis

Signaling analysis provides a built in signaling analysis tool software which is developed independently by KIATEL. The software works along with the trace management functions to analyze the signaling interaction processes in an online or offline way. Signaling analysis provides strong maintenance approaches to quickly locate the cause of a fault and also to optimize the configuration of signaling links.

VII. Traffic measurement

Traffic measurement (traffic statistics) performs measurements and statistics on the services and objects of a variety of call types. By analyzing the statistical data, the running conditions of the *KSS200*, the gateways and the whole network can be known, which provides the basic data for the planning, design, operation, management and maintenance of the telecommunication network.

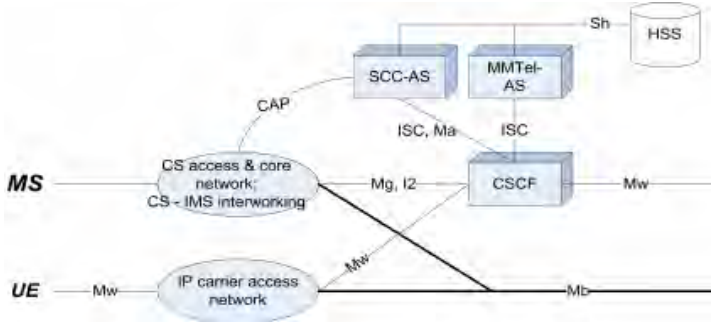
VIII. Environment and power supply monitoring

Environment and power supply monitoring performs monitoring and control, in a remote way, on the running environments, power supply devices and other intelligent devices.

2-3-14- Service Functions

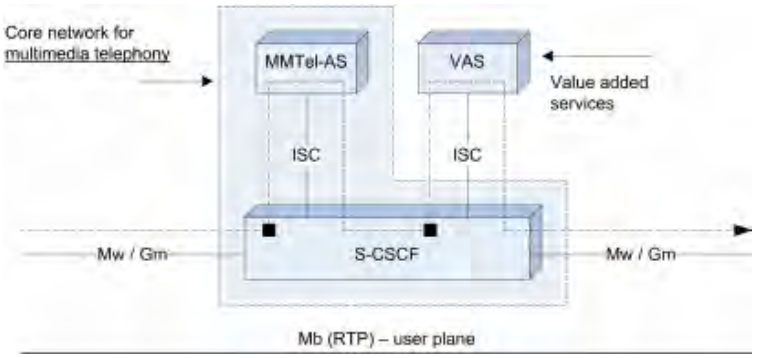
- SCC-AS

KSS200 IMS platform has intended supporting function for centralized services (ICS) allow for centralizing IMS services regardless of whether the mode of the network is circuit-switched (CS) or packet-switched (PS). The ICS function introduces a new entity in the IMS network, the service centralization and continuity application server (SCC-AS). The SCC-AS entity combines the SIP signaling and acts as a back-to-back user agent (B2BUA), providing an anchor point for incoming and outgoing calls. This implementation ensures continuity of service when the subscriber moves from one network in PS mode to a network in CS mode.



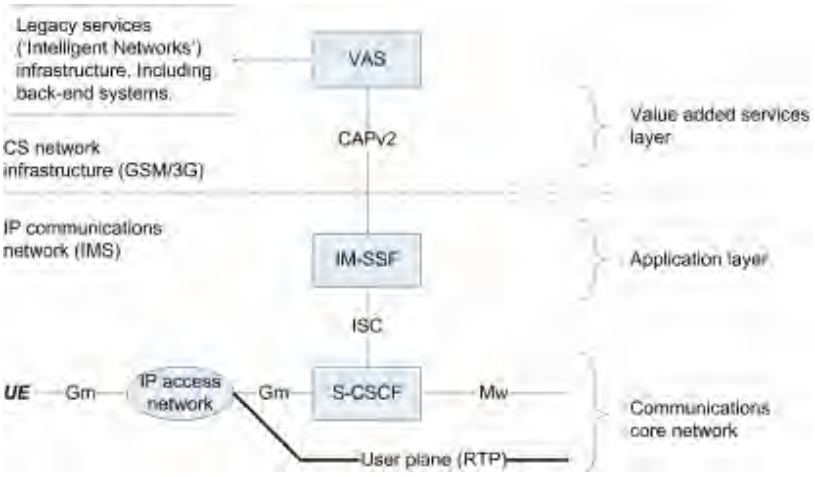
- MM-Tel

MM-Tel is a standardized solution to provide voice, video and other telephony services over LTE network (VoLTE). MM-Tel uses IMS to deliver voice, video and chat services to users. Along with that it specifies the way to share images, videos and files in real time.
KIATEL supports MM-Tel standard as it defined by 3GPP and ETSI/TISPAN. It is considered as the evolution of stereotyped fixed and mobile telephony service which is mostly dependent on circuit-switched technologies. MM-Tel is designed for All-IP networks with support for legacy systems.



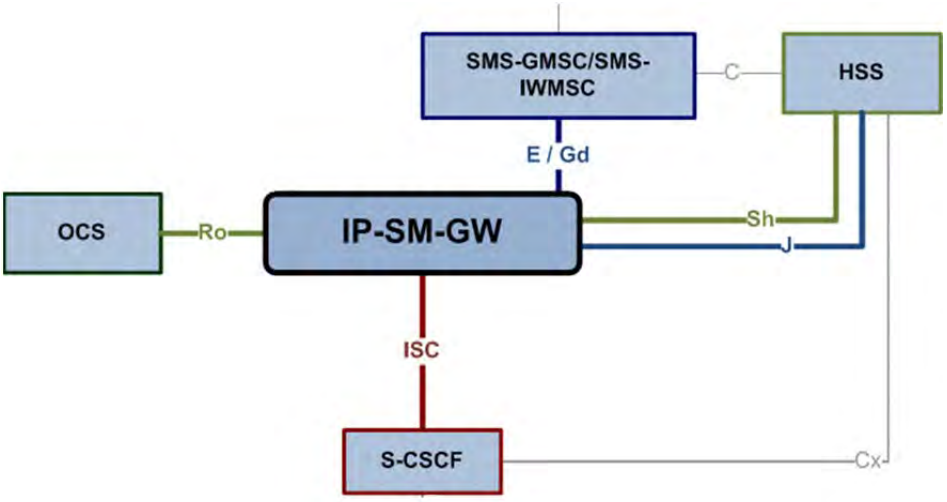
- IM-SSF

Based on the aforementioned view that IMS core network provides communication connectivity and facilitates services such as multi-media telephony and based on the capability of a SIP-AS, *KSS200* has special function module to support IM-SSF.
The IM-SSF acts as SIP-AS. Hence, from IMS point of view, it's an application server that may apply Value added services (VAS). The IM-SSF is built to act as 'converter' between SIP (between S-CSCF and IM-SSF) and CAP (between IM-SSF and IN service). In this manner, existing IN service could be applied to IMS network based IP telephony. IM-SSF is, in practice, deployed rather as embedded capability than as independent functional entity. Embedded capability, in the sense that it (the IM- SSF) is integrated in a SIP-AS that comprises also other functionality, such as multimedia telephony.



- IP-SM_GW

KSS200 provides needed function to support the IP Short Message Gateway which handles SIP based messaging services for IMS subscribers. In addition, the IP-SM_GW will interact with the legacy SMSC using MAP signaling in order to allow IMS to SMS conversion and distribution.



Chapter 3 Interfaces, Signaling and Protocols

3.1 Interface Types

KSS200 supports GE and FE interfaces in both electrical and optical connections. The quantity and purpose of the interfaces are related to system capacity and network configuration.

Table 2-6 shows specifications of *KSS200* network interfaces.

Table 2-6 *KSS200* Network Interfaces

Item	Parameter
Interface Equipment	2 or 3 Layer network switch
Compliant recommendation or standard	● IEEE 802.1s ● IEEE 802.1w ● IEEE 802.1x ● IEEE 802.3ad ● IEEE 802.3af ● IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports ● IEEE 802.1D Spanning Tree Protocol ● IEEE 802.1p CoS classification ● IEEE 802.1Q VLAN ● IEEE 802.3 10BASE-T ● IEEE 802.3u 100BASE-T ● IEEE 802.3ab 1000BASE-T ● IEEE 802.3z 1000BASE-X
Transfer rate	10/100/1000Mbit/s self-adaptation
Transferable distance	100 m
Interface types	●10BASE-T ports: RJ-45 connectors, CAT-5 or 6 STP or UTP cabling ● 100BASE-TX ports: RJ-45 connectors, 2-pair Cat-5 or 6 STP or UTP cabling ● 1000BASE-T ports: RJ-45 connectors, 2-pair Cat-5 or 6 STP or UTP cabling ● 1000BASE-T SFP-based ports: RJ-45 connectors ● 1000BASE-SX, -LX/LH, -ZX, and CWDM SFP-based ports: LC fiber connectors (single mode, or multimode fiber) ● 10GBASE-ER XENPAK-based port (single-mode) ● 10GBASE-LR XENPAK-based port (single-mode) ● Management console port: RJ-45-to-DB9 cable for PC connections
Nominal impedance	100 Ω

3.2 Signaling and Protocols

KSS200 provides open and standard protocol interfaces and supports a number of signaling and protocols, thus achieving interconnection or interworking with a variety of devices.

Main signaling and protocols supported by *KSS200* are shown in below table.

Protocol	Purpose	Compliant recommendation or standard
MGCP	Media gateway control protocol, used for *KSS200* to control the media gateways and also to access MGCP packet terminals.	IETF, RFC2705, Media Gateway Control Protocol (MGCP) Version 1.2
H.248	Media gateway control protocol, used for *KSS200* to control the media gateways and also to access H.248 packet terminals.	IETF, RFC3015, Megaco Protocol Version 1.0 (H.248)
SIP	Session initiation protocol, used for the interconnection between *KSS200* and other IMS or SIP application servers and also to access SIP multimedia packet terminals.	IETF, RFC3261, Session Initiation Protocol (SIP)
SIP-T	The extension protocol of SIP, used for the transparent transfer of ISUP signaling.	IETF, RFC3372, Session Initiation Protocol for Telephones (SIP-T)
H.323	IP call and multimedia communication protocol, used for the interconnection between *KSS200* and Gateways in the traditional H.323 network and also to access H.323 multimedia packet terminals.	ITU-T, H.323, Packet-based multimedia communications systems
SIGTRAN	SCTP, used to provide the reliable data packet transfer service for the adaptation protocols of IP-based Switched Circuit Network (SCN) signaling.	IETF, RFC2960, Stream Control Transmission Protocol (SCTP)
	M2UA used for the interconnection between *KSS200* and Gateways with built-in signaling gateway functions.	IETF, RFC3331, SS7 MTP2 User Adaptation Layer (M2UA)
	M3UA used for the interconnection between *KSS200* and signaling gateway functions.	IETF, RFC3332, SS7 MTP3-User Adaptation Layer (M3UA)
	V5UA used for the interconnection between *KSS200* and UMGs with built-in V5.2 signaling gateway functions.	IETF, draft-ietf-sigtran-v5ua-03, V5.2-User Adaptation Layer (V5UA)
	IUA used for the interconnection between *KSS200* and gateway with built-in DSS1 signaling gateway functions.	IETF, RFC3057, ISDN Q.921-User Adaptation Layer (IUA)
R2	A type of inter-office channel associated signaling, used for the interworking between *KSS200* and exchanges of old mode so that *KSS200* can provide R2 trunks through gateways.	ITU-T, Q.400 to Q.499
STUN	Used to support the interconnection between *KSS200* and STUN Servers.	IETF, draft-ietf-midcom-stun-02, Simple Traversal of UDP Through Network Address Translators (STUN)

SS7	MTP used for the interworking between *KSS200* and the SS7 signaling network so that *KSS200* can be interconnected to SPs or STPs in the SS7 signaling network.	ITU-T Q.701 to Q.707
	TUP used for the interworking between *KSS200* and the PSTN network so that *KSS200* can provide TUP trunks through TMG to interconnect with PSTN exchanges.	ITU-T Q.721 to Q.725
	ISUP used for the interworking between *KSS200* and the PSTN so that *KSS200* can provide ISUP trunks through TMGs and achieve the interconnection with PSTN exchanges.	ITU-T Q.761 to Q.764, Q.730
	SCCP used to bear the INAP protocol so that *KSS200* can be interconnected to SCPs in the IN through the SS7 signaling network.	ITU-T Q.711 to Q.716
	TCAP used to provide the applications of *KSS200* and SCPs with a number of functions and procedures which are not application specific, so that *KSS200* can support the applications pertaining to IN services.	ITU-T Q.771 to Q.775
	INAP used to define the information streams between the functional entities of the IN so that *KSS200* can support the Service Switching Function (SSF), the Call Control Function (CCF), the Specialized Resource Function (SRF) and the Call Control Access Function (CCAF) and act as the SSP over the standard IN architecture.	ITU-T Q.1218, Q.122x, Q.123x ITU-T X.208, X.209
V5.2	Subscriber network signaling used for the interworking between *KSS200* and the V5.2 access network or base station controllers so that *KSS200* can provide V5.2 interfaces through gateways.	ITU-T G.964, G.965
IPSec	Used to protect the security of communications between *KSS200* and the gateways under its control, such as IADs, access gateways, trunk gateways and RGWs.	IETF, RFC2401, Security Architecture for IP (IPSec) IETF, RFC2402, IP Authentication Header (IPSec) IETF, RFC2406, IP Encapsulating Security Payload (IPSec) IETF, RFC2411, IP Security Document Roadmap (IPSec)
SNMP	Used to support the interconnection between *KSS200* and NMS devices so that *KSS200* can provide network management interfaces (SNMP interfaces).	IETF, RFC1157, Simple Network Management Protocol (SNMP)
FTP	Used to support the interconnection between *KSS200* and billing centers so that *KSS200* can provide FTP interfaces.	IETF, RFC0959, File Transfer Protocol (FTP)
FTAM	Used to support the interconnection between *KSS200* and billing centers so that *KSS200* can provide FTAM interfaces.	ISO, ISO8571, File Transfer Access and Management Protocol (FTAM)

Chapter 4 Services and Functions

4.1 *KSS200* Services

KSS200 as the IMS platform provides following services for users:

I. The basic services including voice services, supplementary services, IP Centrex service and IPN service.

II. Enhanced services by means of supporting protocols:

- By interconnecting with the SCP through the INAP protocol, *KSS200* can completely inherit the existing voice intelligent network services such as FPH, ACC, VPN and UPT.
- By interconnecting with the SIP application module through the SIP protocol, *KSS200* can provide a number of value added services which integrate voice, multimedia and Internet, such as Unified Messaging (UM), Instant Messaging (IM), IP800, presence, Personal Communication Assistant (PCA).
- By interconnecting with application servers through a Parlay gateway, *KSS200* can provide third-party or customized services, such as enterprise workflow, enterprise schedule, personal schedule and enterprise package.

Following are *KSS200* services descriptions.

4.1.1 Voice Services

I. Basic voice services

KSS200 supports the basic voice services made among PSTN telephone terminals, MGCP packet terminals, H.248 packet terminals, SIP packet terminals and H.323 packet terminals.

1) Telephony calls made between the local network subscribers, including the urban subscribers, the rural subscribers and the town subscribers in the local network.

2) National /international toll auto direct dialing outgoing calls and national/international toll auto incoming calls.

3) Special service calls, including inquiry, complaint and fire emergency services.

4) Calls made both directly to PBX extensions and to PBX console.

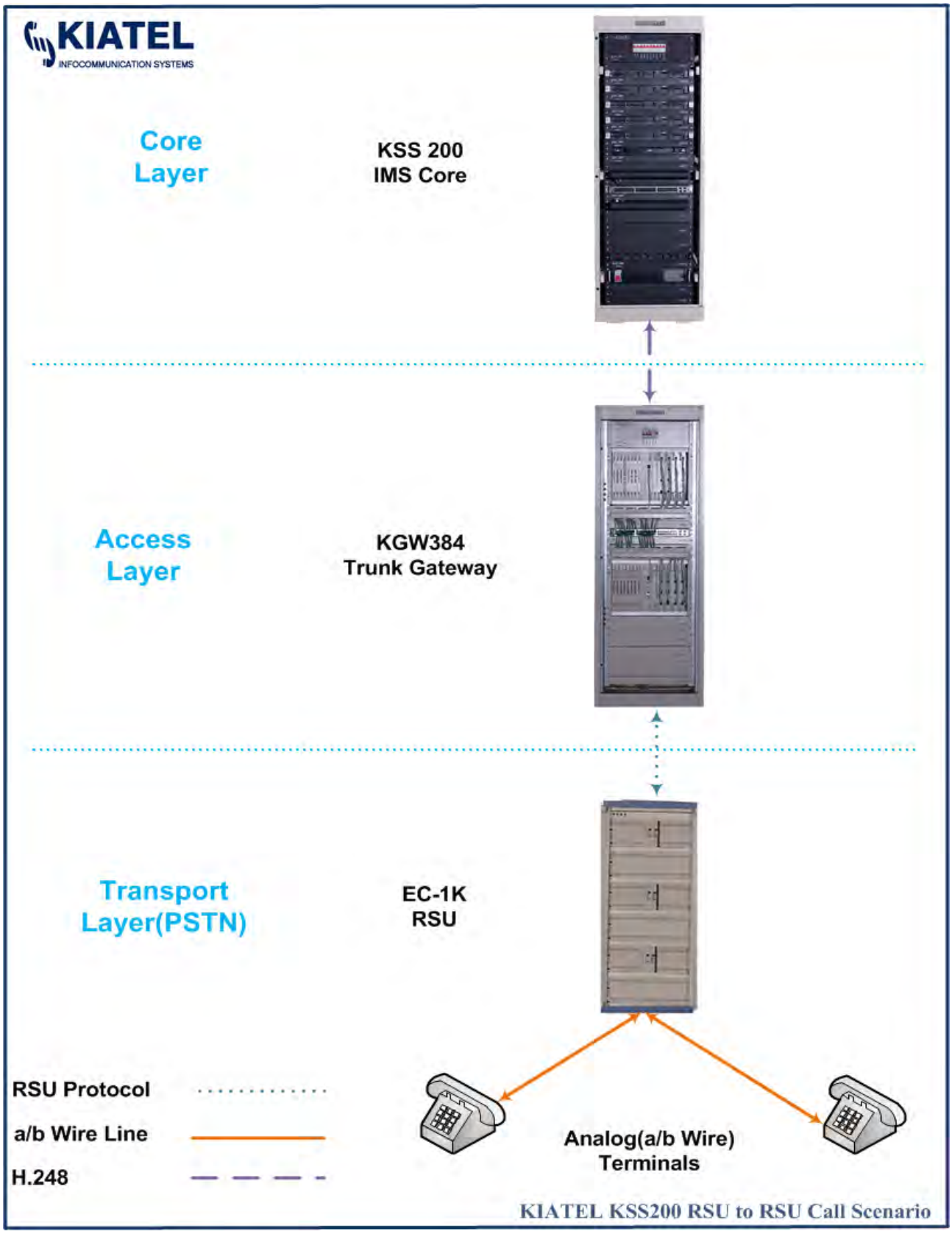
5) Calls made from PBX extensions directly out.

6) Calls made with mobile subscribers and made to wireless paging subscribers.

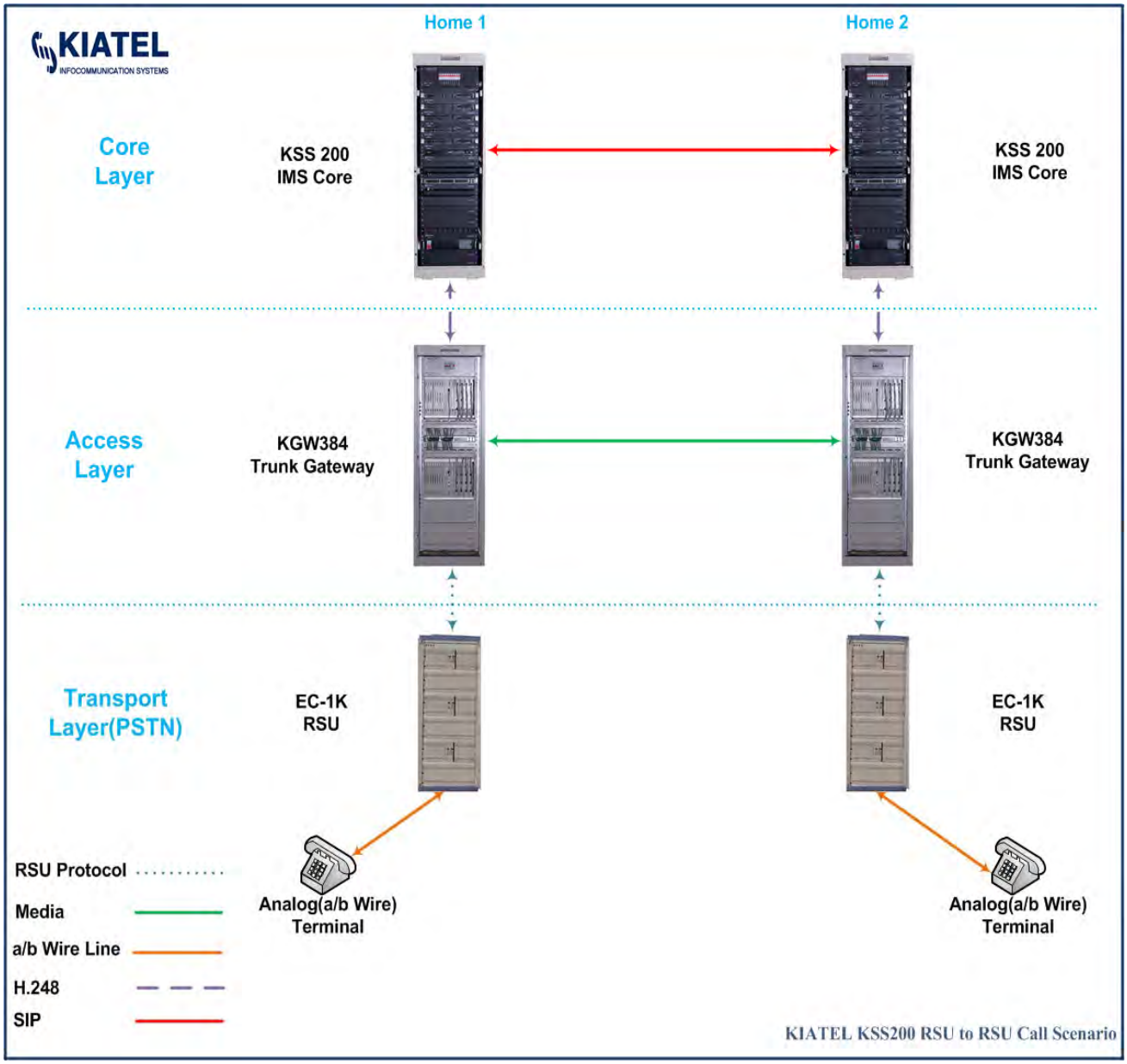
7) Operation calls provided for the maintenance operation personnel.

Call Scenarios and Call flow types for voice services are shown in next pages.

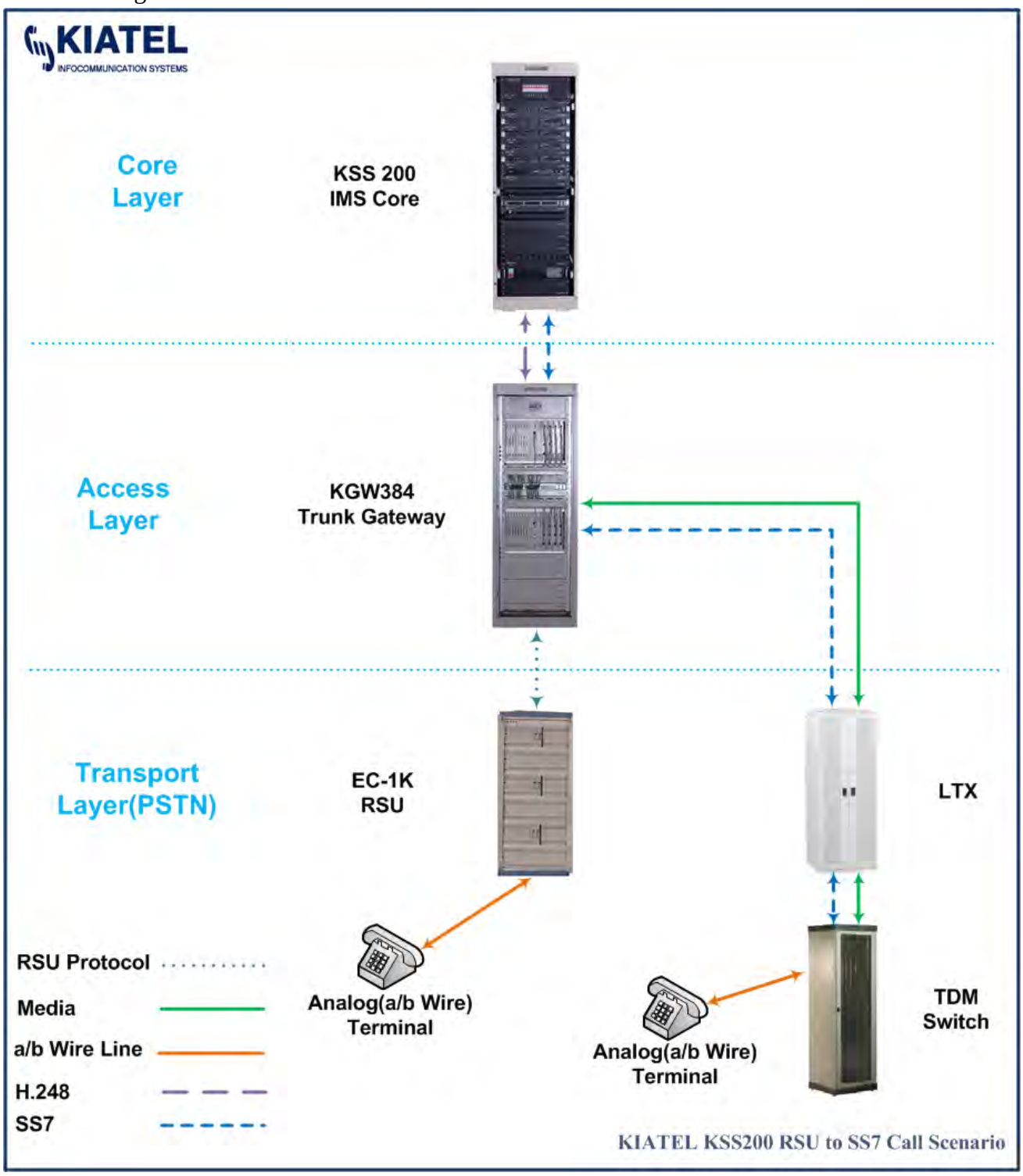
- A PSTN subscriber (via RSU) to PSTN subscriber (via RSU) Call Scenario- Both subscribers are belong to same Home.



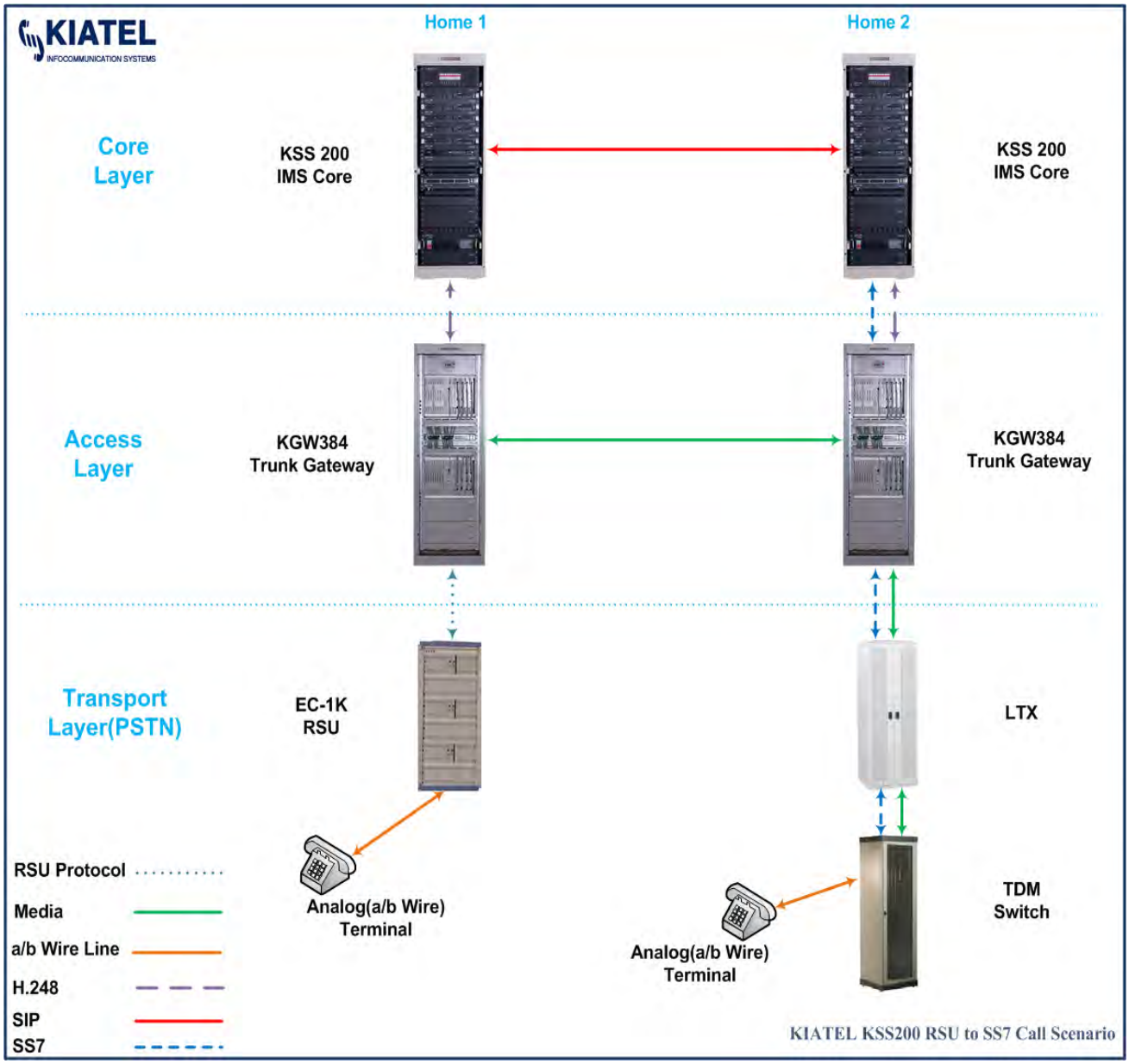
- A PSTN subscriber (via RSU) to PSTN subscriber (via RSU) Call Scenario- Subscribers are belong to different Homes.



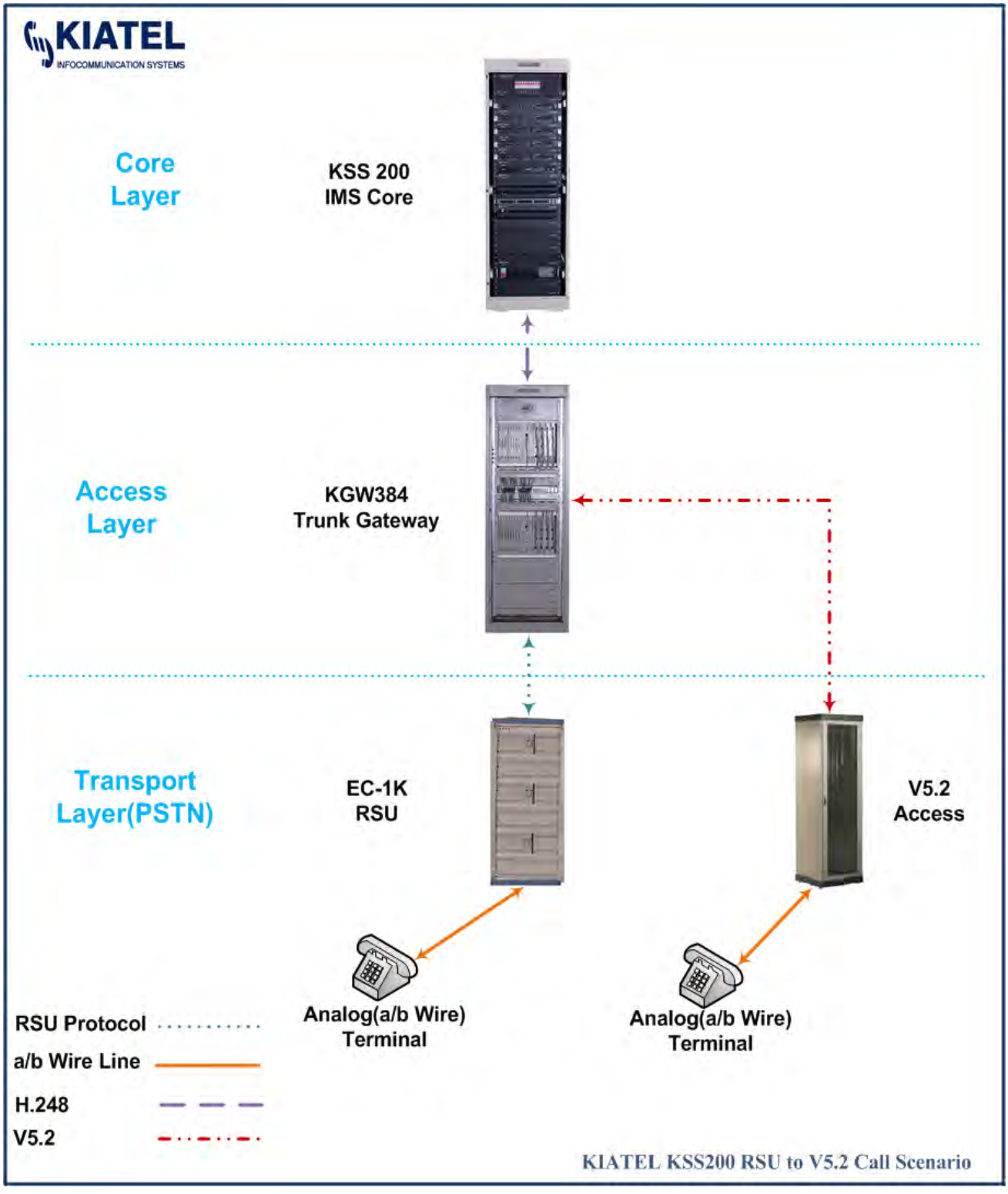
- A PSTN subscriber (via RSU) to SS7 switch subscriber Call Scenario- Both subscribers are belong to same Home.



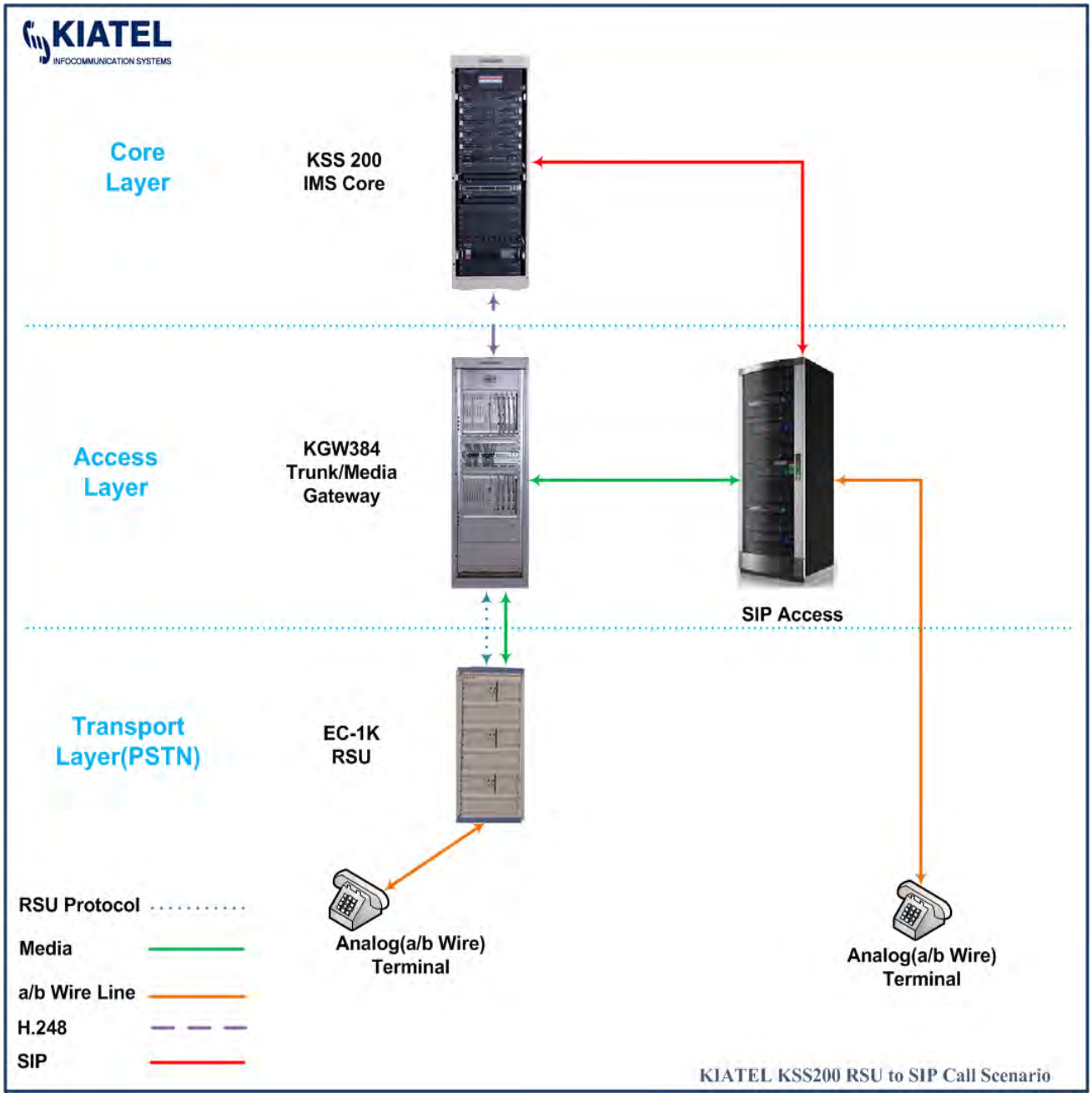
- A PSTN subscriber (via RSU) to SS7 switch subscriber Call Scenario- Subscribers are belong to different Homes.



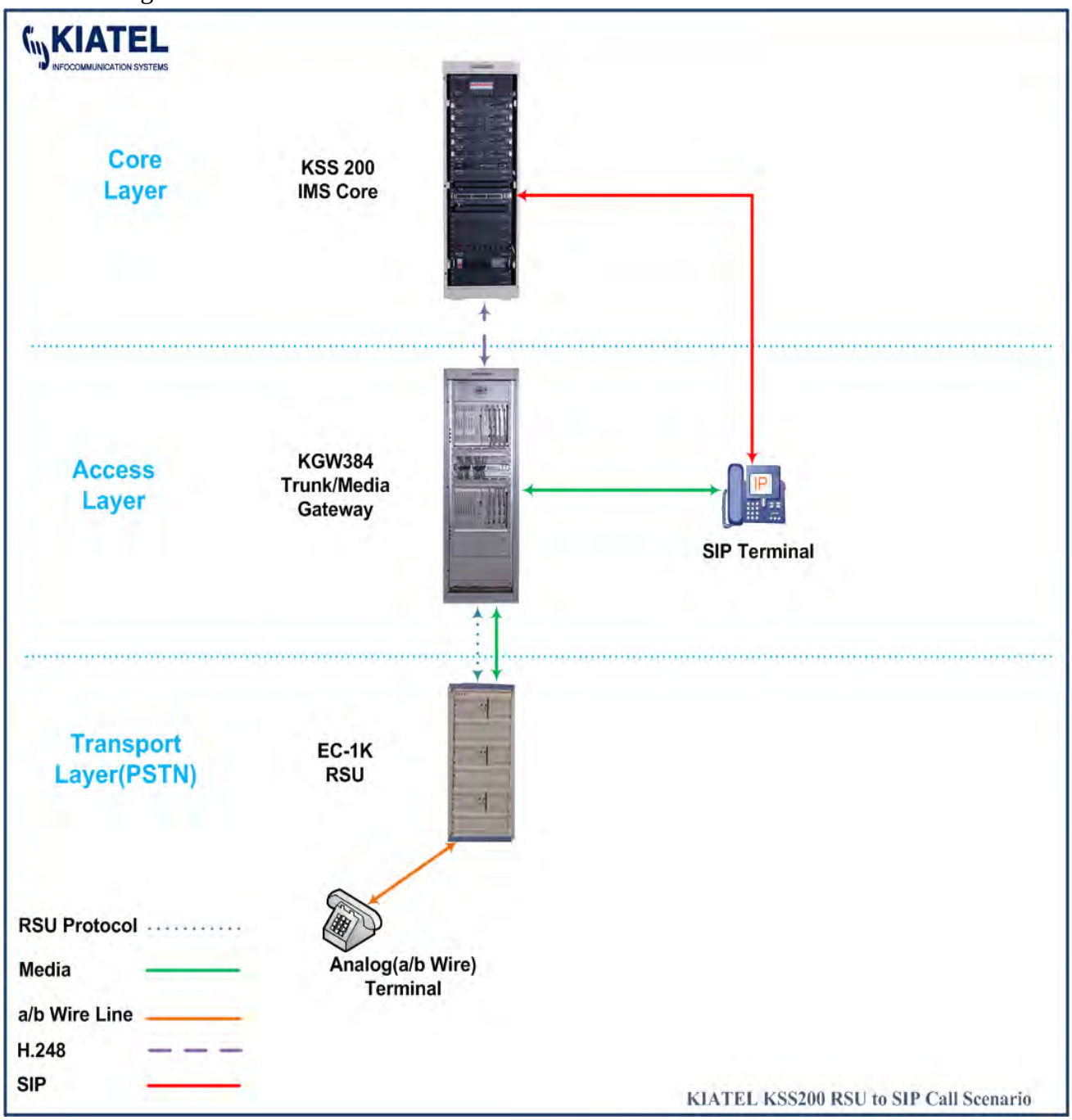
- A PSTN subscriber (via RSU) to V5.2 access subscriber Call Scenario- Both subscribers are belong to same Home.



- A PSTN subscriber (via RSU) to SIP subscriber type 1 Call Scenario- Both subscribers are belong to same Home.

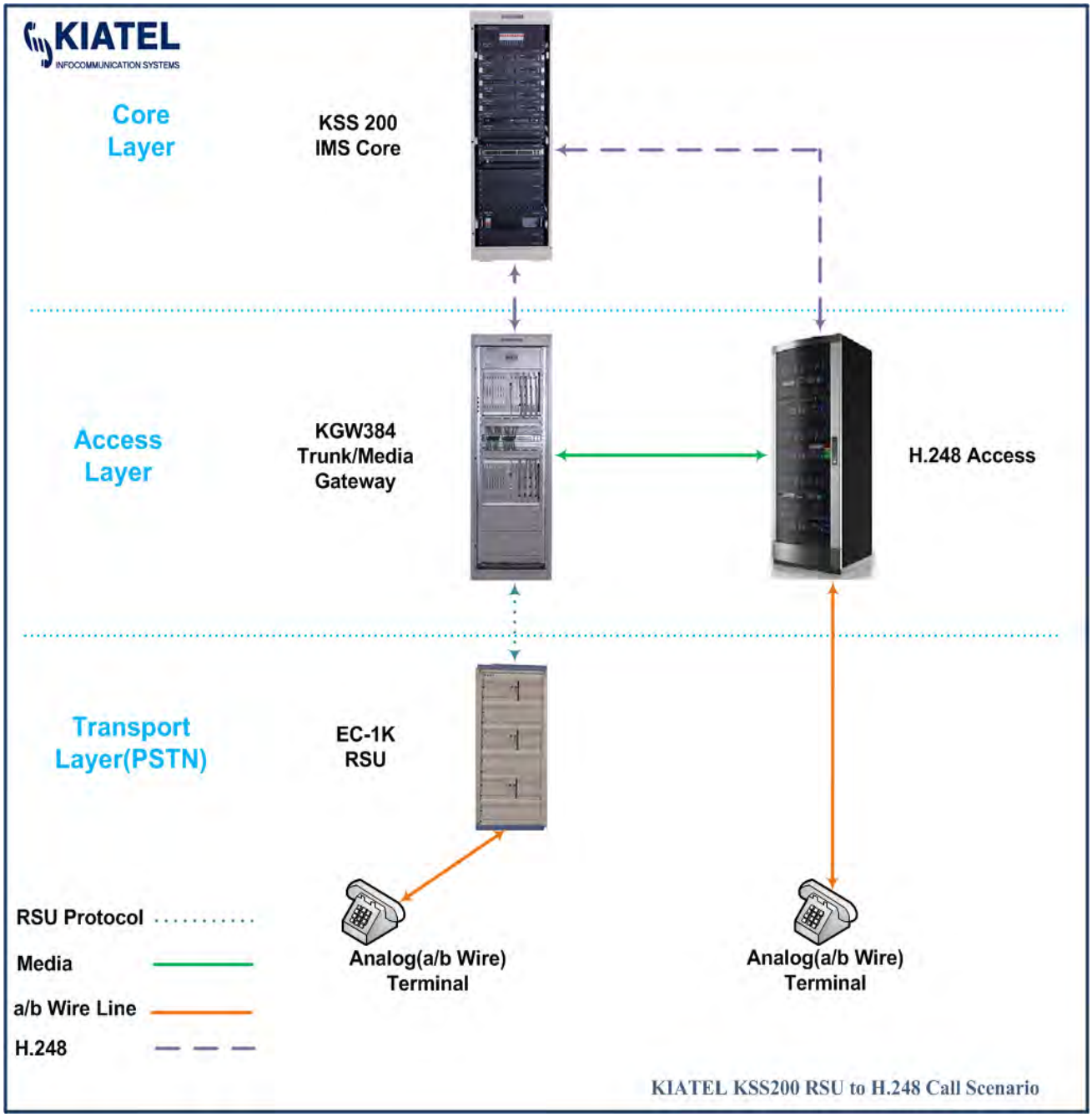


- A PSTN subscriber (via RSU) to SIP subscriber type 2 Call Scenario- Both subscribers are belong to same Home.

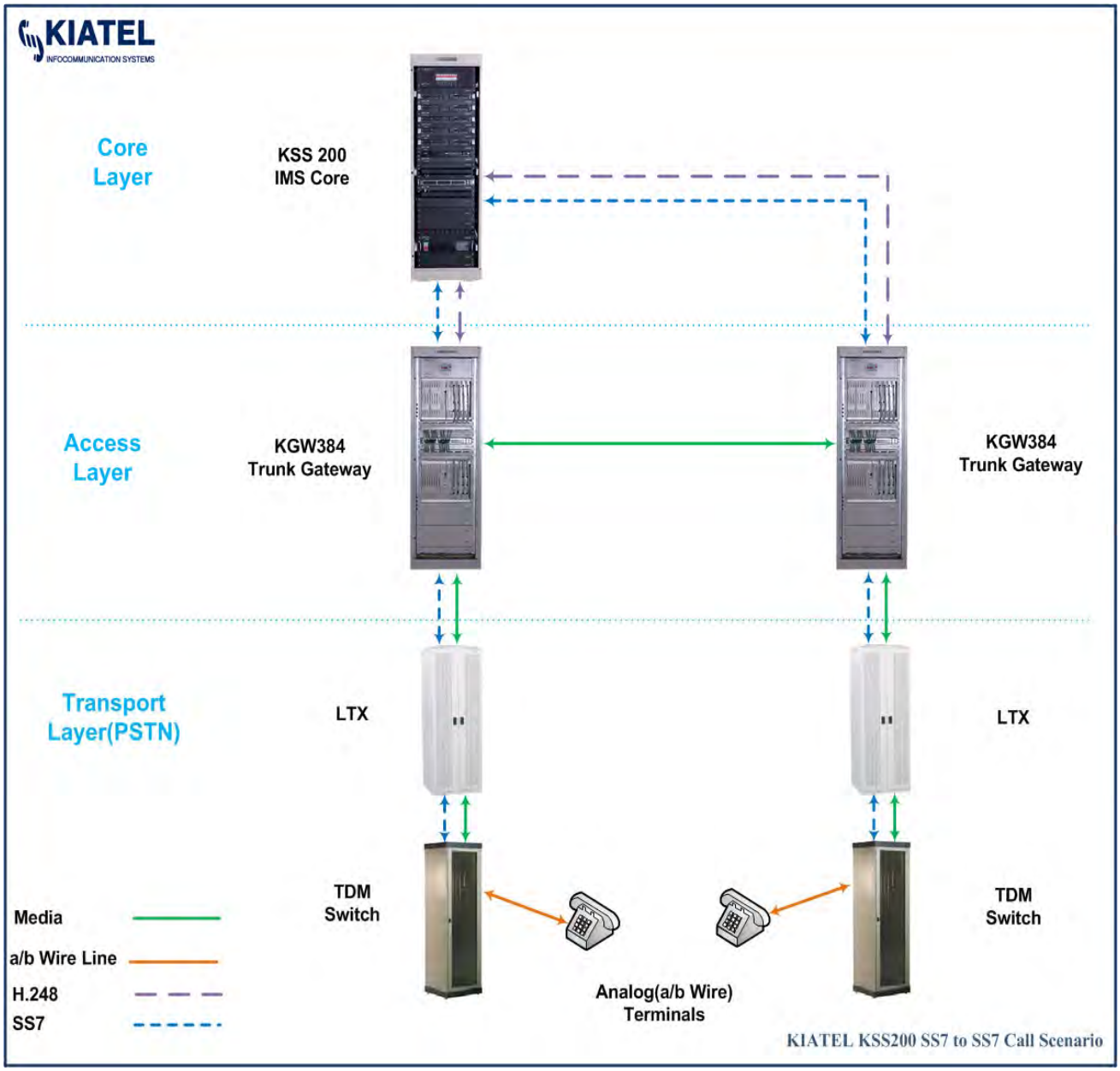


In this scenario, SIP terminal is connected to IMS Core and MGW via network access switch.

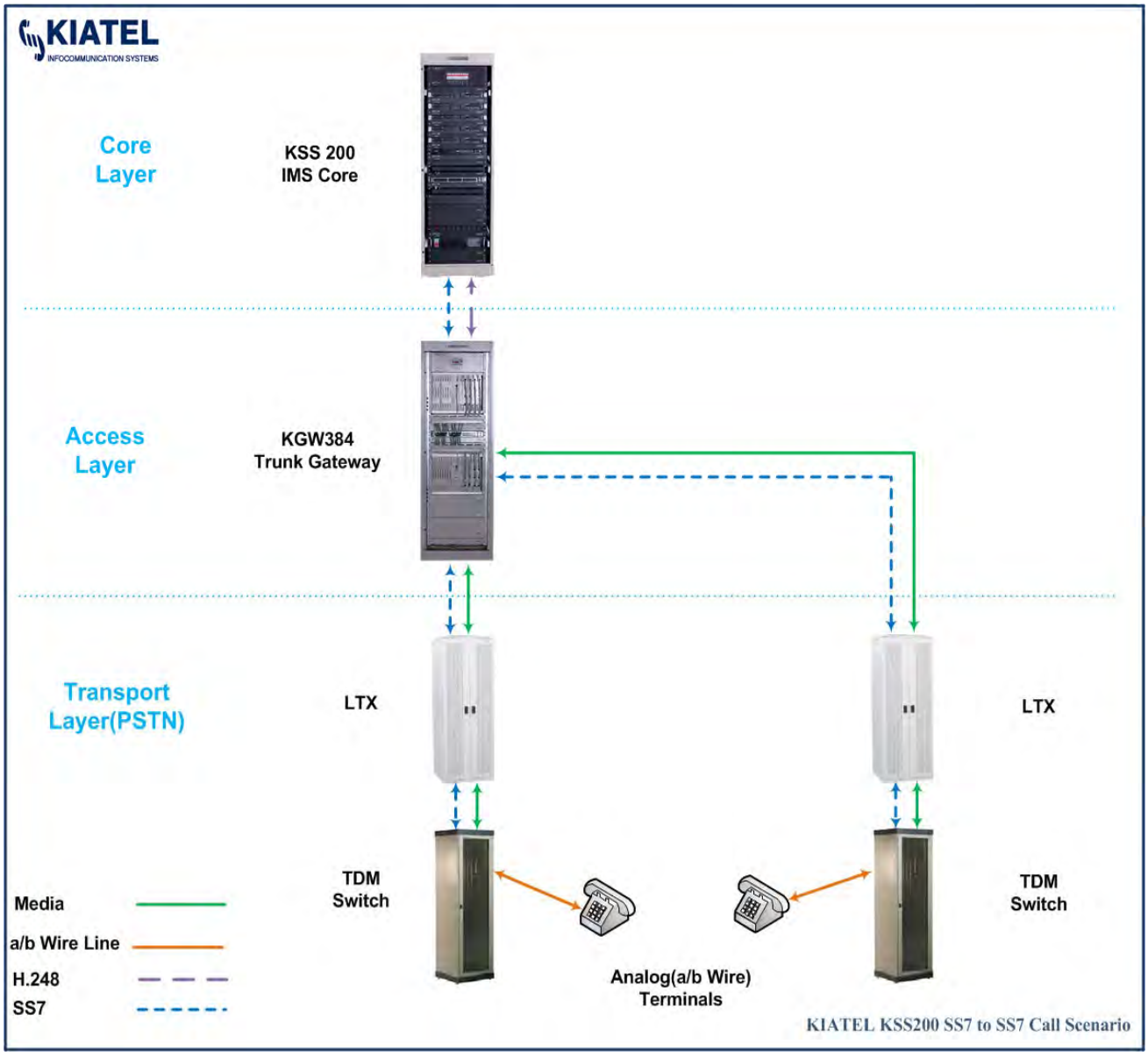
- A PSTN subscriber (via RSU) to H.248/Megaco subscriber Call Scenario- Both subscribers are belong to same Home.



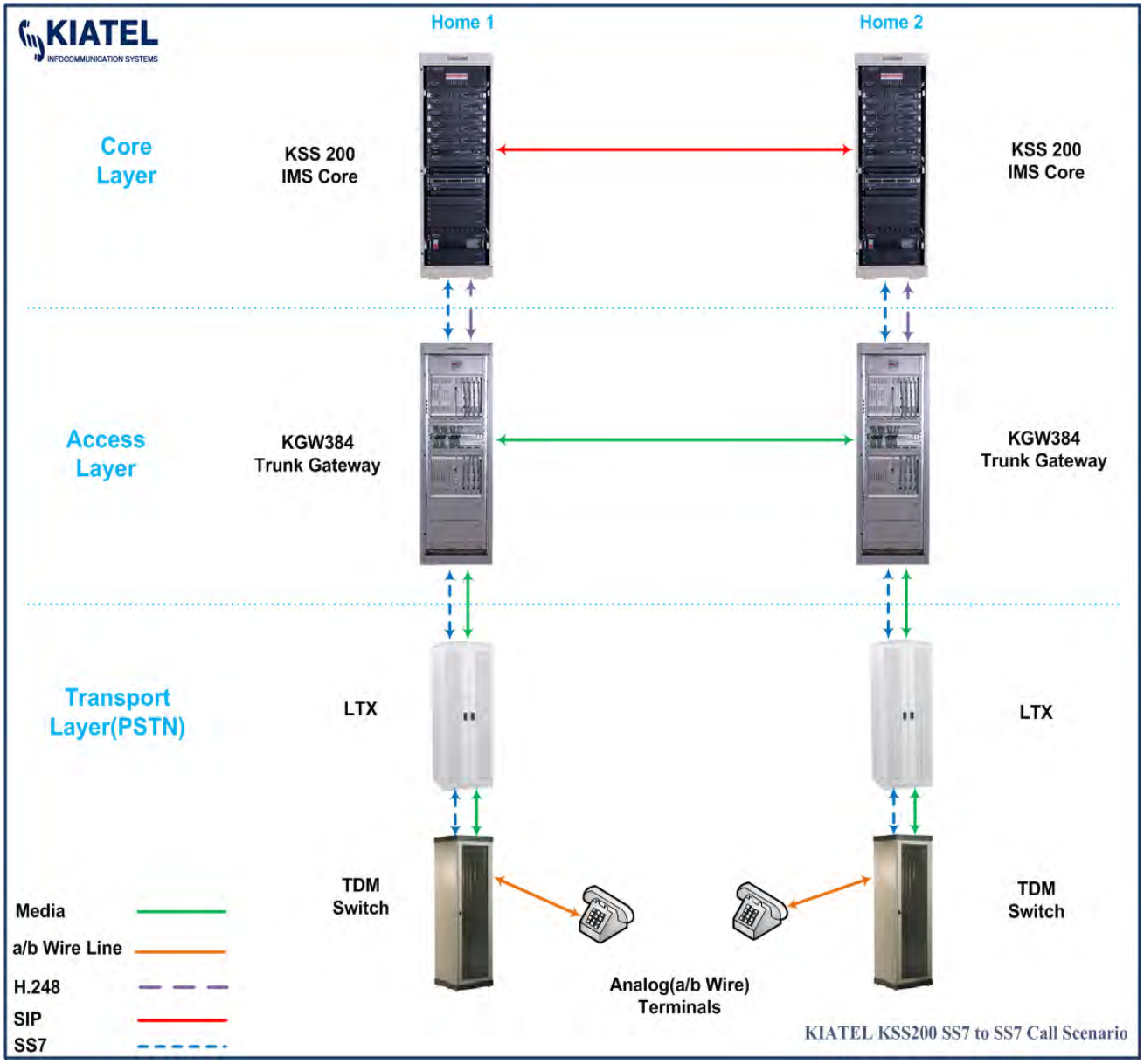
- A SS7 switch subscriber to SS7 switch subscriber type 1 Call Scenario- Both subscribers are belong to same Home.



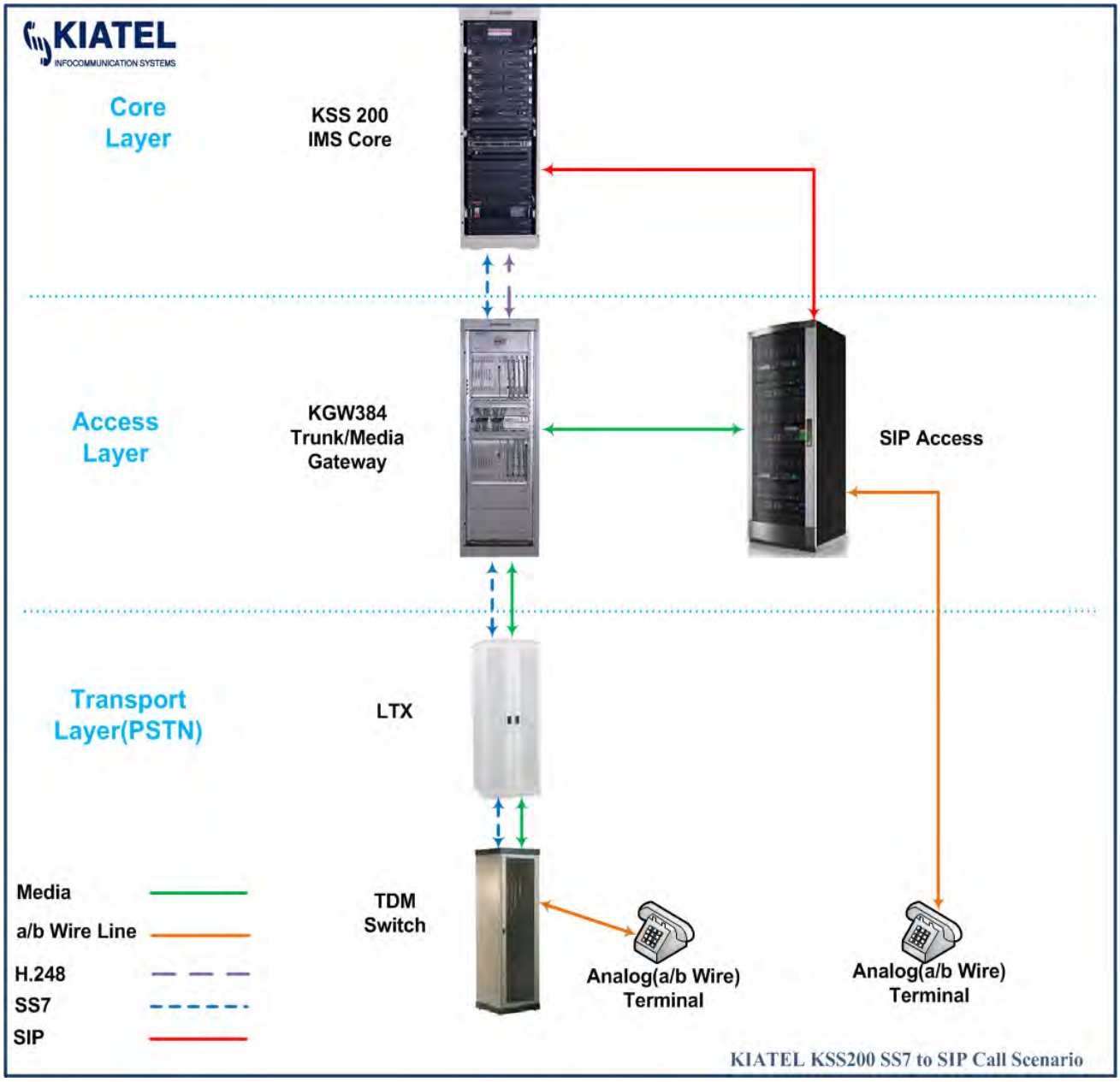
- A SS7 switch subscriber to SS7 switch subscriber type 2 Call Scenario- Both subscribers are belong to same Home.



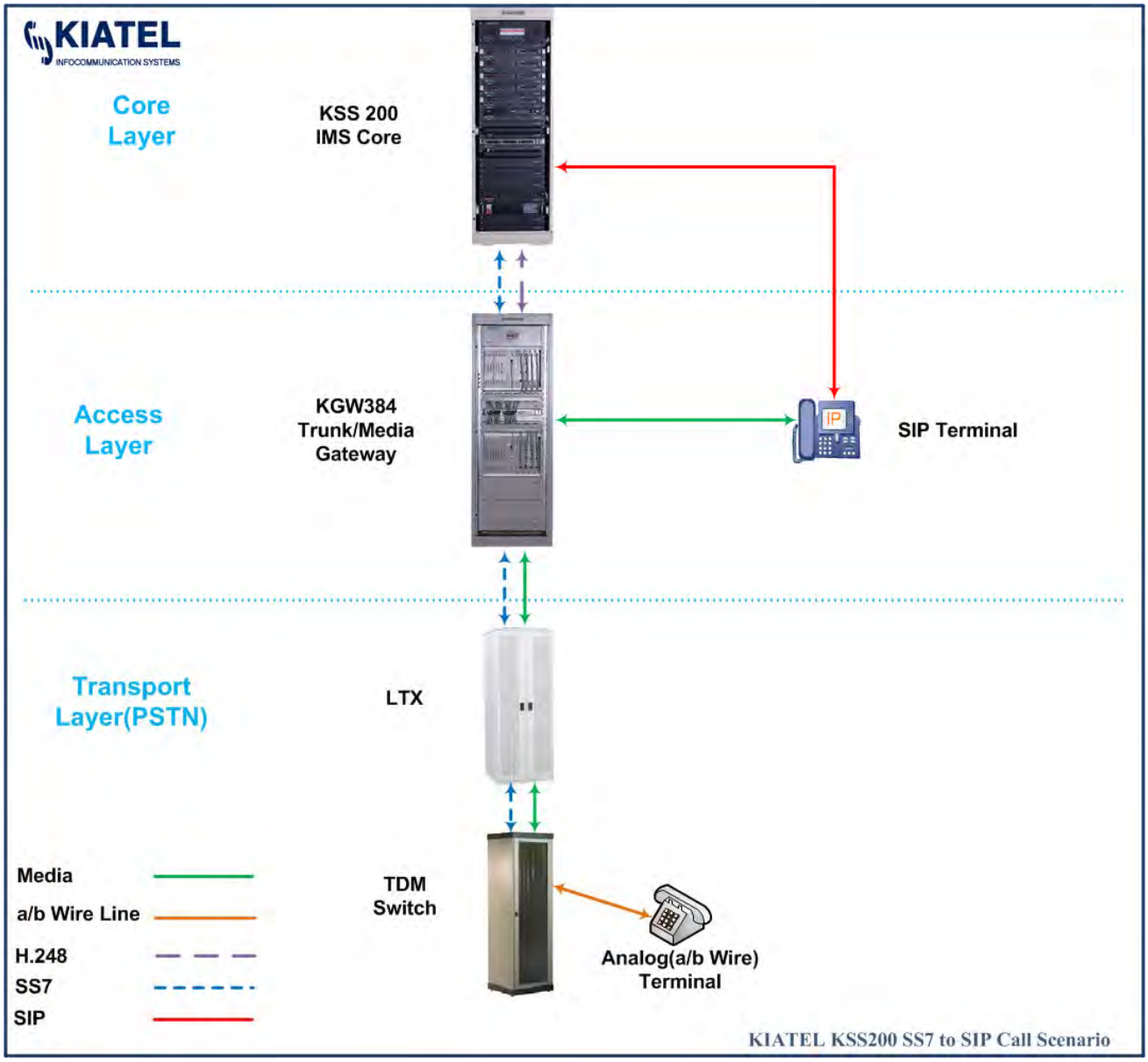
- A SS7 switch subscriber to SS7 switch subscriber Call Scenario- Subscribers are belong to different Homes.



- A SS7 switch subscriber to SIP subscriber type 1 Call Scenario- Both subscribers are belong to same Home.

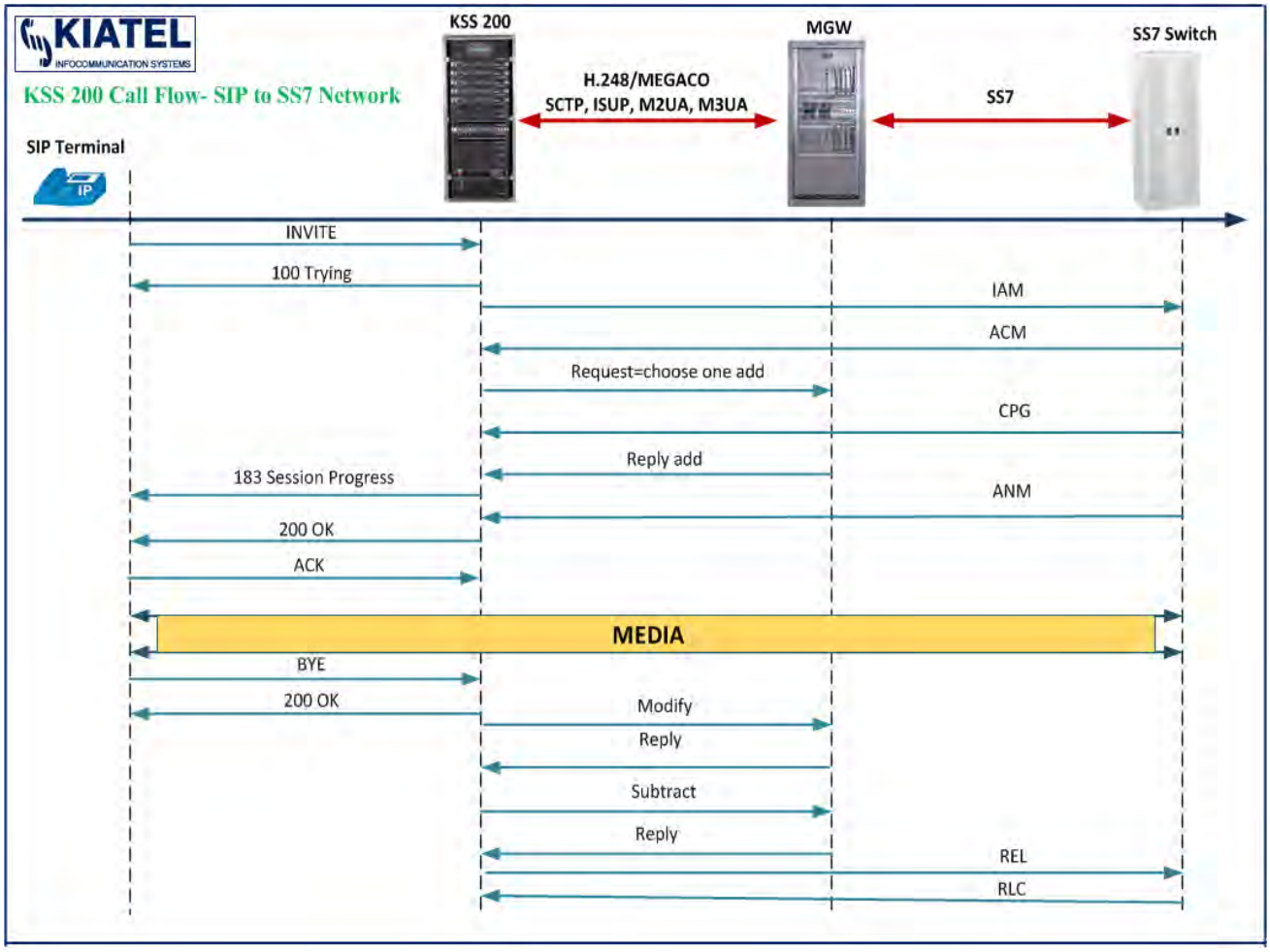


- A SS7 switch subscriber to SIP subscriber type 2 Call Scenario- Both subscribers are belong to same Home.

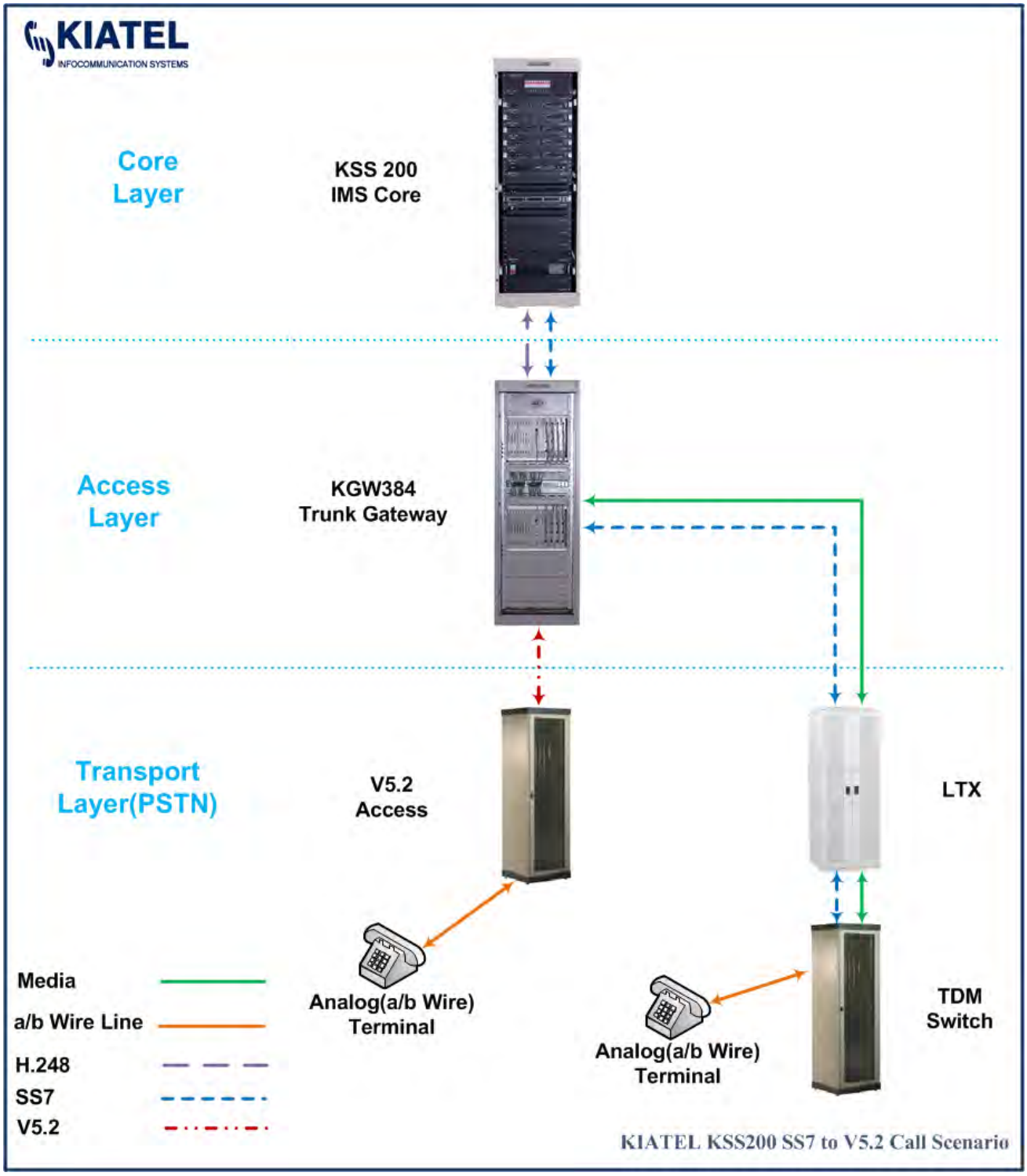


In this scenario, SIP terminal is connected to IMS Core and MGW via network access switch.

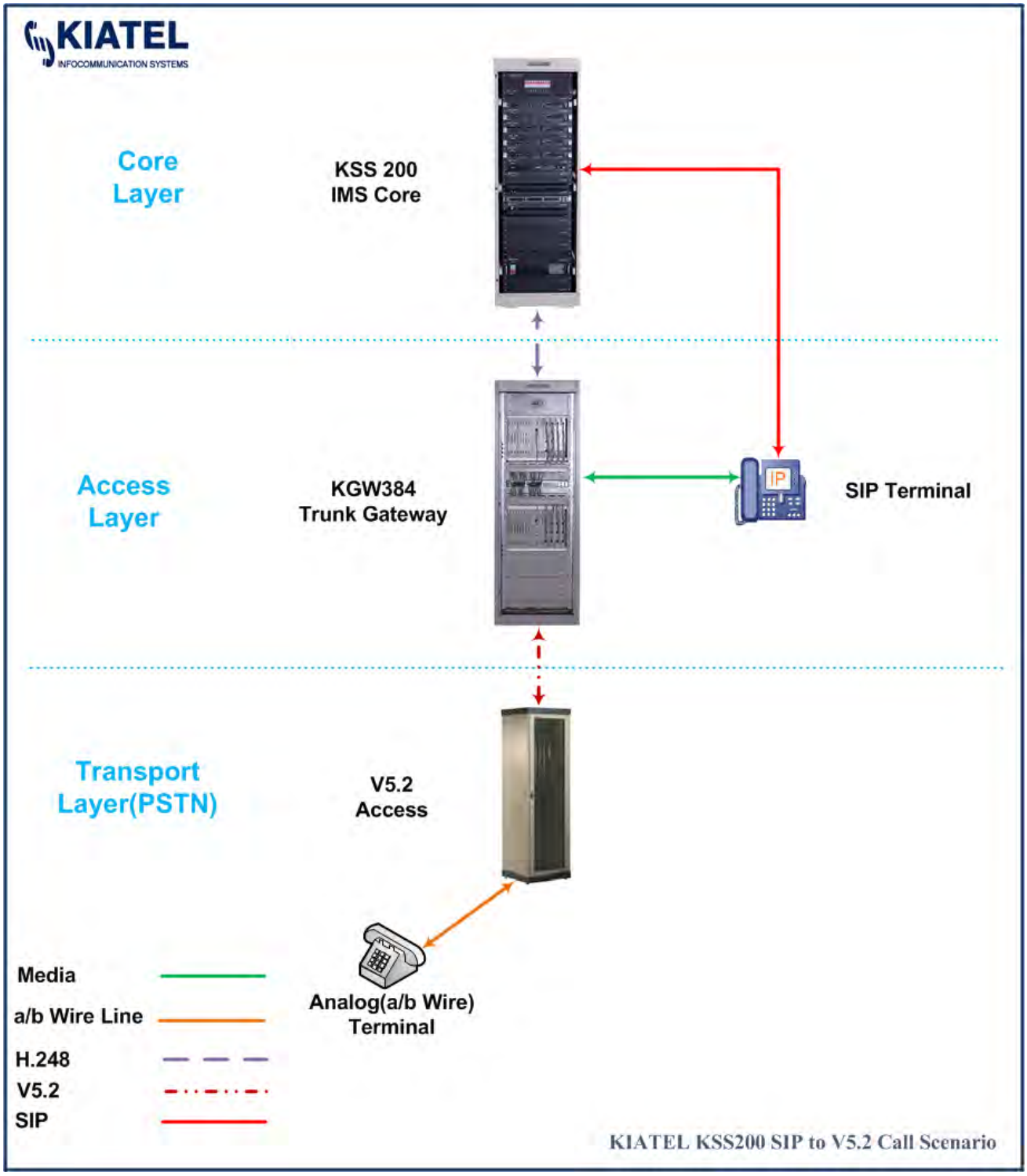
The transaction of signaling messages and media packets is shown in next page diagram.


KIATEL
INFOCOMMUNICATION SYSTEMS
KSS 200 Call Flow- SIP to SS7 Network
SIP Terminal
KSS 200
H.248/MEGACO
SCTP, ISUP, M2UA, M3UA
MGW
SS7
SS7 Switch
INVITE
100 Trying
IAM
ACM
Request=choose one add
CPG
Reply add
183 Session Progress
ANM
200 OK
ACK
MEDIA
BYE
200 OK
Modify
Reply
Subtract
Reply
REL
RLC

- A SS7 switch subscriber to V5.2 access subscriber Call Scenario- Both subscribers are belong to same Home.

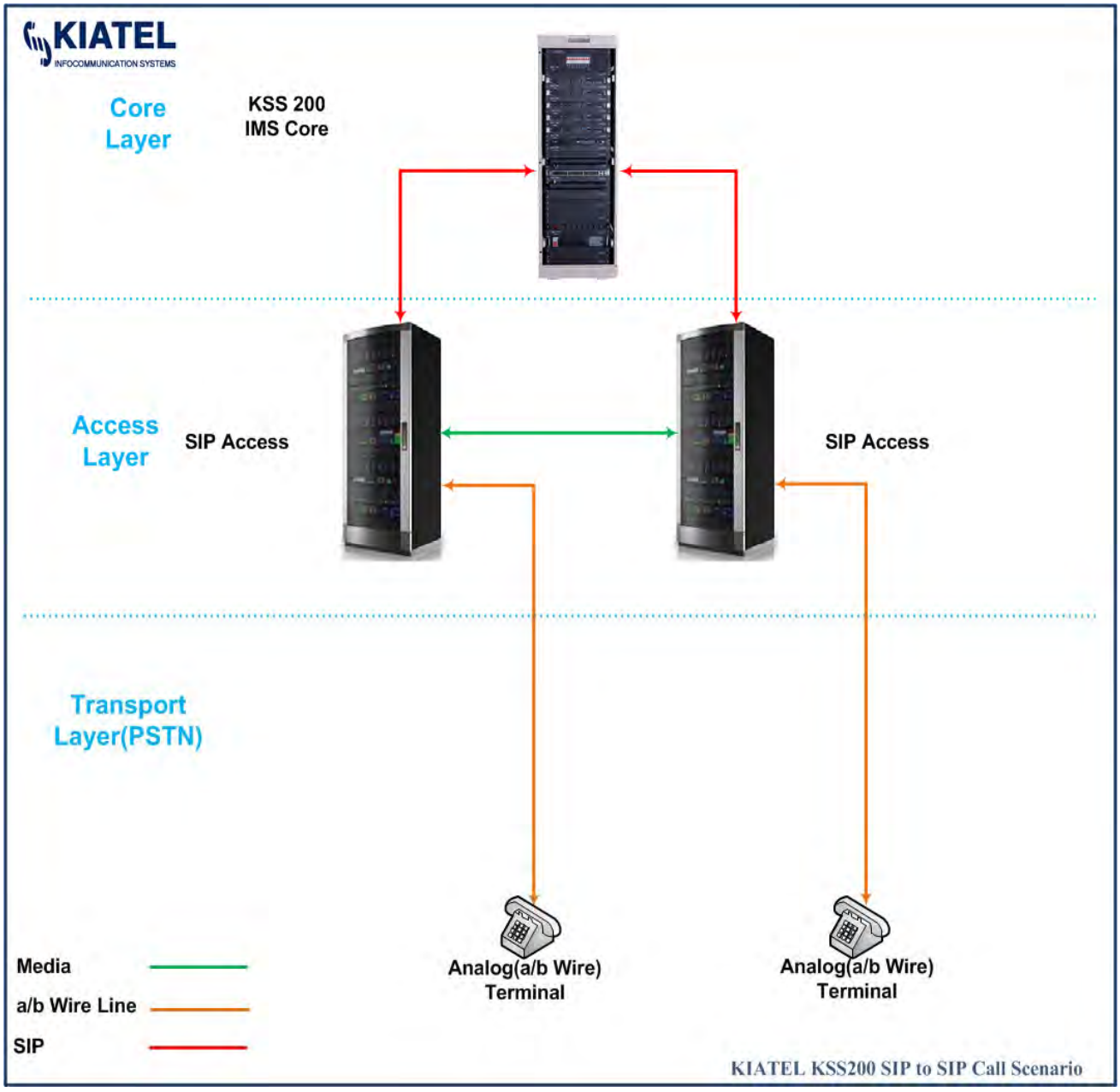


- A SIP subscriber to V5.2 access subscriber Call Scenario- Both subscribers are belong to same Home.

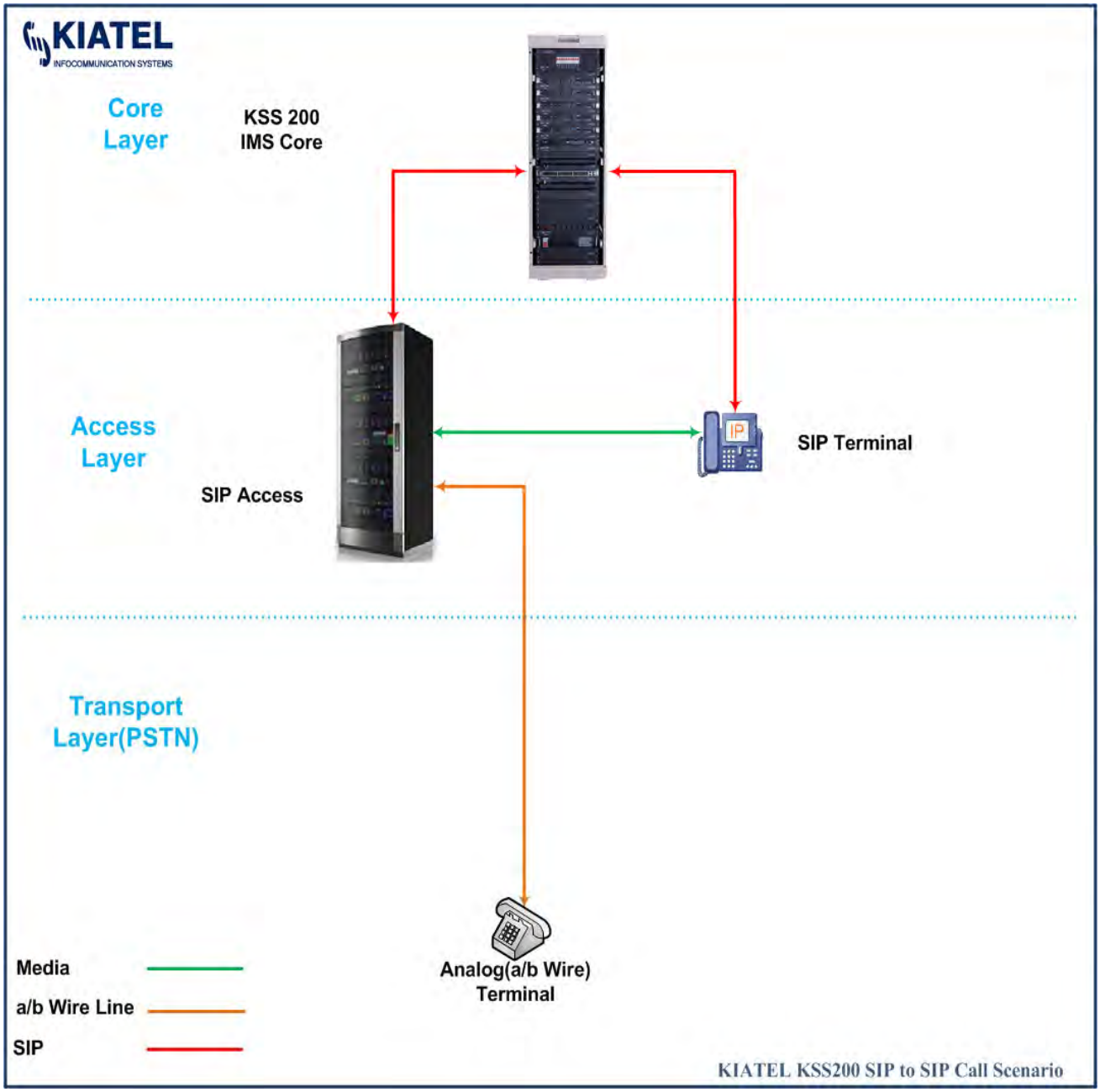


In this scenario, SIP terminal is connected to IMS Core and MGW via network access switch.

- A SIP subscriber to SIP subscriber type 1 Call Scenario- Both subscribers are belong to same Home.

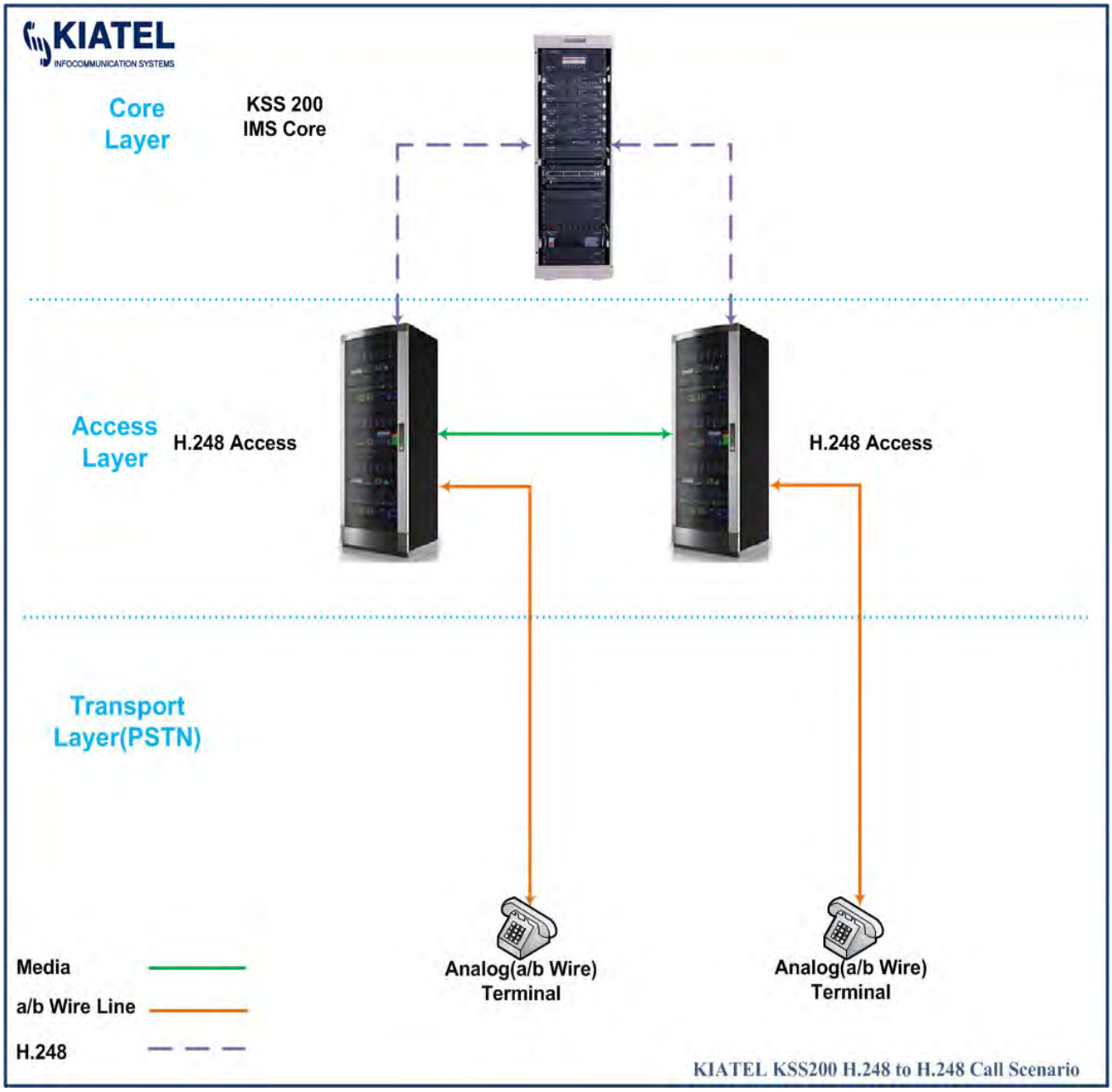


- A SIP subscriber to SIP subscriber type 2 Call Scenario- Both subscribers are belong to same Home.

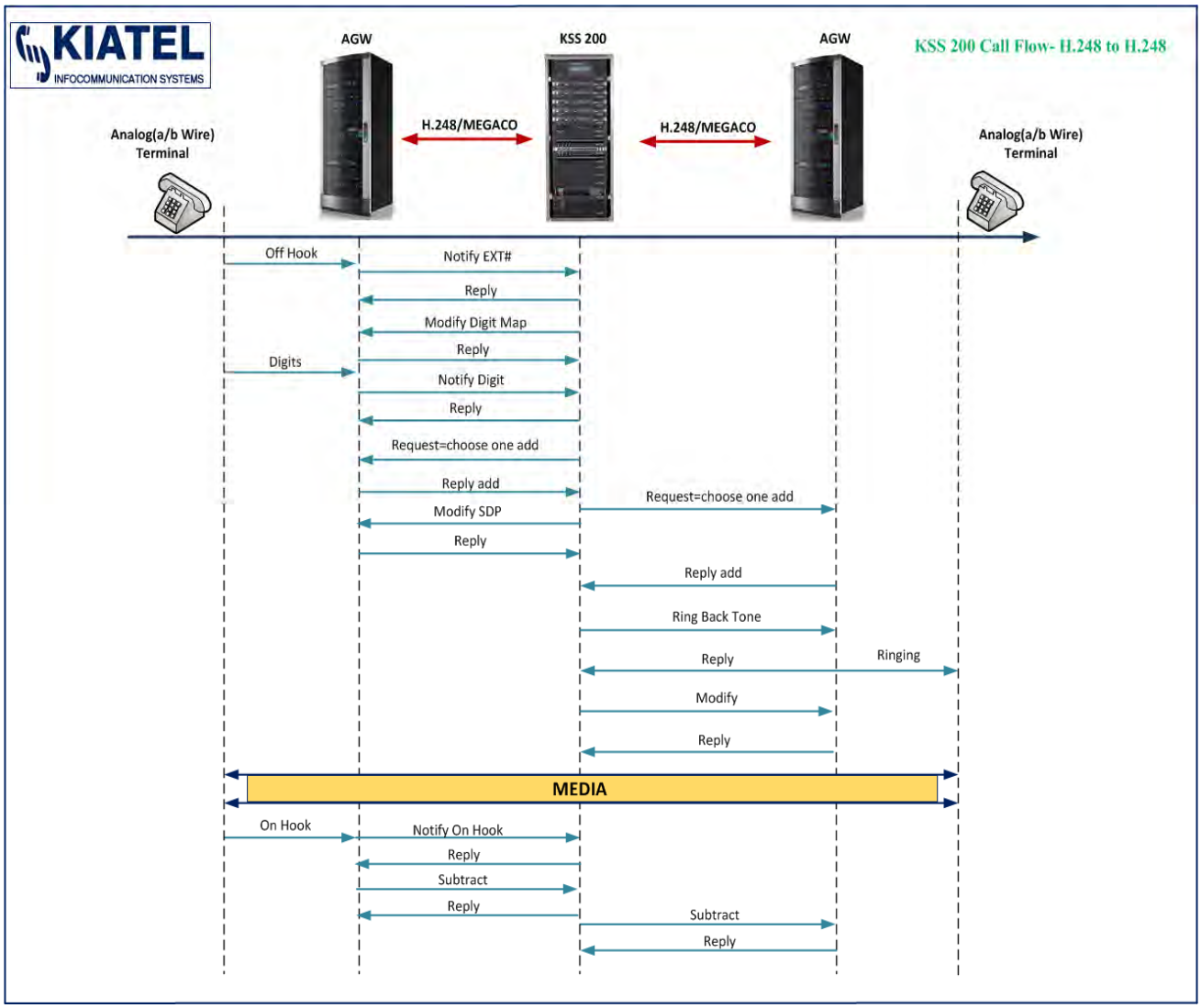


In this scenario, one of the SIP terminals is connected to IMS Core and MGW via network access switch.

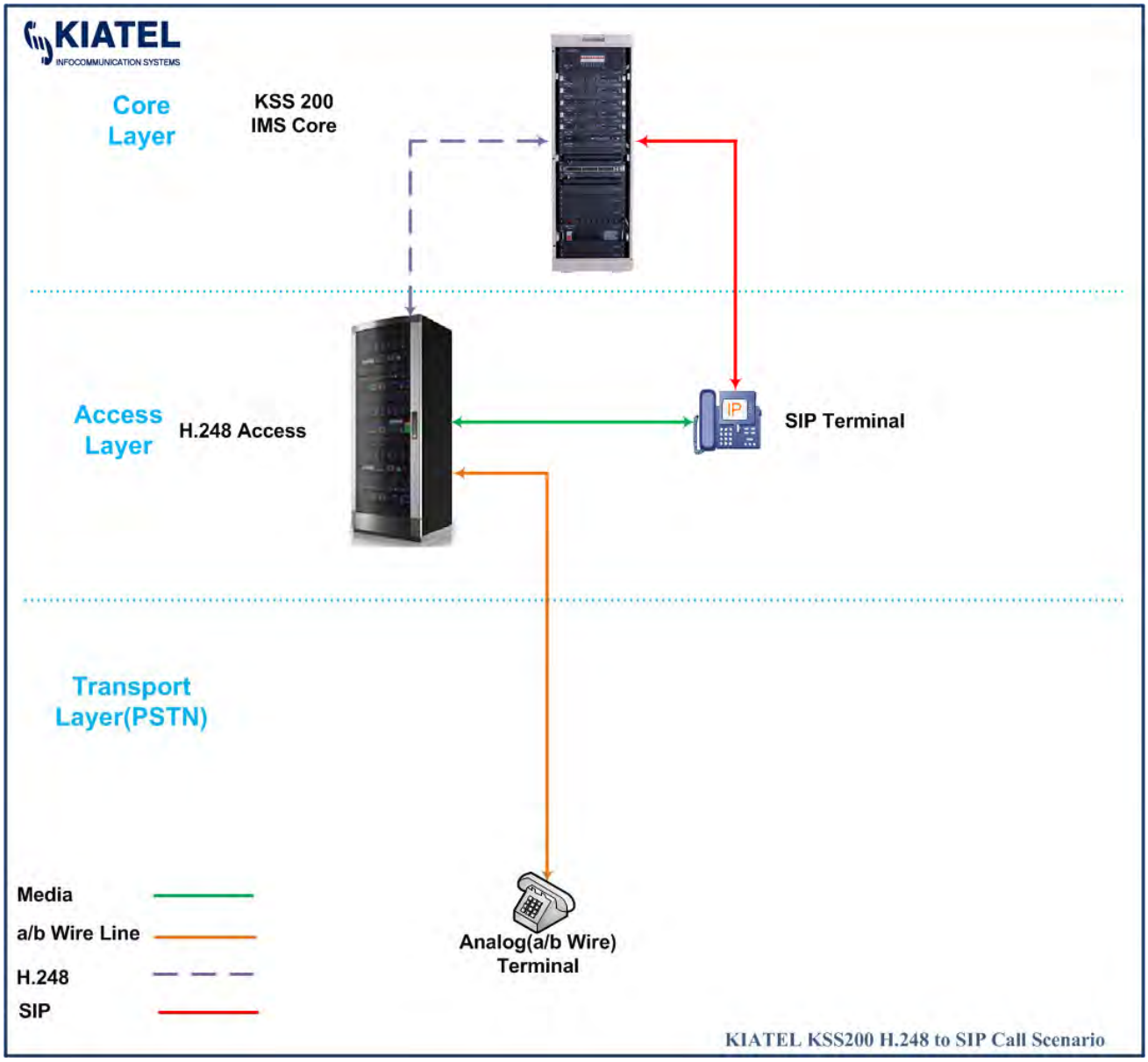
- A PSTN subscriber (via H.248/Megaco Access Gateway) to PSTN subscriber (via H.248/Megaco Access Gateway) Call Scenario- Both subscribers are belong to same Home.



The transaction of signaling messages and media packets is shown in next page diagram.

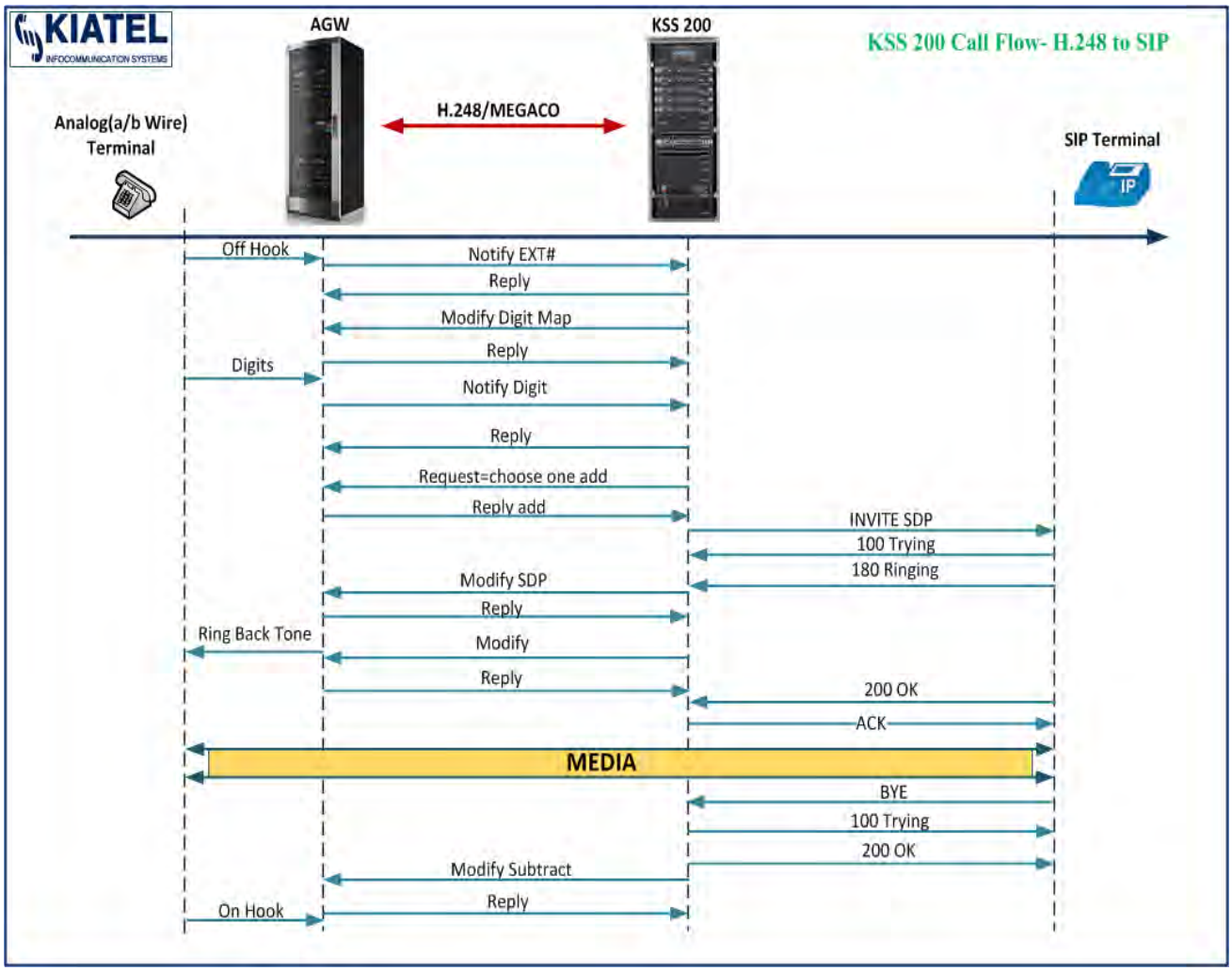

KIATEL
INFOCOMMUNICATION SYSTEMS
KSS 200 Call Flow- H.248 to H.248
AGW
KSS 200
AGW
H.248/MEGACO
H.248/MEGACO
Analog(a/b Wire) Terminal
Analog(a/b Wire) Terminal
Off Hook
Notify EXT#
Reply
Modify Digit Map
Reply
Digits
Notify Digit
Reply
Request=choose one add
Reply add
Request=choose one add
Modify SDP
Reply
Reply add
Ring Back Tone
Reply
Ringing
Modify
Reply
MEDIA
On Hook
Notify On Hook
Reply
Subtract
Reply
Subtract
Reply

- A PSTN subscriber (via H.248/Megaco Access Gateway) to SIP subscriber Call Scenario- Both subscribers are belong to same Home.

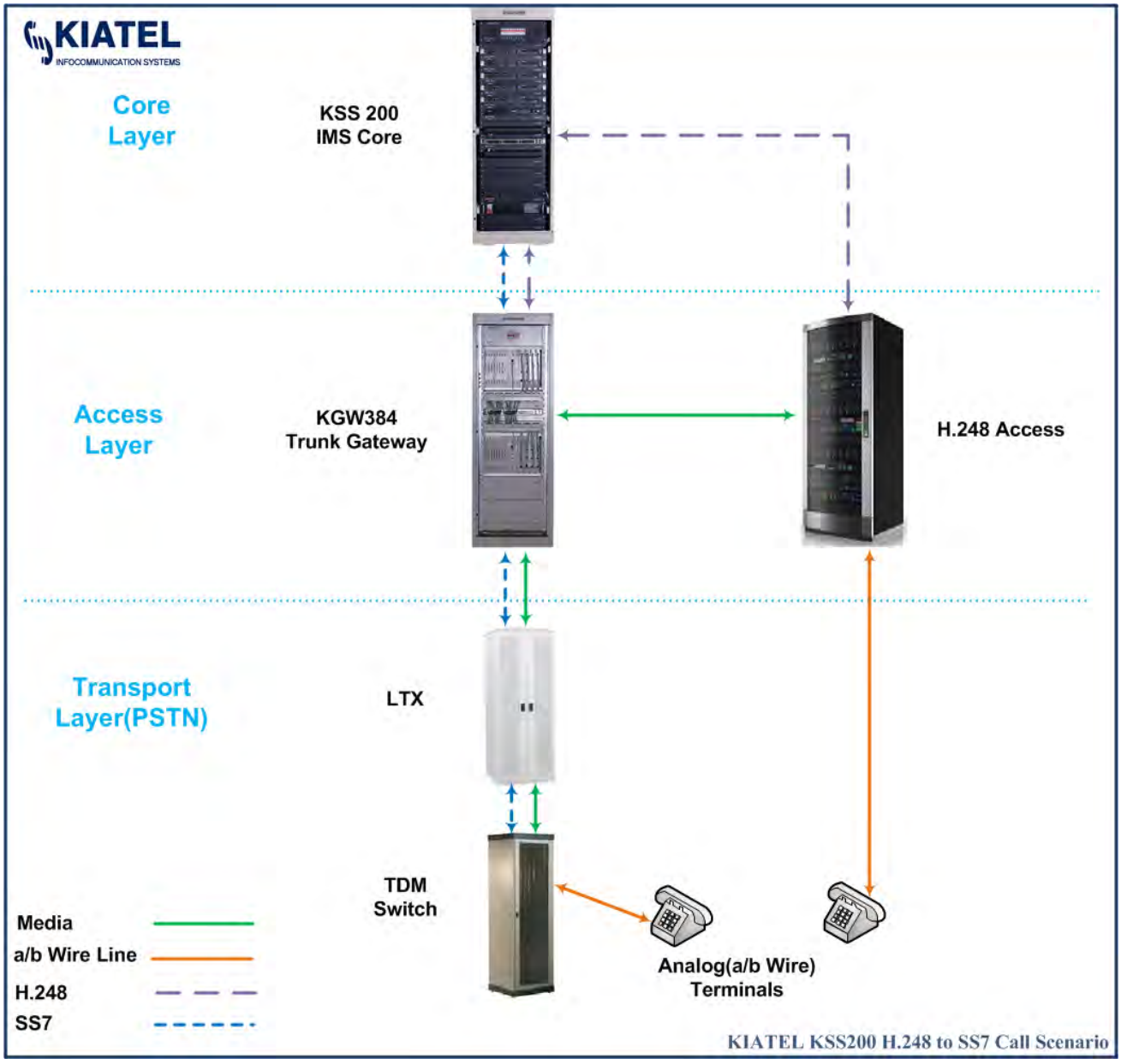


In this scenario, SIP terminal is connected to IMS Core and MGW via network access switch.

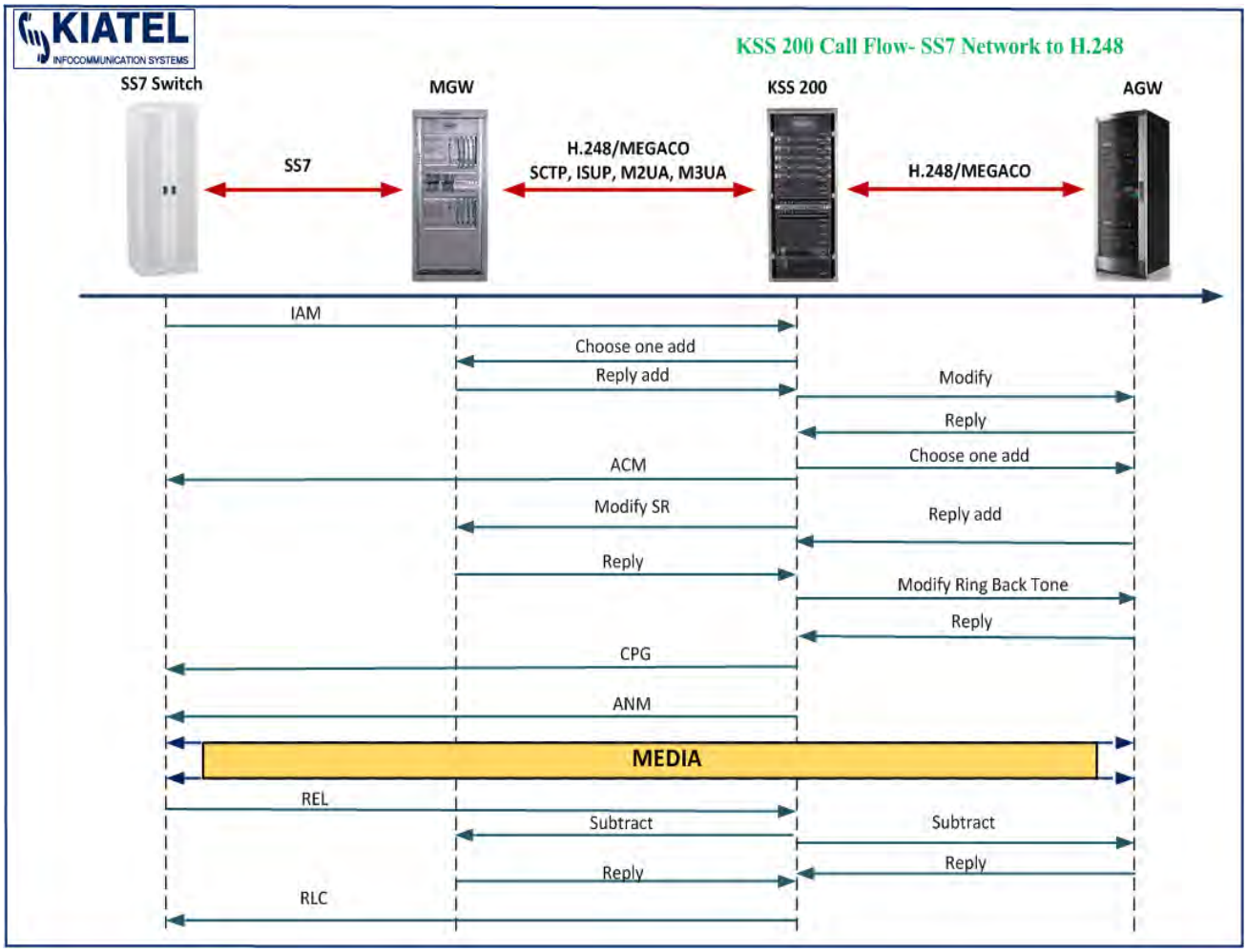
The transaction of signaling messages and media packets is shown in next page diagram.


KIATEL
INFOCOMMUNICATION SYSTEMS
AGW
KSS 200
KSS 200 Call Flow- H.248 to SIP
H.248/MEGACO
Analog(a/b Wire) Terminal
SIP Terminal
IP
Off Hook
Notify EXT#
Reply
Modify Digit Map
Reply
Digits
Notify Digit
Reply
Request=choose one add
Reply add
INVITE SDP
100 Trying
180 Ringing
Modify SDP
Reply
Ring Back Tone
Modify
Reply
200 OK
ACK
MEDIA
BYE
100 Trying
200 OK
Modify Subtract
Reply
On Hook

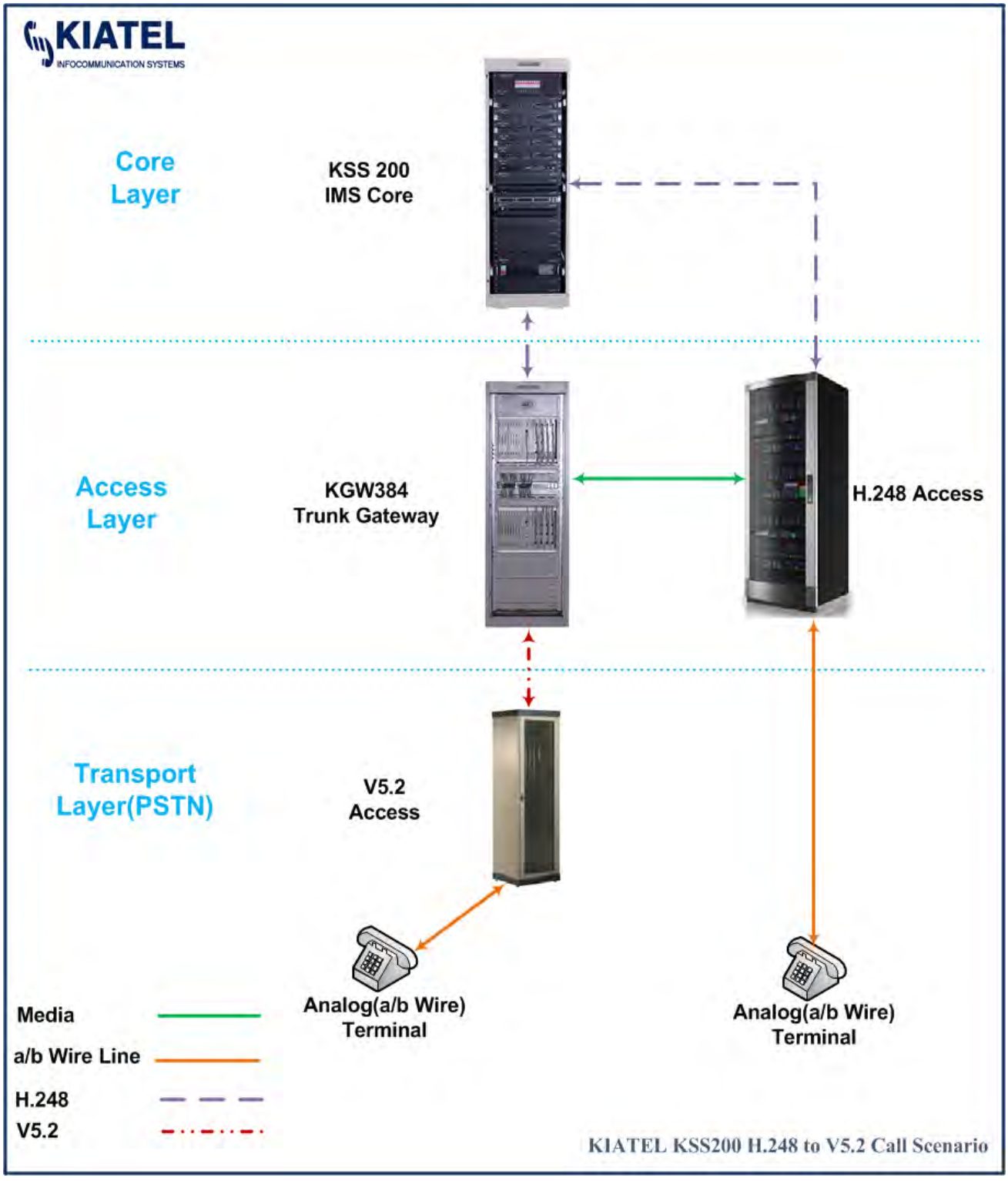
- A PSTN subscriber (via H.248/Megaco Access Gateway) to SS7 switch subscriber Call Scenario- Both subscribers are belong to same Home.



The transaction of signaling messages and media packets is shown in next page diagram.


KIATEL INFOCOMMUNICATION SYSTEMS
KSS 200 Call Flow- SS7 Network to H.248
SS7 Switch
MGW
KSS 200
AGW
SS7
H.248/MEGACO
SCTP, ISUP, M2UA, M3UA
H.248/MEGACO
IAM
Choose one add
Reply add
Modify
Reply
Choose one add
ACM
Modify SR
Reply add
Reply
Modify Ring Back Tone
Reply
CPG
ANM
MEDIA
REL
Subtract
Subtract
Reply
Reply
RLC

- A PSTN subscriber (via H.248/Megaco Access Gateway) to V5.2 access subscriber Call Scenario- Both subscribers are belong to same Home.



II. Fax services

KSS200 supports group-2, group-3 and group-4 fax services. The characteristics are as follows:

1) Access gateway or trunk gateway can report the fax tone.

2) Access gateway with fax machine attached supports the fax services.

3) Codec code switch function is supported. Codec codes can be converted to the T.38 format for the transparent transfer over the packet switched domain, for the purpose of providing users with end-to-end fax communication service of high quality.

III. Supplementary services

KSS200 can provide more than 40 types of supplementary services. Some frequently used supplementary services are described in this table.

No.	Service type	Service description
1	Abbreviated dialing	1 to 2 digits can be used to substitute the actual telephone number which may be a local number, national toll number or international number. For example, if 2 digits are typically adopted to substitute the actual telephone number, so one subscriber has a maximum of 100 abbreviated called numbers.
2	Hotline	This service means if a user does not dial any number in the specified time (for example 5 seconds) after picking up the phone the call will be automatically connected to a particular called party. If a user who has registered the immediate hotline service picks up the phone, the call will immediately reach the registered destination.
3	Outgoing call barring	A user can register to restrict some outgoing authorities (for example, toll calls) of a particular phone set by following a certain dialing procedure.
4	Do-not-disturb service	This service is provided for the user who does not want to be disturbed by incoming calls during some time. When a user applies for this service, all incoming calls will be answered by the exchange, but the originating services of the user will not be affected.
5	Malicious call identification	After applying for this service, a user can find out the originating telephone number by following a certain operation procedure whenever a malicious call is received.
6	Alert service	Once the alerting time set by the user arrives, the user will be alerted by the ringing.
7	Interception service	When a call is made to an absent number or a changed number or a route is blocked temporarily during the call or the user does not operate correctly to make a call, such calls will be automatically intercepted and directed to a pickup device, which avoids virtual connections of the switching equipment.
8	Call forwarding no reply	When a call is made to a certain phone set but it is not answered in the specified time, the call will be automatically forwarded to a pre-designated destination (voice mailbox or auto paging center) based on the forwarding list.
9	Call forwarding unconditional	This service enables a user to transfer incoming calls to another destination. If a user registers this service, when a call comes, the call will be automatically forwarded to a pre-designated destination (voice mailbox or auto paging center) no matter the called subscriber is in any state.
10	Call forwarding busy	If a user registers this service, when a call comes but the called is busy, the call will be automatically forwarded to a pre-designated destination (voice mailbox or auto paging center).
11	Registered call on busy	If a user registers this service, when a call is made but the called is busy, the call will be registered. When the user wants to call this called next time, the call will be automatically put through after the phone is picked up.

12	Absent service	If a user registers this service, when he is absent, the network will answer all his incoming calls by means of playing an announcement.
13	Call back on busy	After a user registers this service, when he dials a number but the called is busy, the served user will be automatically connected once the called becomes free.
14	Call transfer	This service enables the called user to transfer an established call to a third party in a hooking way for the purpose of establishing a new connection between the calling party and the new called party.
15	Call waiting	When user C attempts to establish a connection with user A who is in a conversation with user B, user A will be notified of an incoming call with an indication that there is a user waiting for the connection with him.
16	Three-party service	This service enables a user who is active on a call to hold that call, make an additional call to a third party, switch from one call to the other or join the two calls together into a three-way conversation.
17	Conference calling	This service enables a user to communicate simultaneously with multiple parties. *KSS200* provides two types of conference calling: normal conference calling and auto list conference calling.
18	Designated pickup	This service allows a served user to answer a ringing phone set by dialing the corresponding prefix and the called number to be answered.
19	Secretary service	This service enables a served user to designate another telephone (secretary) to handle all his incoming calls. All incoming calls will be transferred to the secretary telephone and connections can only be established between the secretary and the calling numbers.
20	Secretary station service	This service is an enhanced type of the secretary service. When a telephone set is enabled this service, the incoming calls to the set will be queued. In other words, the incoming calls will be on-hold when the phone is busy and will be answered once the phone becomes idle. The secretary station service can hold a maximum of 5 incoming calls.
21	Calling line identification presentation	This service enables *KSS200* to send the calling party's number to the called party and display the calling number on the called reading device.
22	Calling line identification restriction	This service enables the calling party to restrict presentation of the calling party's number to the called party.
23	Calling line identification restriction override	This service enables a served user to receive the calling party's number unconditionally.
24	Temporary reservation for calling line identification restriction	In normal cases, it is allowed to present the calling party's number to the called party; but by dialing a certain prefix before the called number, the calling party's number will not be presented to the called party in this call. (Class A subscribers)
25	Temporary reservation for calling line identification presentation	In normal cases, it is not allowed to present the calling party's number to the called party; but by dialing a certain prefix before the called number, the calling party's number will be presented to the called party in this call. (Class B subscribers)
26	Quota restricted calling	This service restricts a user's calling expenses. If the served user does not have enough money for the call, the system will prohibit the user to make a new call. It should be noted that the quota restricted calling service is only used for chargeable calls and it has nothing to do with free calls.

27	Restriction alarm	This service enables the system to send an alarm to the OSS-BSS if the remaining chargeable fee of the served user is smaller than a certain threshold. If the served user belongs to a Centrex group, the system will send an alarm to the corresponding console simultaneously. After that, if the user continues the conversation, the system will not send any alarm until a
28	Timed restriction	This service restricts the conversation duration of each call made by a served user. Once the user's conversation expires, the system will forcedly release the call and prohibit the user from continuing the conversation.
29	Call timing restriction	This service restricts the call authorities of Centrex subscribers in one or more time segments. That is, subscribers are allowed to make calls at the corresponding restriction level in the time segments. This service is operated by the operator through the console.

4.1.2 Multimedia Services

I. Point to point multimedia communication

KSS200 supports multimedia communications between SIP-based and H.323-based multimedia terminals and soft terminals. *KSS200* supports multiple audio/video coding formats such as G.711, G.723, G.729a/b, H.261, H.263 and H.264. Depending on the bearer network, the occupied bandwidth can be negotiated between the calling and called parties and then be adjusted dynamically. The point to point multimedia communication services supported by *KSS200* include:

1) Instant messaging: Allows real-time communication by means of text between one terminal user and another who has already logged in.

2) Video communication: A Video Phone user can directly originate a video call to the opposite party and the appropriate video quality can be determined depending on the network bandwidth.

3) File transfer: Transfers files to another user or department where the received files can be saved under a particular directory or a specified directory.

4) Application share: A terminal user shares an application; then the opposite party can use this shared application remotely.

5) Electronic whiteboard: Both parties can write and draw on the same picture, for example, for discussion purposes. This is applicable to many occasions such as remote teaching and technical exchange.

6) Content release: The contents of advertisements and media streams can be released through a multimedia terminal, and a platform can be used to selectively locate the user or to immediately release.

II. Multimedia videoconferencing service

KSS200 has gatekeeper functions and supports the multimedia videoconferencing service under the control of the AS.

1) Supports to hold the conference in reservation convening mode, and users can make reservation through telephone, e-mail or Web.

2) Supports a user to convene and control a conference by means of specific software module which runs on the user terminal and allows the user to manage the conference.

3) Supports data conferences with file transfer, electronic whiteboard and application share functions between terminals by introducing a data conference server.

4) Supports SIP packet terminals and H.323 packet terminals to act as conferencing terminals.

5) Supports both video conference and audio conference.

4.1.3 IP Centrex Services

Based on the IP network, IP Centrex services are a class of NGN value added services which inherits PSTN Centrex services and, based on them, integrates the flexibility of the IP network. Compared with the traditional Centrex services, IP Centrex services are not restricted to voice services. Instead, they integrate multimedia and data services and thus more conveniently provide an optimized and integrated communication solution for group users, such as factories, enterprises, schools, hospitals, government agencies, corporations, hotels and financial organizations.
KSS200 can provide a complete IP Centrex solution to support IP Centrex basic services, IP Centrex supplementary services and IP console services.

I. Major technical characteristics

1) IP Centrex service functions are all provided by specific software module. There's no special requirement for separate user terminals.

2) PSTN telephone terminals are supported as IP Centrex subscribers. MGCP packet terminals, H.248 packet terminals, SIP packet terminals and H.323 packet terminals are also supported as IP Centrex subscribers. Therefore, the networking mode is very flexible.

3) IP Centrex subscribers can enjoy all PBX functions. In addition to all basic services provided for ordinary subscribers, IP Centrex subscribers can enjoy a number of supplementary services.

4) IP Centrex subscribers can be distributed on different media gateways, which help achieve the local network cross-region distribution and the wide area cross-region distribution. The latter is also known as wide area Centrex.

5) The system supports unlimited Centrex groups. The length of the group short numbers ranges from 2 to 8 digits. The number of subscribers in each group only depends on the capacity of the main/backup core servers.

II. IP Centrex basic services

No	Service type	Service description
1	Intra-group calling out	It is possible to make a call between the subscribers in the same Centrex group by dialing the extension number (short number). The PSTN telephone number (long number) of the called party is unnecessarily dialed.
2	Out-group calling out	A Centrex subscriber dials an outgoing prefix, for example 3, and the called party's PSTN number to make a call to anyone outside his Centrex group. The outgoing prefix is determined by the Centrex subscriber.
3	Intra-group calling in	A Centrex subscriber dials the special number of the Centrex group to make a call to another subscriber in the same Centrex group. The length of the special number depends on the size of the Centrex group.
4	Out-group calling in	A subscriber outside a Centrex group dials the PSTN number of the called subscriber who belongs to the Centrex group.
5	Originating call screening	The Centrex group determines calls of which Centrex subscribers are restricted. Out-group calls of certain types can be restricted; out-group calls of all types can be restricted.
6	Emergency call	A Centrex subscriber directly dials the emergency number to make an emergency call without dialing the outgoing prefix, for example, to make a fire emergency call.
7	Distinctive ringing	*KSS200* supports distinctive ringing for intra-group and out-group incoming calls. For example, the short ringing tone is played for intra-group incoming calls and the normal/special ringing tone is played for out-group incoming calls.
8	Call pickup	1.Co-group pickup: A Centrex group is divided into several subscriber sub-groups. If a call is made to an extension in a sub-group but no reply is received, the call can be answered by other subscribers in the same sub-group. 2.Designated pickup: If a call is made to an extension but no reply is received, the call can be answered by other extensions in the same Centrex group.

III. IP Centrex supplementary services

IP Centrex subscribers can not only enjoy all basic services and supplementary services provided for ordinary subscribers, but also can enjoy a number of new services specialized for them. Such specialized services include designated pickup, co-group pickup, remotely set call forwarding unconditional, remotely set call forwarding busy and remotely set call forwarding no reply.

IV. IP console services

KSS200 supports IP console services. With such console and under control of *KSS200*, user achieves voice, data and other service functions through the pure packet switched IP network.

IP console services have the following technical characteristics:

1) IP access feature, which allows the console to access *KSS200* across the IP network so that the console operator can be located far away from *KSS200*.

2) Call control functions such as call transfer, call assistance, incoming call queue and call hold and resume, re-dialing.

3) Call emergency override/transfer functions.

4) Transferring calls to a standby number in the event of console failure.

5) Calling by called party's name and calling name identification presentation functions.

6) Wakeup scheduling.

7) Do-not-disturb service.

8) Night service function.

9) Distinctive presentation for intra-group and out-group incoming calls.

10) Call forwarding to console on busy, no reply or do-not-disturb.

11) Console queue announcement.

4.1.4 IN Services

Fully compliant with the ITU-T Recommendations Q.122x and Q.123x series and the ITU-T Recommendation Q.1218, *KSS200* supports SSF, so *KSS200* can act as an SSP in the IN. With the cooperation of the SCP entity, *KSS200* can provide users with abundant IN services.

I. Free PHone (FPH)

This service enables calls to the service subscriber to be paid by the called party. For example, if a commercial organization or a person applies for this service, the service subscriber will be charged for all the calls to the served user. As such outgoing calls are free for the calling party; they are usually called "Free phones".

II. Account Card Calling (ACC)

This service enables a user to make a call from any card reading telephone and have the charges for the call automatically debited to an account number as defined by the card content. The service subscriber must be provided with a unique card number. When using this service, the subscriber should input the access code, card number and Personal Identification Number (PIN). After the network authenticates the card number and PIN input and returns the confirmative indication, the card user can make normal phone calls.

III. Virtual Private Network (VPN)

This service provides a logically private network for organizations and enterprises to make their services public by using the resources of the public telephone network. VPN supports special numbering of the service subscriber and has flexible charging modes. The VPN special account number is charged for all outgoing calls except those made by means of personal account number by a VPN member.

IV. Universal Personal Telecommunication (UPT)

This service enables the service subscriber to access any network and originate and receive any type of calls across multiple networks by using a unique Personal Telecommunication Number (PTN), which is associated to mobility service. Depending on the requirements of the service subscriber, the UPT number can be translated into the corresponding communication number and routed for transferring the incoming calls to the proper place which is designated by the service subscriber.

V. Mass Calling (MAS)

This service is similar to the hotline service. It mainly features in the capability to prevent network congestion in the case of instant high traffic. For example, this service is probably used when it is advertised that anyone making a call to a particular telephone number during a specific time segment has a chance to be rewarded.

VI. Tele voting (VOT)

This service is provided for consultation or opinion survey. The enterprises, government branches, or commercial organizations requiring opinion survey can apply for one or multiple tele voting numbers for investigating mass opinions by means of the telephone network. Accordingly, people can dial the several specific tele voting numbers to register their votes or dial one tele voting number to express their opinions by following the recorded announcement to press phone set keys.

The network will perform statistics on the number of the calls to a specific tele voting number as well as people's opinion information.

The service subscribers can query the statistical information by means of a terminal or a DTMF phone set at any time.

There are three types of VOT:

• Simple VOT: Only tele voting is provided. Other activities such as reward are not provided.

• Single VOT: Simple VOT and reward are provided.

• Multiple VOT: There are item codes, not opinion codes. A VOT number represents an item. People need to follow the system provided voice prompt to express their opinions. A service subscriber may apply for this service with or without reward.

VII. Wide Area Centrex (WAC)

This service enables a Centrex group distributed over different exchanges to operate on the same virtual private network. Calls between the WAC users under the same Centrex exchange are completed in the exchange itself. Calls of independent users or across different Centrex exchanges are completed with the help of SSP and SCP.

VIII. Number Portability (NP)

This service enables a subscriber to retain the original number after the subscriber's geographical location, serving carrier or enjoyed services are modified. All incoming calls to the NP subscriber's old number will receive a voice prompt indicating the original number has been changed, before the calls are automatically transferred to the new number. For outgoing calls, the calling number is the same.

A user demanding for this service can apply for it and specify the service life. During the specified service life, the subscriber's original number will be preserved, not allocated to others, until the subscribed service expires.

IX. IP800

This service enables all calls to the service subscriber, on the IP network, to be paid by the called

party. The 800 service subscriber who applies for the service specifies the real destination number corresponding to the 800 number. The destination may be a PSTN telephone number, an IP terminal number, an IP address or the user's ID. The 800 service users who enjoy the service are the variety of users on the IP network. They can click the 800 number in a Web page or dial the 800 number to make a phone call.

4.1.5 IPN Services

A variety of IMS terminals are provided with uniform Internet personal numbers. Examples of supported terminals are Ephone subscribers directly connected to *KSS200*, Ephone subscribers connected through IAD or access gateway and PSTN subscribers or mobile subscribers connected through RGW.

An IPN user may own several terminals. However, through a uniform IPN number, the user can originate calls at any place by using any of the terminals through the same account (that is, the same IPN number). Meanwhile, others can make calls to that IPN number to find the user. According to the IPN rules, the calls are routed to the corresponding destination to achieve billing functions.

KSS200 supports IPN calling service, IPN called service, IPN dynamic rule, IPN static rule, as well as an optimized IPN charging ability.

I. IPN calling service

The IPN calling service enables a service subscriber to originate calls by using the IPN number. In this case, the IPN calling service is similar to the pre-paid card service provided by the IN. The IPN number is charged for the calls. It is unnecessary to register the IPN calling service. Once this service is enabled, the subscriber can enjoy it by using the allocated IPN number through various terminals. When a call is originated from an Ephone, or a PSTN phone set or an ordinary soft terminal, this service adopts the dual stage dialing IVR procedure to implement the call.

When a call is originated from KIAPhone (a soft terminal developed by KIATEL), this service also supports the single stage dialing procedure to implement the call.

II. IPN called service

The IPN called service enables calling parties to originate calls to the service subscriber by dialing the subscriber's IPN number. In this case, *KSS200* will route the calls to the called party (that is, the service subscriber) depending on the communication mode and the communication policy (such as a PSTN number, a mobile terminal number, a voice mailbox) pre-determined by the subscriber, so that the subscriber can receive the calls in any place at any time. The purpose is to achieve a flexible billing function.

III. IPN dynamic rule

The IPN dynamic rule enables a service subscriber to register or cancel the IPN called service by using a phone set. For example, the subscriber dials 166 on a PSTN phone set. According to the prompting announcements, the subscriber inputs the IPN number, the IPN password, and then inputs 6 during the function selection. Subsequently, the subscriber can register the called destination number of the IPN. The called destination number may be the number of the phone set on which the registry is performed; the called destination number may also be a different telephone number. Once

the dynamic rule is confirmed, all the calls to the service subscriber will be routed to this called destination number. It should be noted that the IPN dynamic rule is prior to the IPN static rule. If no data is set in the IPN dynamic rule, the IPN static rule will take effect. If data is set in the IPN dynamic rule, the system will not use the IPN static rule even though the calls fail to be connected.

IV. IPN static rule

The IPN static rule enables a service subscriber to perform management operations by means of Web self-service. *KSS200* supports to select a policy based on sequence or based on time. The service subscriber can set different static policies, but only one of them takes effect at any time.

1) Sequence-based policy: The system supports a maximum of five destination numbers. If the calls fail to connect the first destination number or no reply is received from the first destination number, the calls will be routed to the second destination number. Such a selection will go on in this way until a reply is received or all the destination numbers cannot be connected successfully.

2) Time-based policy: The system supports five time segments per day to select a policy. During each time segment, this service enables the service subscriber to bind the IPN number with a different destination number.

V. IPN charging

There are two types of IPN charging, namely pre-payment and post-payment. The pre-payment type allows the service subscriber to transfer money to the IPN number in advance which will be charged for all the calls in the real-time way. The post-payment type is similar to the charging mode of an ordinary PSTN phone set, such as charging every month. The service subscriber must regularly pay the carrier the communication fee consumed in a specific period (for example, a month) by means of cash or through bank.

4.1.6 UC Services

Unified Communication (UC) services refer to the various value added services provided by *KSS200*. The UC system of is a part of KIATEL NGN/IMS platform to provide a variety of solutions and services for users.

I. Click To Dial (CTD)

This service enables a subscriber to be in a VoIP communication through the packet based network with another pre-determined subscriber by clicking a link on a Web page. These two subscribers can be IP telephone terminals which are identified by IP telephone terminal number, personal computers which are used by the users to view Web pages, or ordinary PSTN phone sets which are connected to the packet network through packet gateways.

II. Click To Fax (CTF)

This service enables a subscriber to transfer determined fax information to the called subscriber through the VoIP network by clicking a link on a Web page. *KSS200* supports both the INAP extensions and the T.38, and can transfer fax information to a fax machine.

III. Unified Messaging (UM)

This service enables a subscriber to receive e-mail messages, voice mailbox messages, voice messages, video pictures, short messages and fax information, as well as viewing motion pictures.

IV. Instant Messaging (IM)

This service enables several subscribers to exchange content information in real time. Usually the content information is in the text format and does not need to store. The IM service is different from the e-mail messaging system. In the IM service the characteristic of real-time transfer of text messages is provided. The communication between IM subscribers are still based on text messages.

Combining instant messaging with mobile messaging, Internet messaging and fixed messaging, mobile subscribers, Internet subscribers and fixed terminal subscribers can have a chat in a multimedia manner.

V. Phone To IM

This service enables IM subscribers to communicate in the voice manner. With the proper IM number, telephone subscribers including PSTN telephone terminals, SIP packet terminals and H.323 packet terminals can be in a voice communication with IM subscribers.
After a telephone subscriber dials the IM access code, a voice prompt is played to the telephone subscriber and the dialed IM number is collected. The IM service makes a judgment on the current state of the IM subscriber, for example, whether the IM subscriber is on the Internet and whether the IM subscriber can receive voice communication. And then a voice channel is established between the telephone subscriber and the IM subscriber. Subsequently, the IM subscriber can communicate in a voice manner with the telephone subscriber, for example, by using an earpiece and a microphone connected to the computer; the IM subscriber can also communicate in the text way with other IM subscribers.

VI. Web self-service

This service integrates the next generation voice network and Internet technology. In Web pages, a subscriber can query the charge, bill, subscriber properties information conveniently, and customize supplementary services and online payment. Instead of the complicated operations of PSTN, this service enables the subscriber to customize personal services easily by means of Web GUI. In addition to the convenience for the subscriber, Web self-service, as a special service featuring the advantages of IMS has advanced the applications of various services, thus increasing the service profit of the carrier.

VII. Presence

This service enables a subscriber to modify or publicize the current communication status of the subscriber himself and even the feeling and the mood of the subscriber himself. Besides, this service enables other users to subscribe to the current status of the presence service subscriber. Whenever the communication status of the presence service subscriber changes the presence service notifies the corresponding users of the change.

For example, user A subscribes to the telephone status of user B by the presence service. Once user B's telephone status moves from the conversation status to the available status (for example, the user

hooks on), the presence service notifies user A of the change by means of e-mail, Short Message Service (SMS) or IM. And then user A can select the most appropriate communication way to contact user B.

The presence service can also be combined with other services and provide the subscriber's status information for those services. For example, the presence service is combined with the multimedia conferencing service. The multimedia conferencing service can display the attendance status of the conference members by using the status information provided by the presence service.

VIII. Personal Communication Assistant (PCA)

This service provides a number of functions to realize the management of personal information. For example, a subscriber can put all personal information in the network including the address book, schedule, e-mail address, voice mailbox, fax mailbox, preferred news and preferred stocks. The subscriber operates such information through Web pages or by means of voice interfaces to build a personal communication assistant.

IX. Integrated communication VPN service

The integrated communication VPN service not only inherits all the features of the VPN service based on the traditional PSTN, but also has new service features brought by the integration of the networks. These service features may be the enhancement of the original features, such as the communication between a PSTN telephone and a mobile telephone in the network. They may also be new service features, such as the multimedia communication capability. As *KSS200* NGN/IMS platform is an integrated and open network architecture, a variety of user terminals can be used in the integrated communication VPN service, such as PSTN telephones, mobile phones, SIP phones, pagers, personal computers, fax machines and even personal digital assistants. The integrated communication VPN service subscriber is no longer restricted to voice calls. The service subscriber can also enjoy digital and video communications.

4.2 *KSS200* Functions

KSS200 supports multiple functions or features, satisfying the requirements of various networking or applications.

4.2.1 Support for Multi-Country-Code and Multi-Area-Code Functions

As *KSS200* has been designed to be the main part of NGN/IMS core, it is able to work in a network across several regions and countries. This is a good way to reduce the investment of the network construction and improve the marketing competitive power of the operators.

KSS200 simultaneously supports multi-country-code and multi-area-code functions to fully satisfy the across-region and across-country networking requirements of the carrier:

1) Simultaneously supports unlimited country codes, ensuring the correctness of calling number transmission and number analysis.

2) Simultaneously supports unlimited area codes, ensuring the correctness of calling number transmission and number analysis.

3) The nature of service of the calls between multiple area codes is national toll calls, which can be flexibly charged.

4) The numbers of the users using different area codes can be the same that is numbers can be repeatedly used.

4.2.2 Support for Multi-Signaling-Point-Code Function

KSS200 can control gateways to support many local signaling point codes. This break through the limit of regular SS7 trunk circuits supported by a single office direction at most and extends the number of SS7 trunk circuits supported by a single office direction. This fully satisfies the requirements of a gateway control for a large capacity of trunks.

4.2.3 Support for Dual-Homing Function

As IMs is an open and distributed network, media gateways can access the *KSS200* at any location through the IP packet network. However, because of the complexity issues of the network and variety of natural disasters, gateways may lose the control of the *KSS200* in the event of an interruption of the network, an earthquake where the equipment room is resident, or a fault of the system and therefore gateways cannot provide services for users.

This will directly influence the service quality of the operator and then the users will complain about this.

To solve this problem, *KSS200* provides a dual-homing solution. That is, a gateway device can simultaneously home at two independent *KSS200s*, one of which acts as an active Gateway Controller and the other as a backup controller. A real-time backup mechanism between the *KSS200s* guarantees the data consistency of the controlled gateways. Whenever the active *KSS200* becomes faulty, the backup one immediately receives the control of the gateways against interruption of the services, so that the reliability of the system can be improved and the disaster-proof ability of the network can also be enhanced.

4.2.4 Support for Gateway Functions

KSS200 supports a number of gateway functions such as black and white lists, call authentication and call interception. Depending on the calling subscriber's number or incoming trunk's identifier, *KSS200* can bar or allow incoming calls from certain calling subscribers or incoming trunks to certain destination numbers, including intra-network calls, national toll calls, international toll calls, and other voice services and multimedia services.

KSS200 has the following technical characteristics:

1) Comprehensive authentication and interception capabilities

KSS200 can conduct flexible authentication based on the calling number or calling number prefix, calling subscriber's category, outgoing/incoming trunk group identifier, nature of call service, destination number (called number or called number prefix), and calling time. *KSS200* provides authentication capability associated with black and white lists. The capacity of the black and white lists is unlimited.

2) Precise and flexible charging capabilities

KSS200 provides many charging modes including meter and detailed bill and allows 100% calls to have a bill. The duration precision in the bill is 1 second. Bill statistics function is supported based on the tariff, date and time, destination number, trunk group and area code, for routine maintenance and settlement purposes.

3) Strong and secure bill storage and transmission capabilities

KSS200 adopts a three-level bill storage mechanism (OSS-BSS servers in home#1 and home#2, hot billing center), so that bills can be stored and transmitted securely, rapidly and reliably.

4.2.5 Support for IP Supermarket Function

IP supermarket refers to IP toll call services deployed by the operator at telephone business outlets, for example, telecommunication business halls. The IP supermarket function of *KSS200* is provided in the IP Centrex manner. IP console is used to charge all calls made at the IP supermarket business hall. The technical characteristics are as follows:

1) High connection speed.

2) Precise charge.

3) Centralized management. One console is able manage tens of phone sets.

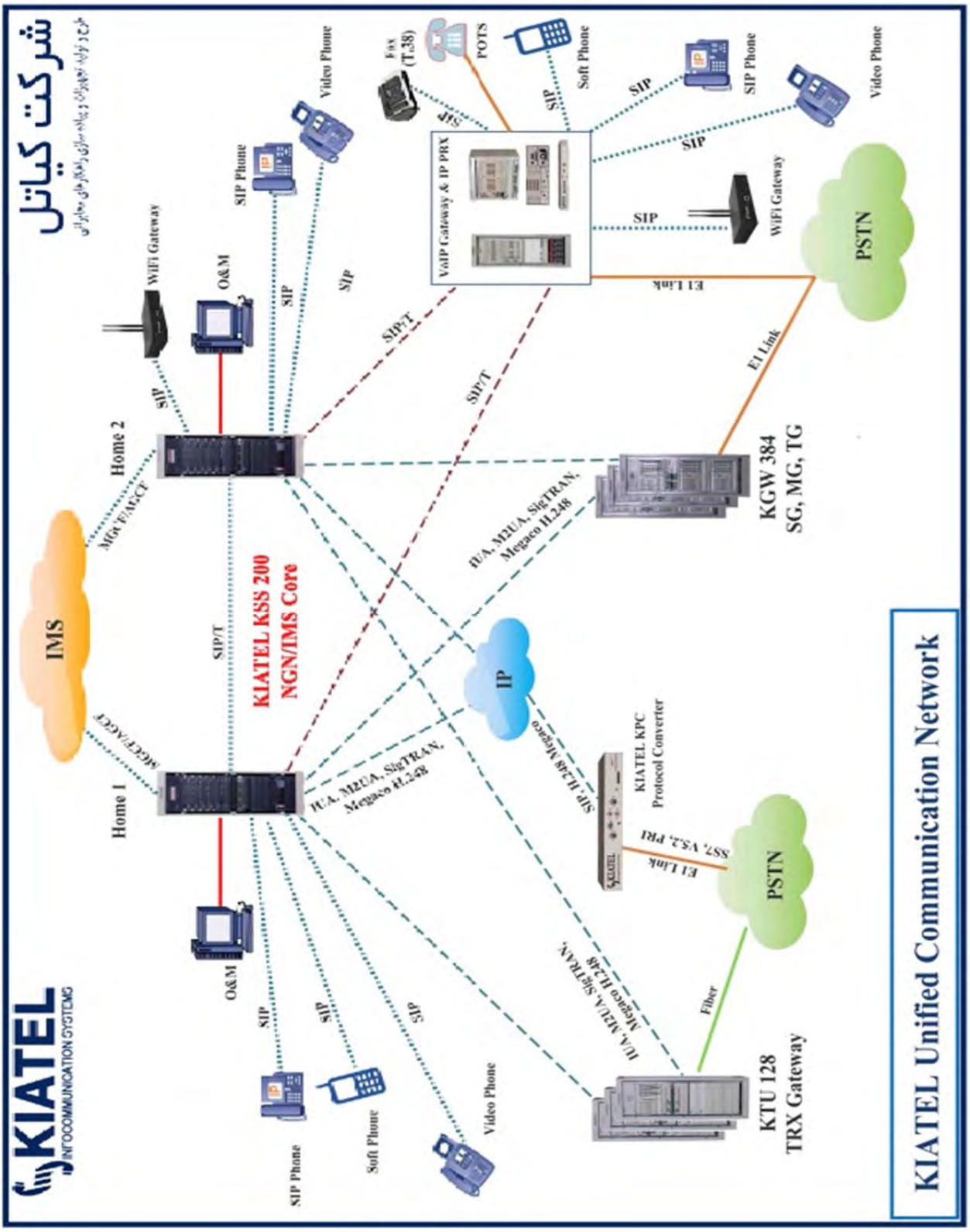
4) Simple and convenient operations. Telephone authorities can be enabled and disabled only by using the mouse of the computer. Whenever a telephone hooks on, a bill is printed immediately. In addition, deposit management and change returning function are completed.

5) Level and authority management functions, that is, authority management for logging on to the console.

Chapter 5 Networking and Applications

5.1 System Networking

KIATEL has developed a total and unified solution for network implementation named KUCN (KIATEL Unified Communication Network). Figure shows this solution.



5.1.1 Multimedia network support

KSS200 supports multiple media gateway control protocols and multimedia communication protocols such as MGCP, H.248, SIP and H.323.

Network topologies are as below:
1) Centralized subscriber access: This scenario is designed for the access of a high density of subscribers where a KIATEL KGW384 gateway is used for the access realization. The KGW384 is connected to *KSS200* in the MGCP/H.248 protocol to achieve voice call and value added services.

2) Distributed subscriber access: This scenario is designed for the access of a small capacity of voice and data subscribers who are relatively centralized. An IAD is used and connected to *KSS200* in the MGCP/H.248 protocol to achieve voice call and value added services. Meanwhile, an IAD with data access functions can be used as a LAN Switch for the access of data subscribers in the Ethernet manner.

3) Individual subscriber access: This scenario is designed for the access of SIP Phones, H.323 Phones, MGCP packet terminals and H.248 packet terminals to *KSS200* to achieve voice and multimedia services. Meanwhile, intelligent terminals can also implement a variety of individualized services and subscriber management.

5.1.2 Tandem Office network support

KSS200 supports a number of routing functions such as the plane static routing, the layered static routing and the dynamic routing. *KSS200* can control a tandem office through gateway.

KSS200 satisfies two networking applications under the layered routing structure:

1) Layered IMS structure mode

In this mode, *KSS200* adopts the plane static routing and transits the incoming calls from the end offices by means of SIP or H.248 trunk.

2) Layered HSS mode

In this mode, *KSS200* adopts the layered static routing or the dynamic routing, equivalent to a HSS. The end offices implement the routing function by sending an address resolution request to *KSS200*.

5.1.3 C5 Office (End Office) control

KSS200 supports a number of signaling transport adaptation protocols including M2UA, V5UA and IUA and supports a number of PSTN signaling including MTP, ISUP, R2, V5.2 and DSS1. When cooperating with KIATEL KGW384, *KSS200* can control a C5 office (end office) in the traditional PSTN.

I. Interworking with RSU (Remote Switch Unit)

As part of the feature applications of KSS200, the RSU accesses the system through gateway and with the internal protocol interface (called E1 interface physically). *KSS200* controls the services in the H.248 protocol. A large-scale application can thus be achieved and it represents a good solution to re-build the existent PSTN exchange network.

II. Interworking with V5 access device

KSS200 can provide standard V5.2 interfaces with the cooperation of KGW384, achieving the interworking with access network devices.

III. Interworking with PBX and NAS

KSS200 can provide standard PRIs or R2 trunks with the cooperation of KGW384, achieving the interworking with PBX and NAS.

5.1.4 C4 Office (Tandem Office)

KSS200 supports M2UA, M3UA, MTP and ISUP. By means of KGW384, *KSS200* can control the C4 office (tandem office) in the traditional PSTN network.
There are three networking scenarios for *KSS200* to interwork with a C5 exchange.

1) In case of M2UA, *KSS200* can interwork with a C5 exchange through KGW384 as this gateway has built-in signaling control functions.

2) In case of M3UA, *KSS200* interworks with a C5 exchange through KGW384. This gateway implements the media stream conversion functions.

3) In case of MTP, *KSS200* interworks with a C5 exchange through KGW384 and SS7 signaling network. KGW384 only implements the media stream conversion functions. *KSS200* achieves the signaling point functions, that is, providing MTP links.

5.1.5 Interworking with H.323 Network

KSS200 interworks with the existent H.323 network in the H.323 protocol, equivalent to a gatekeeper.
When the local network and the H.323 network are owned by different operators, the interworking point is resident between the *KSS200* and the top-level gatekeeper of the opposite IMS domain. When the local network and the H.323 network are owned by the same operator, the interworking point is determined by the operator depending on the actual conditions of the network construction.

5.1.6 Interworking with IN

KSS200 supports SCCP, TCAP, INAP, and provides SSF, CCF, SRF and CCAF. *KSS200* can act as an SSP in the IN.

In the actual networking applications, the operator can adopt any of the following modes for interworking with SCP:

1) Both *KSS200* and SCP provide MTP links to the SS7 signaling network. The INAP protocol of both parties is borne over TCAP/SCCP/MTP.

2) Both *KSS200* and SCP provide M3UA links to the IP core network. The INAP protocol of both parties is borne over TCAP/SCCP/M3UA/SCTP/IP.

3) *KSS200* provides M3UA links to KGW384; SCP provides MTP links to the SS7 signaling network. KGW384 is responsible for the conversion of the protocols. At the *KSS200* side, the INAP

protocol is borne over TCAP/SCCP/M3UA/SCTP/IP; at the SCP side, the INAP protocol is borne over TCAP/SCCP/MTP.

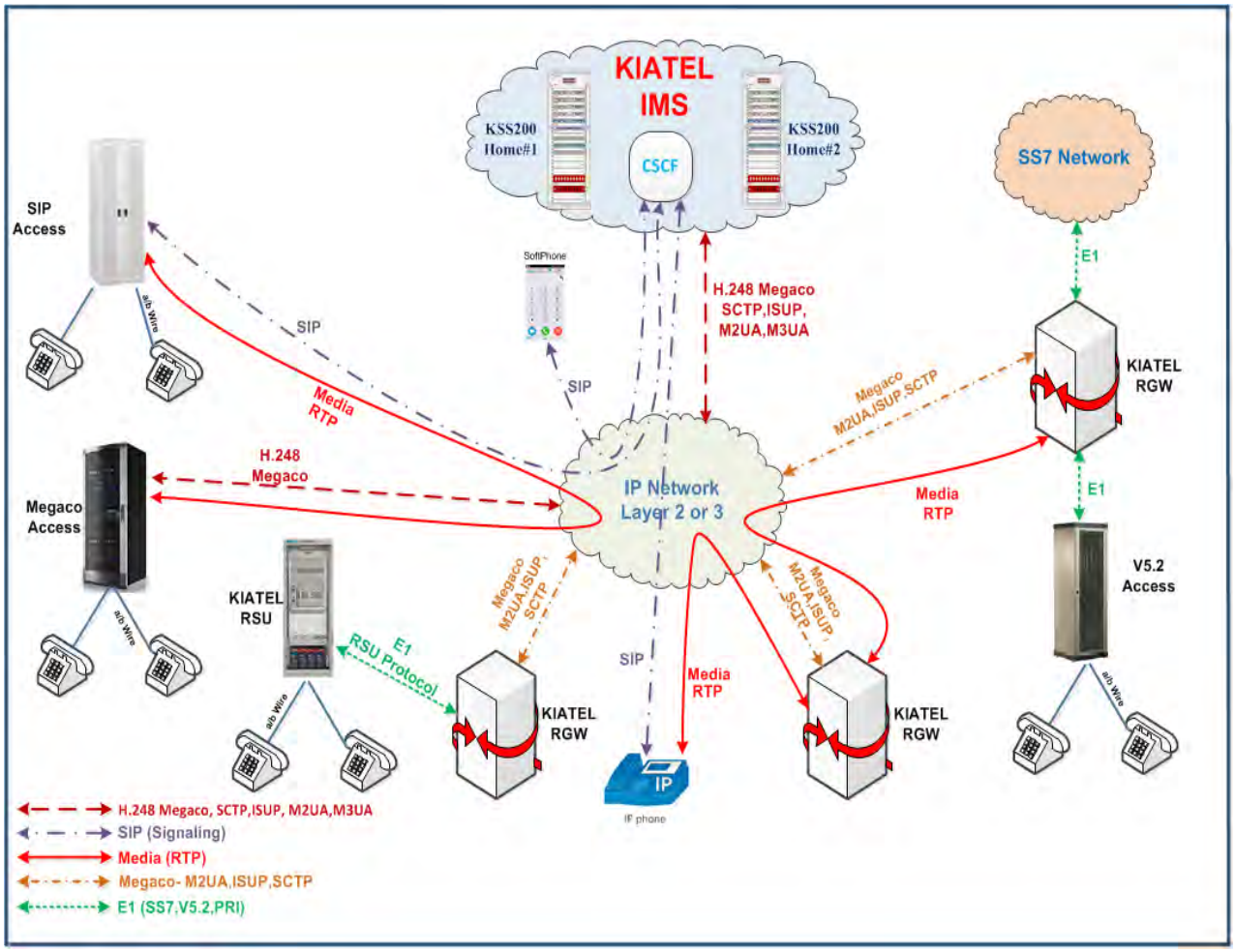
5.1.7 Interworking with SIP Network

KSS200 supports the SIP protocol and can interwork with any SIP application server in the SIP network.

The SIP network application solution furthest reflects the bearer advantages of the services of IMS. *KSS200* provides call control functions and the SIP network services. It enables users to enjoy SIP-based voice services and other services with voice and Internet integrated.

5.1.8 *KSS200* base Implemented Network

Figure shows *KSS200* abilities for supporting various protocols in telecom network.



Chapter 6 Reliability and Security Design

6.1 System Reliability Design

6.1.1 Hardware Reliability

KSS200 is structured in a multi-server configuration and many factors are taken into account to guarantee the reliability of the system hardware. The servers are selected from well-known manufacturers and configured in the main/backup mode with redundant configuration. What are used in *KSS200* are qualified components which are carefully selected and have passed the worst case tests.

I. Synchronize processing

In *KSS200*the synchronize processing is achieved by means of special software module named KRSF (KIATEL Redundancy Synchronization Function) and KDSF (KIATEL Dual Homing Synchronization Function). The functions of the servers are synchronized and controlled by above mentioned modules. The fault of one server does not influence the normal running and operation of the whole system.

II. Dual-Server Dual-processor redundancy technique

KSS200 uses main/backup servers with dual-processor redundancy technique. The MCS, BCS, MDBS, BDBS and BOBS servers are equipped with dual CPU configuration. In the normal conditions both CPUs are engaged in processing and share tasks. If one CPU becomes faulty, other one handles all processing tasks without any interruption. Also the main servers control the running of the modules and the backup servers keep synchronized with the main one in real time. Whenever the main server becomes faulty, the backup one is brought into service immediately. The backup replaces the main to control the running and operation of the modules against service interruption of the system.

6.1.2 Software Reliability

KSS200 software is designed in a hierarchical modularized architecture with protective performance, error tolerance capability and fault monitoring function.

I. Protective performance

Based on near 30 years of KIATEL experiences in telecom systems software development, from requirement analysis, system design to software test, all stages of the development of *KSS200* software follow the Capability Maturity Model (CMM) procedures. Code walk-through, inspection, review, unit test, system test and other useful quality assurance measures taken in *KSS200* software development improve the reliability of the system greatly.

II. Error tolerance capability

By means of timing detection for key software resources, real-time task monitoring, storage protection and data check, *KSS200* effectively prevents minor software faults from imposing a great effect on the whole system, which greatly improves the error tolerance capability of the system.

III. Fault detection and handling

KSS200 is able to automatically detect and diagnose both software and hardware faults. The faulty components can be automatically switched, restarted and reloaded to avoid service interruption.

6.1.3 System Overload Control

KSS200 will never face with overload because system hardware resources and software procedures have been fixed for 2,000,000 registered users and 200,000 concurrent calls.

6.1.4 Reliability of charging

I. Hardware reliability

In *KSS200* the OSS-BSS Server is employed as the charging processor and recorder. This server has Dual-processor redundancy and Hot RAID5 hard disk array, which realizes the dual backup and mass storage of the bill data.

II. Software reliability

1) Program reliability

The OSS-BSS Server is capable of transferring detailed alarm information to the central management office in real-time mode for centralized alarming purposes, thus facilitating the removal of the faults of the OSS-BSS Server in time.

2) Reliability of bill data

I. Against bill loss or bill repetition

After saving the original bill data, the OSS-BSS Server sends a confirmation message to the core. At the same time, the current bill confirmation state is recorded in detail against bill loss or bill repetition. The OSS-BSS Server is restored after each start to ensure the consistency between the original bill data and the final bill data.

II. Data backup

The OSS-BSS Server is responsible for backing up bill files and other important data in predefined schedule.

3) Bill error tolerance

• A protective mechanism of the bill pool is provided.

• The system is able to create the bill directory automatically for recovery after it is deleted intentionally.

• Offline repair of error bills is available.

4) Transmission reliability

The OSS-BSS Server transmits bills to the billing center by means of Telnet and Web service access to bill data has been provided as well. Both retransmission and broken retransmission are supported.

III. Three-level buffer of bill information

From the completion of a call to the successful transfer of bill information to the billing center, there are three levels of bill buffer against bill data loss due to abnormal causes. The three levels are core bill pool buffer, original bill file buffer and final bill file buffer.

1) Core bill pool buffer

Every core server provides a bill buffer for about 100,000,000 original bills.

2) Original bill file buffer

After transferred from the core bill pool to the OSS-BSS Server, the original bills are stored first in the hard disk as the level-two buffer. At the full configuration, the OSS-BSS Server can accommodate 12,000,000,000 bills.

3) Final bill file buffer

After having processed the original bills, the OSS-BSS Server saves in the hard disk the final bill data to be sent to the billing center, thus implementing the level-three buffer.

IV. Security of OSS-BSS terminal

1) OSS-BSS terminal is secured by Username and password. If the user makes no operation for a long time, the OSS-BSS terminal will automatically log off against unauthorized access.

2) Operation restriction of OSS-BSS terminal and logs can be viewed at the OSS-BSS terminal, but they cannot be deleted or modified for the purpose of ensuring the security of bill data.

3) IP address restriction of OSS-BSS terminal is possible by configuring the Web Service to restrict the IP address of this terminal to prevent unauthorized nodes from accessing.

6.2 System Security Design

6.2.1 Networking Application Security

I. Closing unused protocol interfaces

KSS200 provides protocol interfaces to communicate with telecom network. On these interfaces, except necessary services such as MGCP, H.248, SIP, H.323 and INAP, any other unnecessary network services such as HTTP are disabled, so as to prevent intrusion by unauthorized users through invalid services.

II. Supporting IPSec protocol against DoS attacks

KSS200 uses very reliable procedures to implement the firewall functions and supports a complete IPSec protocol, which effectively prevents the system from being attacked by unauthorized access by means of DoS.

6.2.2 Protocol and Conversation Security

KSS200 supports encryption processing on the security and packets of the MGCP, H.248, SIP and H.323 protocols for the purpose of guaranteeing the security of both protocols and call conversations.

6.2.3 User Security

I. Supporting access certification and authentication

KSS200 supports certification processing on all gateways, SIP Phones and soft terminals to avoid unauthorized registration.

II. Supporting encryption and ciphering of certification information

KSS200 supports encryption and ciphering processing on certification information and identification and tracking on malicious certification requests. *KSS200* refuses any malicious certification requests.

6.2.4 Data Security

System provides strict data protection mechanisms:

1) *KSS200* supports a synchronous data backup mechanism between the main and backup servers in the real-time manner. Whenever a server goes down, its backup is automatically switched to be the active one. All programs and data on the server take effect immediately.

2) *KSS200* supports the backup of the data from the main server to a removable storage, which enables a quick restart of the main server after getting data from this storage.

3) *KSS200* supports an automatic backup mechanism of the bills.

6.2.5 Operation and Maintenance Security

The following measures are taken in *KSS200* to ensure the operation and maintenance security of the system:

1) *KSS200* supports the dual-certification logon security management based on account and terminals IP address to avoid dormant troubles caused by account disclosure.

2) *KSS200* supports the multi-level user authority management against authorized access.

3) All operations performed by the maintenance personnel are recorded in a log to ensure the traceability of the operations history.

4) Prompting alarms are available against system exceptions due to unintentional mistakes.

5) An excellent check function is available for operator's configuration activities. Unauthorized configurations will be refused.

6) The maintenance and operation system has a protection for usernames and passwords. If the user makes no operation for a long time, the system will automatically log off against unauthorized access.

Chapter 7 Technical Specifications and Environmental Requirements

7.1 Technical Specifications

7.1.1 System Capacity

Item		Specification
Maximum number of supported gateways (MGW, SGW, TGW, AGW)		1024
Maximum number of supported TDM trunks (through Gateways)		4,000,000
Maximum number of registerable subscribers	POTS subscribers	2,000,000 Interchangeable
	V5.2 subscribers	
	IPN subscribers	
Maximum number of supported multimedia terminals	SIP terminals	
	H.323 terminals	

7.1.2 System Processing Capability

Item	Specification
BHCA of main or backup core server	1,4M
Total BHCA of the system	1M
Call drop rate	< 0.0002%
Call setup time	Calls between intra-domain subscribers: <200 ms
	Calls between both intra-domain subscribers and out-domain subscribers: < 500 ms

7.1.3 Protocol Processing Capability

Item	Specification
Number of supported local signaling point codes	512
Maximum IP signaling bandwidth	4 x 1Gbit/s
Maximum number of supported M2UA links	2,640
Maximum number of supported M3UA links	2,640
SIP session holding capability of main or backup core server	84,000
Number of SCTP associations of main or backup core server	264
Capability of SCTP associations of main or backup core server	3000

7.1.4 Bill Processing Capability

Item	Specification
Buffering capacity of the billing server	4,096 Mbytes
Transfer capability of the billing server	1,200 bills/second
Storage capacity of the OSS-BSS server	1.8 Tbytes
Transfer capability of the OSS-BSS server	1M bills/second

7.1.5 Reliability Specifications

Item	Specification
Repair rate	0.2%
Usability	99.999%
Mean time between failures (MTBF)	> 35 years
Mean time to repair (MTTR)	25 minutes
Pause time	1 minute/year

7.1.6 Power Supply and Power Consumption

I. Power supply

1) Rated voltage: -48 VDC

Servers and network switch are supplied by 220 VAC through a 3KVA inverter.

2) Voltage fluctuations: -56 V to -42 V

II. System power consumption

The power consumption of the system components in a *KSS200* cabinet are shown in Table 8-6.

Functional unit	Power consumption (W)	Type	Configuration
Main core server	< 200	HP DL360 G9	RAM=32(2x16)GB, HDD=SAS 15 146GB x2, CPU=Intel Xeon E5-2620 V3 x2 , RAID #5 Support
Backup core server	< 200	HP DL360 G9	RAM=32(2x16)GB, HDD=SAS 15 146GB x2, CPU=Intel Xeon E5-2620 V3 x2 , RAID #5 Support
Main database server	< 250	HP DL360 G9	RAM=64(4x16)GB, HDD=SAS 15 600 x4, CPU=Intel Xeon E5-2620 V3 x2 , RAID #5 Support
Backup database server	< 250	HP DL360 G9	RAM=64(4x16)GB, HDD=SAS 15 600 x4, CPU=Intel Xeon E5-2620 V3 x2 , RAID #5 Support
OSS-BSS server	< 250	HP DL360 G9	RAM=64(4x16)GB, HDD=SAS 15 600 x4, CPU=Intel Xeon E5-2620 V3 x2 , RAID #5 Support

Network switch	< 100	CISCO WS-C3750G -48TS-S	48 Ports-10/100/1000
Monitoring console	< 60	Aten KVM Switch CL1008	8 Ports
Fan	< 15	48 VDC	Multi Speed
Lighting	< 20	48 VDC	High Bright LED

7.1.7 Cabinet Specifications

Item	Parameter or model
Cabinet model	Ver.5
Cabinet dimensions (height x width x depth)	1750 mm x 650 mm x 1000 mm
Weight of cabinet (at full configuration)	175 kg
Available height of cabinet	42 U (1 U = 44.45 mm)

7.1.8 Environmental Specifications

I. Environmental adaptation

KSS200 can operate normally for a long term in the following environmental conditions:

Height above sea level	< 4,000 m
Atmospheric pressure	75 KPa to 100 KPa
Temperature	-8 °C to +50 °C
Relative humidity	5% to 85%
Earthquake-proof performance	According to type of supports
Air Cleanness	No explosive, conductive, magneto-conductive or corrosive dust.

Chapter 8 Compliant Recommendations and Standards

KSS200 is compliant with the following recommendations and standards.

Serial No.	Recommendation or standard	Issued by
H.248	Media Gateway Control Protocol	ITU-T
H.323	(including H.225.0, H.245, H.450) Packet-based multimedia communications systems	ITU-T
IEC60297	Mechanical structures for electronic equipment - Dimensions of mechanical structures of the 482,6 mm (19 in) series	IEC
Q.701	functional description of the message transfer part (MTP) of Signaling System No.7	ITU-T
Q.702	Signaling Data Link	ITU-T
Q.703	Message Transfer Part Signaling Link	ITU-T
Q.704	Message Transfer Part - Signaling network functions and messages	ITU-T
Q.705	Signaling network structure	ITU-T
Q.706	Message Transfer Part - Signaling performance	ITU-T
Q.707	Message Transfer Part - Testing and maintenance	ITU-T
Q.711	Functional description of the Signaling Connection Control Part (SCCP)	ITU-T
Q.712	Definition and function of SCCP messages	ITU-T
Q.713	SCCP formats and codes	ITU-T
Q.714	Signaling Connection Control Part Procedures	ITU-T
Q.716	Signaling Connection Control Part (SCCP) Performance	ITU-T
Q.730	ISDN user part supplementary services	ITU-T
Q.762	General function of messages and Signals of ISUP	ITU-T
Q.763	Formats and codes of ISUP	ITU-T
Q.764	Signaling procedures of ISUP	ITU-T
Q.771	Specifications of Signaling System No.7; Functional description of transaction capabilities (TC)	ITU-T
Q.772	Specifications of Signaling System No.7; Transaction capabilities information element definitions	ITU-T
Q.773	Specifications of Signaling System No.7; Transaction capabilities formats and encoding	ITU-T
Q.774	Specifications of Signaling System No.7; Transaction capabilities procedures	ITU-T
draft-ietfmidcom-stn-02	Simple Traversal of UDP Through Network Address Translators (STUN)	IETF
draft-ietfsigtran-v5a-03	V5.2-User Adaptation Layer (V5UA)	IETF
FC0768	User Datagram Protocol (UDP)	IETF
FC0791	Internet Protocol (IP)	IETF
FC0792	Internet Control Message Protocol (ICMP)	IETF
FC0793	Transmission Control Protocol (TCP)	IETF
FC0959	File Transfer Protocol (FTP)	IETF
FC1035	Domain Names Implementation and Specification	IETF
FC1157	Simple Network Management Protocol (SNMP)	IETF
FC2327	SDP: Session Description Protocol	IETF
FC2396	Uniform Resource Identifiers (URI): Generic Syntax	IETF
FC2401	Security Architecture for IP (IPSec)	IETF
FC2402	IP Authentication Header (IPSec)	IETF

Serial No.	Recommendation or standard	Issued by
FC2406	IP Encapsulating Security Payload (IPSec)	IETF
FC2411	IP Security Document Roadmap (IPSec)	IETF
FC2543	SIP: Session Initiation Protocol	IETF
FC2705	Media Gateway Control Protocol (MGCP)	IETF
FC2719	Framework Architecture for Signaling Transport	IETF
FC2871	A Framework for Telephony Routing over IP	IETF
FC2897	Proposal for an MGCP Advanced Audio Package	IETF
FC2916	E.164 number and DNS	IETF
FC2960	Stream Control Transmission Protocol (SCTP)	IETF
FC3015	Megaco Protocol Version 1.0 (H.248)	IETF
FC3057	ISDN Q.921-User Adaptation Layer (IUA)	IETF
FC3064	MGCP CAS Packages	IETF
FC3261	Session Initiation Protocol (SIP)	IETF
FC3309	Stream Control Transmission Protocol (SCTP) Checksum Change	IETF
FC3331	SS7 MTP2 User Adaptation Layer (M2UA)	IETF
FC3332	SS7 MTP3-User Adaptation Layer (M3UA)	IETF
FC3372	Session Initiation Protocol for Telephones (SIP-T)	IETF

Chapter 9 Acronyms and Abbreviations

Reader can find some useful Acronyms and Abbreviations in below table.

Abbreviation	Full name
3G	The Third Generation
3GPP	Third Generation Partnership Project
3rd AS	3rd Party Application Server
A	
AAA	Authentication Authorization and Accounting
ACC	Account Card Calling
ACL	Access Control List
AMG	Access Media Gateway
API	Application Programming Interface
AS	Application Server
ATM	Asynchronous Transfer Mode
B	
BHCA	Busy Hour Call Attempt
BICC	Bearer independent Call Control Protocol
C	
CAS	Channel Associated Signaling
CCB	Call Control Block
CCC	Credit Card Calling
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CE	Conformity European
CN	Core Network
CODEC	Coder-decoder
CORBA	Common Object Request Broker Architecture
CRBT	Caller Ring Back Tone
CS	Circuit Switched
CTD	Click To Dial
CTF	Click to FAX
D	
DC	Digital Center
DL	Digital Local
DNS	Domain Name Server
DOPRA	Distributed Object-oriented Programmable Real-time Architecture
DoS	Denial of Service
DSS1	Digital Subscriber Signaling No.1
DTMF	Dual-Tone MultiFrequency

E	
EMC	Electromagnetic Compatibility
ETS	European Telecommunication Standards
F	
FAM	Front Administration Module
FE	Fast Ethernet
FPH	Free Phone
FTAM	File Transfer Access and Management Protocol
FTP	File Transfer Protocol
G	
GK	Gatekeeper
GUI	Graphical User Interface
GW	Gateway
H	
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
I	
IAD	Integrated Access Device
ICP	Internet Content Provider
ICW	Internet Call Wait(ing)
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
IP	Internet Protocol
IPN	Internet Personal Number
IPSec	Internet Protocol SECurity extensions
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
IUA	ISDN Q.921 - User Adaptation Layer
IVR	Interactive Voice Response
M	
M2PA	MTP2-User Peer-to-Peer Adaptation Layer
M2UA	Message Transfer Part 2 (MTP2) - User Adaptation Layer
M3UA	Message Transfer Part 3 (MTP3) - User Adaptation Layer
MAN	Metropolitan Area Network
MAS	Mass calling

MGW	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MML	Man Machine Language
MRS	Media Resource Server
MTBF	Mean Time Between Failure
MTP	Message Transfer Part
MTTR	Mean Time To Repair
N	
NAS	Network Access Server
NAT	Network Address Translation
NEBS	Network Equipment Building System
NGN	Next Generation Network
NMS	Network Management System
NP	Number Portability
O	
OSS-BSS	Operation Service Support-Business Service Support
P	
PBX	Private Branch Exchange
PCA	Personal Communication Assistant
PDA	Personal Digital Assistant
PGW	Parlay Gateway
PLMN	Public Land Mobile Network
POTS	Plain Old Telephone Service
PPS	Pre-Paid Service
PRI	Primary Rate Interface
PS	Packed Switched
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
PTN	Personal Telecommunication Number
Q	
QoS	Quality of Service
R	
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Arrays of Inexpensive Disks
RGW	Regional Gateway
RTP	Real-time Transport Protocol
S	
SCCP	Signaling Connection Control Part
SCN	Switched Circuit Network
SCP	Service Control Point

SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SDP	Service Data Point
SGW	Signaling Gateway
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol
SMP	Service Management Point
SMS	Service Management System
SNMP	Simple Network Management Protocol
SP	Signaling Point
SS7	Signaling System No.7
SSP	Service Switching Point
STP	Signaling Transfer Point
STUN	Simple Traversal of UDP Through Network Address Translators
T	
TCAP	Transaction Capabilities Application Part
TCP	Transport Control Protocol
TDM	Time Division Multiplex(ing)
TGW	Trunk Gateway
U	
UC	Unified Communication
UDP	User Datagram Protocol
UM	Unified Messaging
UNI	User Network Interface
UPS	Uninterrupted Power Supply
UPT	Universal Personal Telecommunication
UTP	Unshielded Twisted Pair
V	
V5UA	V5.2 - User Adaptation Layer
VoIP	Voice Over IP
VOT	Tele voting
VPN	Virtual Private Network
W	
WAC	Wide Area Centrex
WWW	World Wide Web
X	
xDSL	x Digital Subscriber Line
XML	Extensible Markup Language


KIATEL
KSS 200
PDB
KSS 200
MCS
KSS 200
BCS
KSS 200
MDBS
KSS 200
BDBS
KSS 200
BDBS
KSS 200
KVMS
KSS 200
INVM