
Remember when you were blown away by technology . . .
IMS as never before seen
VoLTE
VoIP
IPTV
. . .
ut there, your 360° virtual reality

REPUBLIC OF YEMEN
SANA'A UNIVERSITY
FACULITY OF ENGINEERING
ELECTRICAL DEPARTMENT

الجـــمهوريـــة اليمنيـــة
جـــامـــعـــة صنعـــــــاء
كليـــــــــة الهـــندسة
قســـم الهندســـة الكهربائية

IP MULTIMEDIA SUBSYSTEM

(IMS)

«Simulation And Emulation »

***Supervisor*:**

Dr. Ali Naji –Nosary

Assistant :

Eng.Ghada AL-Asadi

Presented by/

Kholoud Saleh Hazzam (123/2013) **Najla Abulkhaleq AL-Zubairi (49/2013)**

Leena Abdulbaset AL-Huribi (285/2013) **Anwaar Ahmed AL-Hamdani (307/2013)**

Dedication

For those whom we share love with them, family and friends.

Acknowledgements

At first, we thank Allah for his unlimited gifts.

We would like to express our deepest thanks and gratitude to people whom helped us to achieve this project:

Our parents, the lights of our life.

Our supervisor Dr. Ali Naji Nosary who has accepted to supervise our project, that was such a great honor for us. We would like to thank him for his valuable instructions and notes and for his precious advices.

Eng. Ghada AL- Asadi for listening to us with a big heart and giving us her tips

Eng. Nebras Al-fleesy thanks a lot for his unconditional help every time

Every person whom helped us out to learn from their knowledge and experience to get this project perfectly done, Specially PTC team.

Table of contents:

PART I

Chapter 1

Chapter 2: IMS Architecture

PART II
(Simulation & Emulation)

Chapter 5: VOIP & IPTV

Chapter 6: VOLTE (OPNET)

Figures

Part I

- Chapter 1: Introduction
- Chapter 2: IMS Architecture
- Chapter 3: IMS services and application
- Chapter 4: LTE and VOLTE

Preface

IMS – IP Multimedia Subsystem – is an international, recognized standard; it specifies interoperability and roaming; and it provides bearer control, charging and security. Moreover, it is well integrated with existing voice and data networks, while adopting many of the key characteristics of the IT domain. This makes IMS a key technology for integrating different kinds of networks and providing various well-secured services with minimum operating costs. Therefore, we have chosen IMS as the subject of our project, not only because of its grown importance worldwide, but also because of the need of such technology in our telecommunication networks in Yemen.

The objectives of our project in the following points:

1. Provide a complete well-organized theoretical Introduction to IMS technology.

2. Apply IMS techniques practically using sophisticated software that can simulate and emulate IMS real networks to provide realistic results that can help our national telecommunication organizations.

3. The simulation also showing the stunning capabilities of IMS networks in real applications.

This work took months of hard work. We faced many difficulties during the process of collecting information for the theoretical report. In addition, the software we used required advanced hardware. However, with patience and organized teamwork we finally reached our goals.

In this report, It describes the security threats and the models used to secure communications in the IMS. Introduction of IMS will be introduced in chapter one. Chapter two explains the architecture of IMS that shows layers and protocols. Chapter three explains applications and services. Chapter four explains VOLTE, it shows the LTE basic structure and the connection with IMS core network. Chapter five shows the simulation of each application of IMS, it shows the simulation of VOLTE by OPNET 14.5 software and connection of with practical of IPTV with VOIP by using CUCM, GNS3 and VLC. At the end of the report, the case study of IMS will be clarified between PTC and YM.

Finally, The result of passing VOIP calling ,VOLTE and IPTV had low delay, And multimedia (voice and video) had good quality.

1

Introduction:

The IP Multimedia Subsystem (IMS) has become the leading architecture enabling communication service providers to offer VoIP and multimedia services. The IMS standards, which were developed by 3GPP and embraced by the European Telecommunications Standards Institute and the Telecom & Internet converged Services & Protocols for Advanced Networks (ETSI/TISPAN), are now becoming widely established. Packet Cable, paving the way for future fixed-mobile convergence and Triple Play services, has also adopted these standards. Designed to work with multiple access types, such as Global System for Mobile communications (GSM), Wideband (WCDMA), Code Division Multiple Access (CDMA) 2000, WiMax and Wire line broadband, IMS has become the solution of choice for many communication service providers as a substantial enabler of growth.

Numerous IP telephony and multimedia services are widely available on the traditional internet. However, IMS allows operators to control the Quality of Service of each IMS application from end to end and provides a secure authentication and security access based on the user's SIM card. It will also enable full control to charge the user for the services and ensure interoperability between other networks and terminals [3] .

1.1 The development internet protocol multimedia subsystem:

The new communication paradigm is about networking Internet Protocol (IP)-based mobile devices. These terminals have large, high-precision displays; they have built-in cameras and many resources for applications. They are always-on-always connected application devices. This redefines application. Applications are no longer isolated entities exchanging information only with the user interface. The next generation of more exciting applications are peer-to-peer entities, which facilitate sharing: shared browsing, shared whiteboard, shared game experience, shared two-way radio session. The concept of being connected will be redefined. Dialing a number and talking will soon be seen as a narrow subset of networking. The ability to establish a peer-to-peer connection between the new IP enabled mobile devices is the key ingredient required (Figure 1.1). This new paradigm of communications reaches far beyond the capabilities of good old telephony. It can be built on current General Packet Radio Service (GPRS) networks. In order to communicate, the IP-based applications must have a mechanism to reach the correspondent.

The telephone network currently provides this critical task of establishing a connection.

By dialing the B number, the network can establish an *ad hoc** (refer to chapter 4) connection between any two terminals.
This critical IP connectivity capability is offered only in isolated and single-service provider environments in the Internet. We need a global system—the IMS. It enables applications in mobile devices to establish peer-to-peer connections. True integration of voice and data services increases productivity and overall effectiveness, while the development of innovative applications integrating voice, data and multimedia will create demands for new services, such as presence, multimedia chat, conferencing, push to talk and conferencing. The skill to combine mobility and the IP network will be crucial to service success in the future.

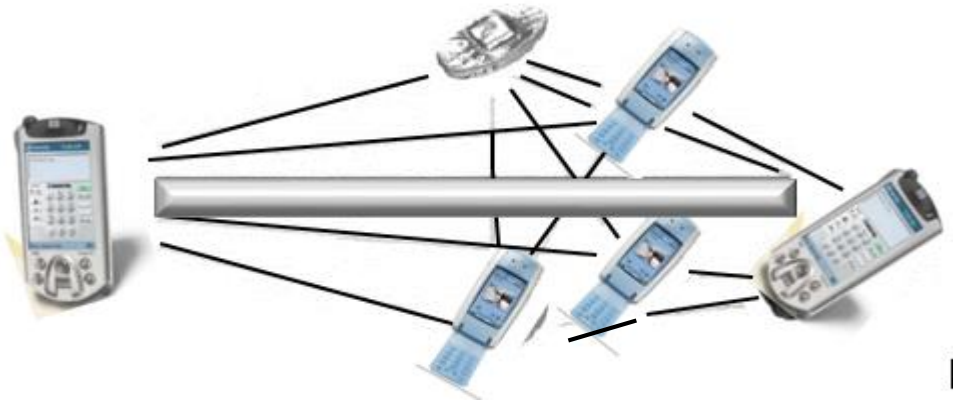


Figure 1.1: The key ingredient to new, enriching user experiences is peer-to-peer IP connections applications.

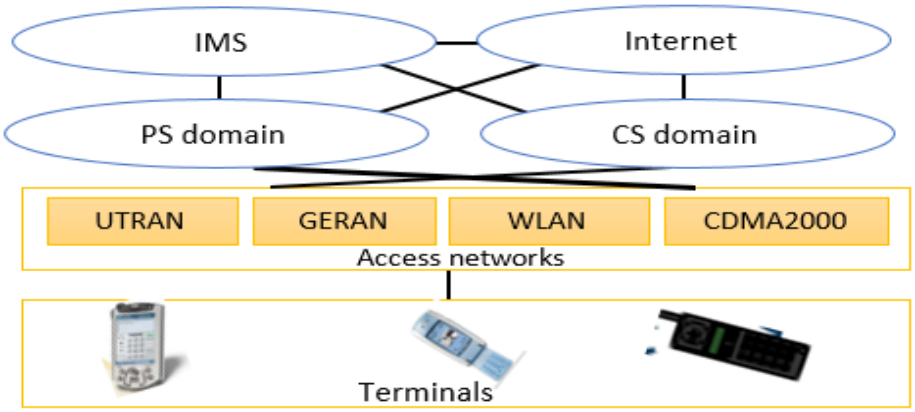


Figure 1.2: The IMS and its relationship with existing communication systems.

Figure 1.2 shows a consolidated network where the IMS introduces multimedia session control in the packet-switched domain and at the same time brings circuit switched functionality in the packet-switched domain. The IMS is a key technology for network consolidation. Traditionally, the mobile communication system has been
connection. Divided in three parts: terminals, the radio access network (RAN) and the core network.

Ad hoc means to connect two or more pcs without routers or central point.it also means peer to peer
This approach needs one change when we are talking about an IMS-based system.

The term "radio access network" should be replaced by "access network" because an IMS system can be deployed over non-RANs as well. It is important to remember that each of these parts can be further split into smaller functional parts along different interfaces. It is important that these interfaces are open and standardized. This book splits IMS into smaller parts and describes how it works as defined in the Third Generation Partnership Project (3GPP) [3].

1.2 The origin of IMS:

1.2.1 from GSM to 3GPP Release 6

The European Telecommunications Standards Institute(ETSI) was the standardization organization that defined the Global System for Mobile Communications (GSM) during the late 1980s and 1990s. ETSI also defined the GPRS network architecture. The last GSM-only standard was produced in 1998, and in the same year the 3GPP was founded by standardization bodies from Europe, Japan, South Korea, the USA and China to specify a third-generation mobile system comprising Wideband Code Division Multiple Access (WCDMA) and Time Division/Code Division Multiple Access (TD-CDMA) radio access and an evolved GSM core network. Most of the work and Cornerstone specifications were inherited from the ETSI Special Mobile Group (SMG). The 3GPP originally decided to prepare specifications on a yearly basis, the first specification release being Release 99.

1.2.2 3GPP Release 99 (3GPP R99)

It took barely a year to produce the first release—Release 1999. The functionality of the release was frozen in December 1999 although some base specifications were frozen afterward—in March 2001. Fast completion was possible because the actual work was divided between two organizations: 3GPP and ETSI SMG. 3GPP developed the services, system architecture, WCDMA and TD-CDMA radio accesses, and the common core network. ETSI SMG developed the GSM/Enhanced Data Rates for Global Evolution (EDGE) radio access. WCDMA radio access was the most significant enhancement to the GSM-based 3G system in Release 1999. In addition to WCDMA, UTRAN (UMTS terrestrial radio access network) introduced the Iu interface as well. Compared with the A and Gb interfaces, there are two significant differences. First, speech transcoding for Iu is performed in the core network. In the GSM it was logically a BTS (base transceiver station) functionality. Secondly, encryption and cell-level mobility management for Iu are done in the radio network controller (RNC). In the GSM they were done in the Serving GPRS Support Node (SGSN) for GPRS services. The Open Service Architecture (OSA) was introduced for service creation. On the service side the target was to stop standardizing new services and to concentrate on service capabilities, such as toolkits (CAMEL, SIM Application Toolkit and OSA). This principle was followed quite well, even though the virtual home environment (VHE), an umbrella concept that covers all service creation, still lacks a good definition.

1.2.3 3GPP Release 4

After Release 1999, 3GPP started to specify Release 2000, including the so-called All-IP that was later renamed as the IMS. During 2000, it was realized that the development of IMS could not be completed during the year. Therefore, Release 2000 was split into Release 4 and Release 5. It was decided that Release 4 would be completed without the IMS. The most significant new functionalities in 3GPP Release 4 were: the MSC Server-MGW concept, IP transport of core network protocols, LCS enhancements for UTRAN and multimedia messaging and IP transport for the Gb user plane. 3GPP Release 4 was functionally frozen and officially completed in March 2001. The backward compatibility requirement for changes, essential for the radio interface, was enforced as late as September 2002.

1.2.4 3GPP Release 5 and Release 6

Release 5 finally introduced the IMS as part of 3GPP standards. The IMS is supposed to be a standardized access-independent IP-based architecture that interworks with existing voice and data networks for both fixed (e.g., PSTN, ISDN, Internet) and mobile users (e.g., GSM, CDMA). The IMS architecture makes it possible to establish peer-to-peer IP communications with all types of clients with the requisite quality of services. In addition to session management the IMS architecture also addresses functionalities that are necessary for complete service delivery (e.g., registration, security, charging, bearer control, roaming). All in all, the IMS will form the heart of the IP core network. The content of Release 5 was heavily discussed, and finally the functional content of 3GPP Release 5 was frozen in March 2002. The consequence of this decision was that many features were postponed to the next release—Release 6. After freezing the content, the work continued and 21 months later, there are still a number of changes to be made in Release 5 IMS. Release 6 IMS is going to fix the shortcomings in Release 5 IMS SIP-based IP multimedia service machinery. It contains a functionality of logical elements, a description of how elements are connected, selected protocols and procedures. It is important to realize that optimization for the mobile communication environment has been designed in the form of user authentication and authorization based on mobile identities, definite rules at the user network interface for compressing SIP messages and security and policy control mechanisms that allow radio loss and recovery detection. Moreover, important aspects from the operator point of view are addressed while developing the architecture, such as charging framework and policy and service control.

The development of IMS is distributed to multiple working groups in 3GPP. 3GPP follows a working method in which the work has three different stages. In stage 1 a service description from a service user and operator point of view are evaluated. In stage 2 problems are broken down into functional elements and the interactions between the elements are identified. In stage 3 all the protocols and procedures are defined in detail. Figure 1.3 shows the most important working groups and responsibility areas that are involved in the development of IMS.

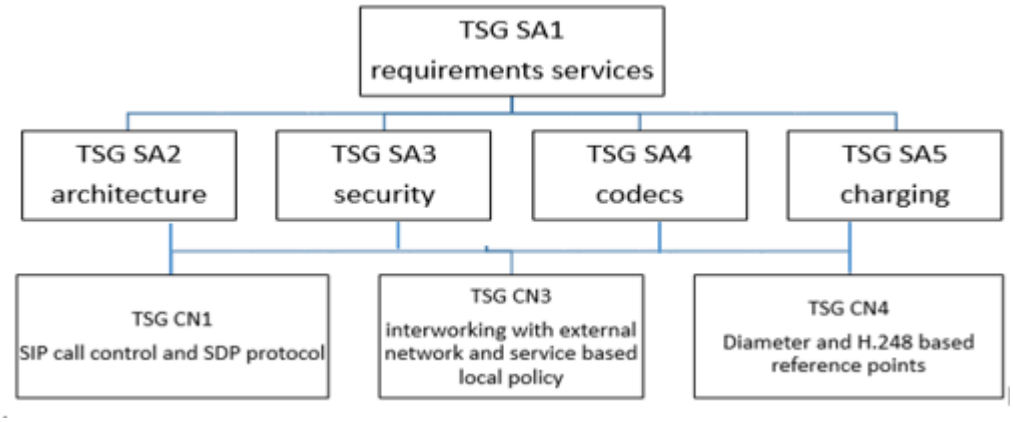


Figure 1.3: Main 3GPP working groups doing IMS work

1.3 Other relevant standardization bodies

1.3.1 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a standardization body that assumes the task of developing and evolving the Internet and its architecture, as well as ensuring the smooth and secure operation of it. The IETF is made up of network designers, academics, engineers and researchers from many companies, volunteering their time and effort to achieve the common goal. IETF participation does not require membership and is open to any individuals who share the same interests. The IETF is divided into areas that are managed by area directors. Each area has a specific topic to work on. Each area has a number of working groups each tasked to complete a specific charter, concentrating on a specific topic within the area. The areas are : applications, general, Internet, operations and management, routing, security, sub-IP and transport. Each working group produces Internet Drafts that, after many reviews, become standards and are labelled as Requests For Comment (RFC) which get assigned a number.

1.3.2 Open Mobile Alliance

In June 2002 the mobile industry set up a new, global organization called the Open Mobile Alliance (OMA). OMA has taken its place as the leading standardization organization for doing mobile service specification work. OMA's role is to specify different service enablers, such as digital rights management and push to talk over the cellular service (PoC). OMA has recognized that it is not beneficial for each service enabler to have its own mechanism for security, quality of service, charging, session management, etc. On the contrary, service enablers should be able to use an infrastructure that provides these basic capabilities. This is where the IMS steps into the OMA landscape. Different service enablers developed in OMA can interface to the IMS, can utilize IMS capabilities and the resources of their underlying network infrastructure via the IMS. Usage of the IMS infrastructure would greatly shorten the specification time of service enablers and would bring modularity to the system, which is definitely a common interest in the industry. Therefore, co-operation between the

OMA and 3GPP will increase in the future. It is very likely that the OMA will gradually take overall responsibility for the invention and design of various applications and services on top of the IMS architecture, while 3GPP will continue to develop the core IMS.

1.3.3 Third Generation Partnership Project 2 (3GPP2)

The Third Generation Partnership Project 2 (3GPP2) is a collaborative project for developing a third-generation mobile system for the ANSI (American National Standards Institute) community. 3GPP2 comprises organizational partners (ARIB, CCSA, TIA, TTA and TTC) and market representation partners (the CDMA Development Group and the IPv6 Forum).
3GPP2's role in IMS standardization lies in specifying IMS as part of the Multimedia Domain solution that further contains the Packet Data Subsystem. The Multimedia Domain and the CDMA2000 Access Network together form the third-generation All IP Core Network in 3GPP2. 3GPP2 has adopted core Release 5 IMS specifications as a baseline from its sister project, 3GPP. However, there are differences between 3GPP2 IMS and 3GPP IMS Release 5solutions due to different **10** The IMS underlying packet and radio technology. Additionally, in some areas 3GPP2 has defined further additions or limitations.
Here are some of the main issues that relate to the first IMS releases:

- IP Policy Control between IMS and the Packet Data Subsystem is not supported in 3GPP2.
- The IMS entry point P-CSCF may be located in a different network than the Packet Data Subsystem. In 3GPP the P-CSCF and the Gateway GPRS Support Node are always located in the same network.
- IP version 4 is also supported in 3GPP2 IMS, whereas 3GPP IMS exclusively supports IP version 6.
- No default codec is specified in 3GPP2.
- Differences in charging solutions.
- No support for a Universal Integrated Circuit Card that could contain an IP Multimedia Services Identity Module for storing, say, IMS access parameters.
- Customized Applications for Mobile Network Enhanced Logic (CAMEL)- related functions are not supported.
- The architecture does not contain the Subscription Locator Functional entity nor a reference point for discovering a database that holds the user's subscription. IMS was originally defined by an industry forum called 3G. IP, formed in 1999. 3G. IP developed the initial IMS architecture, which was brought to the 3rd Generation Partnership Project (3GPP), as part of their standardization work for 3G mobile phone systems in UMTS networks [1].

1.4 Why do we need IMS (IP Multimedia Subsystem)

Why do we need IMS, if all the power of Internet is already provided by latest 4G/LTE networks deployed across the world. The three most important reason:

1) QoS (Quality of Service)
2) Charging
3) Integration of different services

The main issue with the packet-switched domain to provide real-time multimedia services is that it provides a best-effort service without QoS. The network offers no guarantees about the amount of bandwidth a user gets for a particular connection or about the delay the packets experience. Consequently, the quality of a VoIP conversation can vary dramatically throughout its duration. Trying to maintain a conversation (or a videoconference) with poor QoS can soon become a nightmare. So, one of the reasons for creating the IMS was to provide the QoS required for enjoying, rather than suffering, real-time multimedia sessions. The IMS takes care of synchronizing session establishment with QoS provision so that users have a predictable experience.

Another reason for creating the IMS was to be able to charge multimedia sessions appropriately. A user involved in a videoconference over the packet-switched domain usually transfers a large amount of digital information. Operators typically charge based on the number of bytes transferred. The user's operator cannot follow a different business model to charge the user because the operator is not aware of the contents of those bytes: they could belong to a VoIP session, to an instant message, to a web page, or to an email. On the other hand, if the operator is aware of the actual service that the user is using, the operator can provide an alternative charging scheme that may be more beneficial for the user. That's exactly what the IMS does. The IMS does not mandate any particular business model. Instead, it lets operators charge as they think more appropriate. The IMS provides information about the service being invoked by the user, and with this information the operator decides whether to use a flat rate for the service, apply traditional time-based charging, apply QoS-based, or perform any new type of charging.
Providing integrated services to users is the third main reason for the existence of the IMS. Although large equipment vendors and operators will develop some multimedia services, operators do not want to restrict themselves to these services. Operators want to be able to use services developed by third parties, combine them, integrate them with services they already have, and provide the user with a completely new service. For example, an operator has a voicemail service able to store voice messages and a third party develops a text-to-speech conversion service. If the operator buys the text-to speech service from the third party, it can provide voice versions of incoming text messages for blind users. The IMS defines the standard interfaces to be used by service

developers. This way, operators can take advantage of a powerful multi-vendor service creation industry, avoiding sticking to a single vendor to obtain new services.

1.5 Features of IMS:

Features of IMS, which have attracted both wireless and wireline service providers are:

i) Integration of multimedia services:

Service providers can integrate voice, video and data services and provide them on a single platform. IMS brings the internet's power to the communication world. Today voice is the only application that is completely "converged" — all mobiles can access all fixed lines and vice versa. However, it is not always possible to send text from a fixed device, have a PC instant messaging session with a mobile device, or a video call across the two networks. Making this possible clearly has significant revenue implications, and is in line with the trend towards fixed-mobile convergence.

ii) Mobility:

Without depending upon the location of the user, IMS provides access to the user's specific set of services.

iii) Vendors' independence:

Due to the modular architecture of IMS, various service providers can integrate different components or modules from different solution providers into the same system. This also optimizes the investment involved [3].

iv) Interworking with legacy networks:

As IMS is progressively introduced in the operational networks, there will be a need for supporting both new and existing services in either the conventional CS or in the IMS mode, or, in fact, both in the CS and IMS modes. In the long term, all services are likely to be provided using the IMS. However, there will be a no negligible transitional period, where some services will be offered to a user over both CS and IMS. It is important, therefore, that during this transitional period the user experience remains favorable. One of the goals of the IMS is to provide a unified way of handling communications not only for operators but also for users. The IMS users should be able to communicate with all users supported by legacy networks, such as the PSTN. The IMS architecture includes gateways toward other networks in order to provide its users with cross network communications. For example, the gateways
can convert VoIP sessions of the IMS to CS calls of the PSTN or SIP-based instant messages of the IMS to SMSs on a cellular network. Thus, the IMS enables the

integration of different communication islands into a single universal communication network. It also allows users to communicate with other users in a universal way, regardless of the specifics of the network or of the communication community to which these users connect. In this way, all isolated personal communication islands may be connected in a unified fashion, regardless of the specific communications services requested.

V) Hardware Platform:

Fig. 1.4 illustrates an example hardware platform designed for the IMS nodes such as the HSS and CSCF. 12 UPBs were installed in a sub rack of this hardware platform. Every UPB relies on two Intel Xeon 5138 (2.13 GHz) low power-consumption dual-core processors. Each processor has 4-MB level-2 cache. The UPB supports a maximum of four FB-DIMMs. The storage capacity of a memory module may be 512 MB, 1 GB, 2 GB, or 4 GB. Therefore, the maximum memory capacity of the UPBs is 8 GB, and they are capable of employing ECCs and an SDCC. A UPB has two Base interfaces (Ethernet 10/100/1000 M Base-T), two fabric interfaces (Ethernet 1000 M Base-BX), and one Update interface (Ethernet 1000 M Base-BX). Based on this platform, an example of the HSS may be capable of supporting up to ten million IMS subscribers, which is sufficiently high for any realistic teletraffic scenario across the globe. The HSS guarantees a 99.9% message delivery success ratio.
The transaction delay is less than 500 ms and the user registration time is less than 1 s. This CSCF product is capable of implementing I-, P-, and S-CSCFs [6].

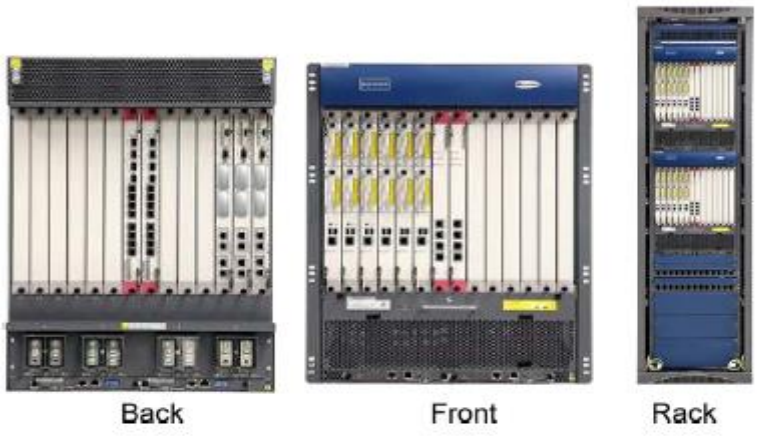


Figure 1.4: Huawei's hardware platform for the IMS.

IV) Many other feature:

- ✓ IMS also provides features like security and QoS thus making it a perfect and complete service platform for NGN.
- ✓ It also provides a uniform environment for billing, enabling more flexible ways for operators to charge subscribers. This is becoming increasingly important as operators try to find the best way to charge for different

services as well as put together attractive bundles for different market segments.

- ✓ Among the new services being enabled by IMS are: video sharing, presence service, Instant Messaging (IM), VoIP, Push-to-Talk over Cellular (PoC), ref. to Figure1.5, conferencing, rich-call features, multimedia gaming, and voice messaging [3].

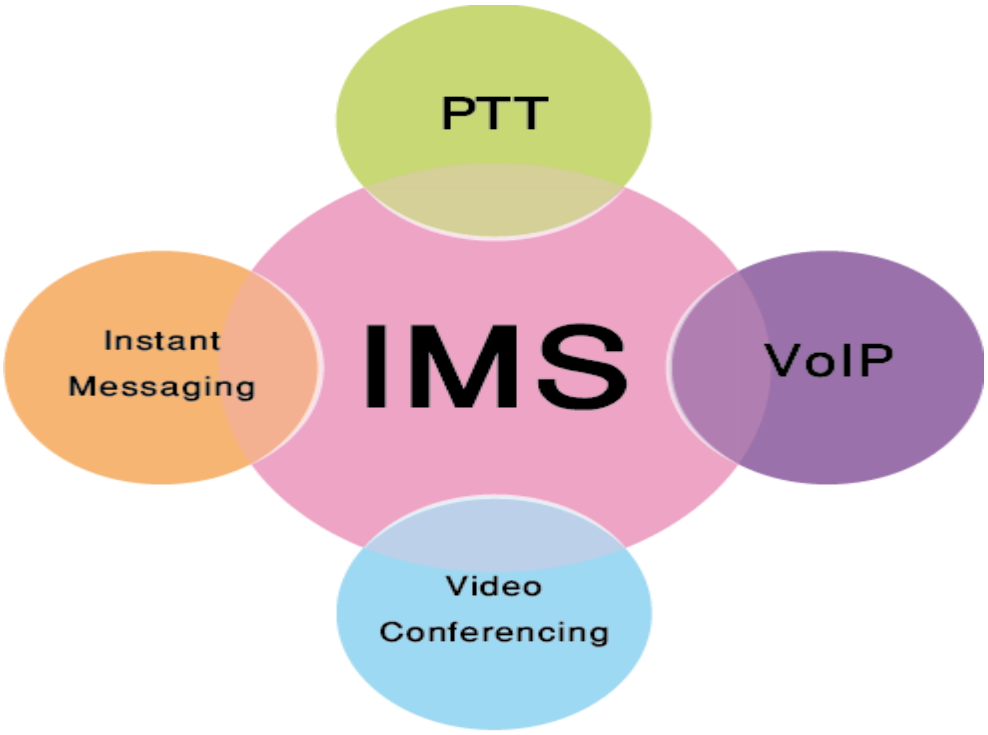


Figure 1.5: IMS video sharing, Instant Messaging (IM), VoIP, Push-to-Talk

Chapter 2
IMS Architecture

2

IMS architecture

The IP-Multimedia Subsystem (IMS) defines the functional architecture for a managed IP-based network. It aims to provide a means for carriers to create an open, standards-based network that delivers integrated multimedia services to increase revenue, while also reducing network CapEx and OpEx. IMS was originally designed for third-generation mobile phones, but it has already been extended to handle access from Wi-Fi networks, and is continuing to be extended into an access-independent platform for service delivery, including broadband fixed-line access. It promises to provide seamless roaming between mobile, public Wi-Fi and private networks for a wide range of services and devices. The IMS architecture has been designed to enable operators to provide a wide range of real-time, packet-based services and to track their use in a way that allows both traditional time-based charging as well as packet and service-based charging. It has become increasingly popular with both wire line and wireless service providers as it is designed to increase carrier revenues, deliver integrated multimedia services, and create an open, standards-based network [7].

2.1 Architectural requirements

There is a set of basic requirements which guides the way in which the IMS architecture has been created and how it should evolve in the future. This section covers the most significant requirements.

2.1.1 IP connectivity

A fundamental requirement is that a client has to have IP connectivity to access IMS services. IP connectivity can be obtained from either the home network or the visited network.

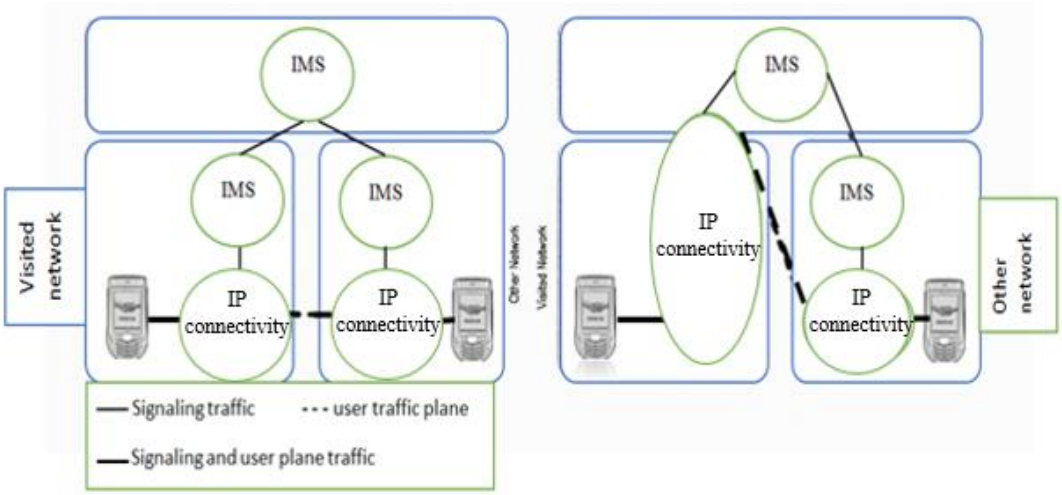


Figure 2.1: IMS connectivity options when a user is roaming.

The leftmost part of Figure 2.1 presents an option in which user equipment (UE) has obtained an IP address from a visited network. In the Universal Mobile network (RAN), Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) are located in the visited network when a user is roaming in the visited network. The rightmost part of Figure 2.1 presents an option in which a UE has obtained an IP address from the home network. In the UMTS network, this means that the RAN and SGSN are located in the visited network when a user is roaming in the visited network. Obviously, when a user is located in the home network, all necessary elements are in the home network and IP connectivity is obtained in that network. It is important to note that a user can roam and obtain IP connectivity from the home network as shown in the figure. This would allow users to use new, fancy IMS services even when they are roaming in an area that does not have an IMS network but provides IP connectivity. In theory, it is possible to deploy an IMS network in a single area/country and use, say, General Packet Radio Service (GPRS) roaming to connect customers to the home network. In practice this would not happen because routing efficiency would not be high enough. Consider routing real time transport protocol (RTP) voice packets from the USA to Europe and then back to the USA.
However, this deployment model is important when operators are ramping up IMS networks or, in an initial phase, when they are offering non or near-real time multimedia services.

2.1.2 Access independence

The IMS is designed to be access-independent so that IMS services can be provided over any IP connectivity networks (e.g., GPRS, WLAN, broadband access x-Digital Subscriber Line). Unfortunately, Release 5 IMS specifications contain some GPRS specific features. In Release 6 (e.g., GPRS) access-specific issues will be separated from the core IMS description. 3GPP uses the term "IP connectivity access network" to refer to the collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities. In this book we use GPRS as an example [7].

2.1.3 Ensuring quality of service for IP multimedia services

On the public Internet, delays tend to be high and variable, packets arrive out of order and some packets are lost or discarded. This will no longer be the case with the IMS. The underlying access and transport networks together with the IMS provide end-to-end quality of service (QoS).
Via the IMS, UE negotiates its capabilities and expresses its QoS requirements during a Session Initiation Protocol (SIP) session set-up or session modification procedure.

The UE is able to negotiate such parameters as:

- Media type, direction of traffic.
- Media type bit rate, packet size, packet transport frequency.
- Usage of RTP pay load for media types.
- Bandwidth adaptation.

After negotiating the parameters at the application level, UEs reserve suitable resources from the access network. When end-to-end QoS is created, the UEs encode and packetize individual media types with an appropriate protocol (e.g., RTP) and send these media packets to the access and transport network by using a transport layer protocol (e.g., TCP or UDP) over IP. It is assumed that operators negotiate service-level agreements for guaranteeing the required QoS in the interconnection backbone. In the case of UTMS, operators could utilize the GPRS Roaming Exchange backbone.

2.1.4 IP policy control for ensuring correct usage of media resources

IP policy control means the capability to authorize and control the usage of bearer traffic intended for IMS media, based on the signaling parameters at the IMS session. This requires interaction between the IP connectivity access network and the IMS. The means of setting up interaction can be divided into three different Categories:

- The policy control element is able to verify that values negotiated in SIP signaling are used when activating bearers for media traffic. This allows an operator to verify that its bearer resources are not misused (e.g., the source and destination IP address and bandwidth in the bearer level are the same as used in SIP session establishment).
- The policy control element is able to enforce when media traffic between end points of a SIP session start or stop. This makes it possible to prevent the use of the bearer until the session establishment is completed and allows traffic to start/ stop in synchronization with the start/stop of charging for a session in IMS.
- The policy control element is able to receive notifications when the IP connectivity access network service has either modified, suspended or released the bearer(s) of a user associated with a session. This allows IMS to release ongoing session because, for instance, the user is no longer in the coverage area.

2.1.5 Secure communication

Security is a fundamental requirement in every telecommunication system and the IMS is not an exception. The IMS provides at least a similar level of security as the corresponding GPRS and circuit-switched networks: for example, the IMS ensures that users are authenticated before they can start using services, and users are able to request privacy when engaged in a session. Section 3.6 will discuss security features in more detail.

2.1.6 Charging arrangements

From an operator or service provider perspective the ability to charge users is a must in any network. The IMS architecture allows different charging models to be used.
This includes, say, the capability to charge just the calling party or to charge both the calling party and the called party based on used resources in the transport level. In the latter case the calling party could be charged entirely on IMS-level session: that is, it is possible to use different charging schemes at the transport and IMS level. However, an operator might be interested to correlate charging information generated at transport and IMS (service and content) charging levels. This capability is provided if an operator utilizes a policy control reference point. As IMS sessions may include multiple media components (e.g., audio and video), it is required that the IMS provides a means for charging per media component.
This would allow a possibility to charge the called party if she adds a new media component in a session. It is also required that different IMS networks are able to exchange information on the charging to be applied to a current session. The IMS architecture supports both online and offline charging capabilities. Online charging is a charging process in which the charging information can affect in real time the service rendered and therefore directly interacts with session/service control. In practice, an operator could check the user's account before allowing the user to engage a session and to stop a session when all credits are consumed. Prepaid services are applications that need online charging capabilities. Offline charging is a charging process in which the charging information does not affect in real time the service rendered. This is the traditional model in which the charging information is collected over a particular period and, at the end of the period, the operator posts a bill to the customer.

2.1.7 Support of roaming

From a user point of view, it is important to get access to her services regardless of her geographical location. The roaming feature makes it possible to use services even though the user is not geographically located in the service area of the home network. Section 2.1.1 has already described two instances of roaming: namely, GPRS roaming and IMS roaming. In addition to these two there exists an IMS circuit-switched (CS) roaming case. GPRS roaming means the capability to access the IMS when the visited

network provides the RAN and SGSN and the home network provides the GGSN and IMS. The IMS roaming model refers to a network configuration in which the visited network provides IP connectivity (e.g., RAN, SGSN, and GGSN) and the IMS entry point (i.e., P-CSCF) and the home network provides the rest of the IMS functionalities. The main benefit of this roaming model compared with the GPRS roaming model is optimum usage of user-plane resources. Roaming between the IMS and the CS CN domain refers to inter-domain roaming between IMS and CS. When a user is not registered or reachable in one domain a session can be routed to the other domain. It is important to note that both the CS CN domain and the IMS domain have their own services and cannot be used from another domain. Some services are similar and available in both domains (e.g., Voice over IP in IMS and speech telephony in CSCN). Figure 2.2 shows different IMS/CS roaming cases.

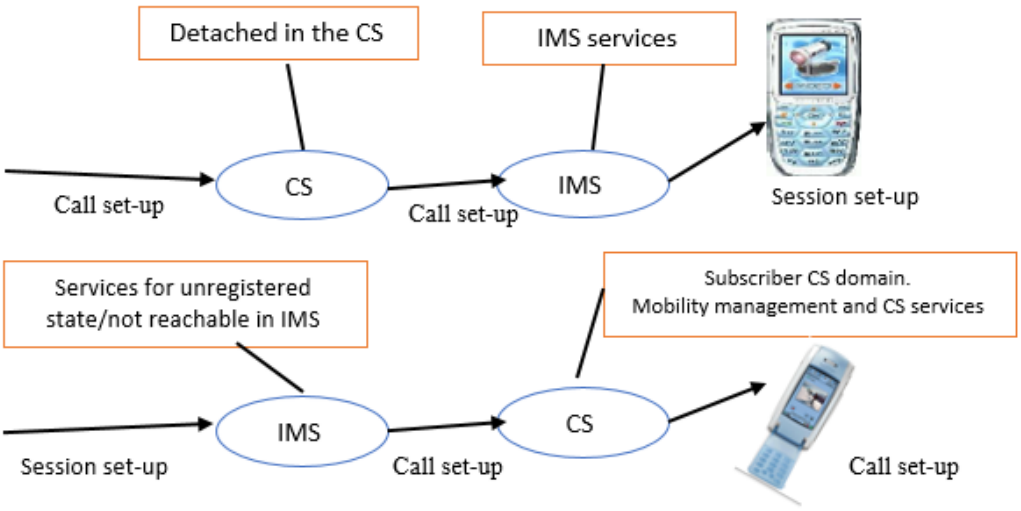


Figure 2.2: IMS/CS roaming alternatives.

2.1.8 Interworking with other networks

It is evident that the IMS is not deployed over the world at the same time. Moreover, people may not be able to switch terminals or subscriptions very rapidly. This will arise the issue of being able to reach people regardless of what kind of terminals they have or where they live. To be a new, successful communication network technology and architecture the IMS has to be able to connect to as many users as possible. Therefore, the IMS supports communication with PSTN, ISDN, mobile and Internet users. Additionally, it will be possible to support sessions with Internet applications that have been developed outside the 3GPP community.

2.1.9 Service control model

In 2G mobile networks, the visited service control is in use. This means that, when a user is roaming, an entity in the visited network provides services and controls the traffic for the user. This entity in 2G is called a visited mobile service-switching center.

In the early days of Release 5 both visited and home service control models were supported. Supporting two models would have required that every problem have more than one solution; moreover, it would reduce the number of optimal architecture solutions, as simple solutions may not fit both models. Supporting both models would have meant additional extensions for Internet Engineering Task Force (IETF) protocols and increased the work involved in registration and session flows. The visited service control was dropped because it was a complex solution and did not provide any noticeable added value compared with the home service control. On the contrary, the visited service control imposes some limitations. It requires a multiple relationship and roaming models between operators. Service development is slower as both the visited and home network would need to support similar services; otherwise roaming users would experience service degradations. In addition, the number of interoperate reference points increase, which requires complicated solutions (e.g., in terms of security and charging). Therefore, the home service control was selected; this means that the entity that has access to the subscriber database and interacts directly with service platforms is always located at the user's home network.

2.1.10 Service development

The importance of having a scalable service platform and the possibility to launch new services rapidly has meant that the old way of standardizing complete sets of teleservices, applications and supplementary services is no longer acceptable. Therefore, 3GPP is standardizing service capabilities and not the services themselves. The IMS architecture should actually include a service framework that provides the necessary capabilities to support speech, video, multimedia, messaging, file sharing, data transfer, gaming and basic supplementary services within the IMS.

2.1.11 Layered design

3GPP has decided to use a layered approach to architectural design. This means that transport and bearer services are separated from the IMS signaling network and session management services.

Further services are run on top of the IMS signaling network. Figure 2.3 shows the design. In some cases, it may be impossible to distinguish between functionality at the upper and lower layers. The layered approach aims at a minimum dependency between layers. A benefit is that it facilitates the addition of new access networks to the system later on.

Wireless Local Area Network (WLAN) access to the IMS, in 3GPP Release 6, will test how well the layering has been done. Other accesses may follow (e.g., fixed broadband).

The layered approach increases the importance of the application layer. When applications are isolated and the underlying can provide common functionalities IMS network the same applications can run on UE using diverse access types.

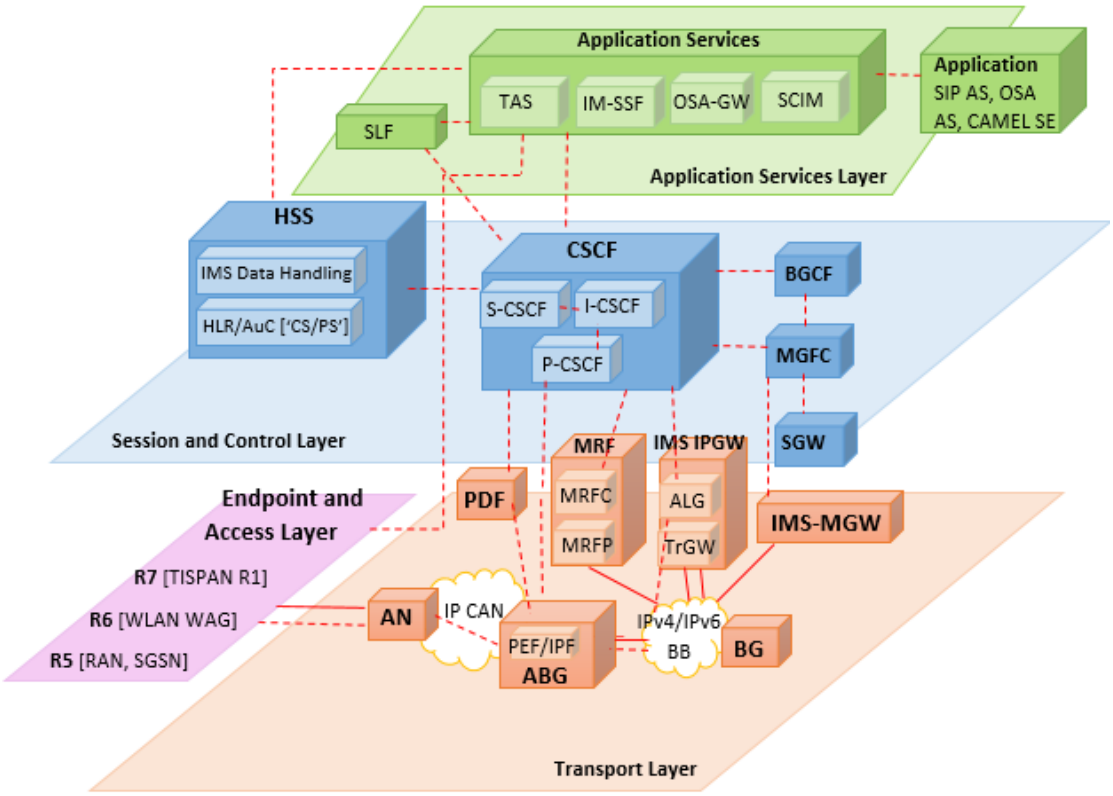


Figure 2.3: IMS units and layering architecture.

IMS was originally designed for third-generation mobile phones, but it has already been extended to handle access from Wi-Fi networks, and is continuing to be extended into an access-independent platform for service delivery, including broadband fixed-line access. It promises to provide seamless roaming between mobile, public Wi-Fi and private networks for a wide range of services and devices. The IMS architecture has been designed to enable operators to provide a wide range of real-time, packet-based services and to track their use in a way that allows both traditional time-based charging as well as packet and service-based charging. It has become increasingly popular with both wire line and wireless service providers as it is designed to increase carrier revenues, deliver integrated multimedia services, and create an open, standards-based network [1].

2.2 IMS layers

The diagram below shows the IP Multimedia Subsystem architecture.

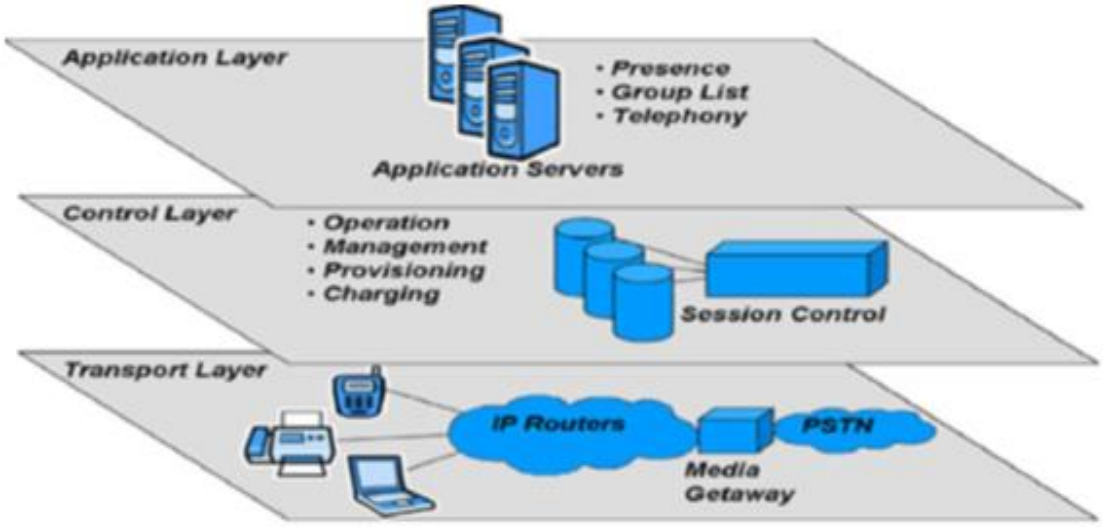


Figure 2.4: Layers of IMS

2.2.1 Three layers of core network

The IMS core network is defined as a layered network consisting of a Media Transport Layer (e.g. voice, video, data etc.), Control Layer (e.g. SIP control, transport control etc.) and Service or application Layer (to provide added functionality to IMS core network) ref. to Figure 2.4.

1. Transport layer

This layer is responsible for the network access. It allows different IMS devices and user equipment's connect to the IMS network. IMS devices may connect to the network in the transport layer using different techniques like fixed access (DSL, cable modems, Ethernet etc.), mobile access (wideband code division multiple access i.e. WCDMA, GPRS) and wireless access (WiMax or WLAN). This layer also lets IMS devices to receive and place calls to and from the public switched telephone networks (PSTN) or any other circuit switched network through the media gateways. This layer establishes the user equipment IP connectivity. After getting an IP address and ability to exchange SIP messages user equipment will be responsible for its own IMS interaction, independent of the underlying network access technology [1].

2. Control layer

This layer is the home of various call session control functions (CSCFs). Three SIP signaling servers handle these functions:

- The proxy CSCF (P-CSCF)
- The interrogating CSCF (I-CSCF)
- The serving CSCF (S-CSCF)

3. Service or application layer

Two layers mentioned above provide an integrated and standardized network platform to let the service provider's offer various multimedia services in the service layer. Application servers provide the interface with the control layers using the SIP protocol [1].

2.2.2 Description of the components

1. Call State Control Functions (CSCFs):

The SIP (Session Initiation Protocol) is used as the signaling protocol that establishes controls, modifies and terminates session of voice, video and messaging between two or more participants. These signaling points are known as Call State Control Functions (CSCFs). The three CSCF's are described below:

a. Proxy Call Session Control Function:

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, 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). Some networks might use a Session Border Controller for this function.

b. Interrogating Call Session Control Function:

An 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.
- Up to Release 6 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).
- From Release 7 onwards this "entry point" function is removed from the I-CSCF and is now part of the IBCF (Interconnection Border Control Function). The IBCF is used as gateway to external networks, and provides NAT and Firewall functions (pin holing).

c. Serving Call Session Control Function:

An 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**.**

- It 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.
- it 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. The HSS assigns the S-CSCF to a user, when it is queried by the I-CSCF.

2. Policy decision function PDF:

- Responsible for making policy decisions based on session and media-related information obtained from the P-CSCF.
- Acts as policy decision point for Service-based Local Policy (SBLP) control.
- Some of policy decision point functionalities:
  - To store session and media-related information.
  - The capability to enable the usage of an authorized bearer (e.g. PDP context)
  - To inform P-CSCF when the bearer is lost or modified.
  - To pass an IMS-charging identifier to the GGSN and to Pass a GPRS-charging identifier to the P-CSCF.

3. Home Subscriber Server or User Profile Server Function UPSF:

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
- It contains subscription information used by the service layer
- it provides data used to perform authentication and authorization of the user
- it 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.

4. Signaling gateway:

Used to interconnect different signaling networks, such as SCTP-IP-based signaling networks and SS7 signaling networks.

- Performs signaling conversion at the transport level.
- Does not interpret application layer messages.

5. Subscription Locator Function

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.

6. Media Resource Function

An MRF is a source for network initiated and network managed media streams in the home network.
It is exploited for:

- 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.

7. IMS Core Network Element: BGCF Break Out Gateway Control Function

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.
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.

8. IMS Core Network Element: PSTN Gateways

The interworking with the Circuit Switched network is realized by several components, for signaling, media and control functionalities:
SGW (Signaling Gateway) 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.
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.
- 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).

9. Application Servers

Application Servers 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 to the IMS infrastructure.
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
- Conference call services
- Location based services
- SMS, MMS
- Presence information, Instant messaging
- Voice Call Continuity Function (VCC Server) or Fixed Mobile Convergence

10. IP Multimedia - Service-Switching Function:

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. [4]

2.3 Security threats for IMS:

There are a number of security threats already established for IP networks (and well exploited). These attacks can be prevented through some practices and do not necessarily require huge investments to prevent. The main threats today are:

- Eavesdropping
- Registration hijacking
- Server impersonation
- Message body tampering
- Session teardown
- Denial-of-service
- Amplification

Security measures should be deployed at different points in the network to provide a range of security aspects, including:

- User authentication
- Network-to-network authentication
- Service authorization, according to subscriptions, roaming agreements, etc.
- Charging policies and enforcement, preventing fraud, ensuring accurate billing
- Resourcing policy enforcement, protecting against DoS or misuse of resources
- Security key management for reliable identification
- Data confidentiality and user privacy, protecting network data as well as the user's data
- Data integrity, preventing database corruption or "poisoning"

There are numerous ways one can secure networks. In GSM networks, subscriber authentication is already implemented. The use of SIMs containing cipher and authentication keys within a GSM phone allows networks to verify the device is legitimate and the subscriber is authenticated.

Encryption is supported as well over the air interface. This prevents eavesdropping over the radio waves, which is a major concern within GSM circles. There are already a number of devices that support "sniffing" the airwaves and capturing GSM signaling, unless they are encrypted. Keeping the subscriber confidential is also supported in the GSM world. The concept of the private user identity and the public user identity actually comes from GSM. The private user identity is maintained closely and kept from other networks, so only the home network knows this identity [5].

2.4 IMS protocols

2.4.1 Diameter

1. Introduction

Diameter is an authentication, authorization and accounting (AAA) protocol developed by the Internet Engineering Task Force (IETF). Diameter is used to provide AAA services for a range of access technologies. Instead of building the protocol from scratch, Diameter is loosely based on the Remote Authentication Dial in User Service (RADIUS) 1, which has previously been used to provide AAA services, at least for dial-up and terminal server access environments. As the basis for the Diameter work, the AAA Working Group first gathered requirements for AAA services as they apply to network access from different interest groups:

- IP Routing for Wireless/Mobile Hosts WG (MOBILEIP).
- Network Access Server Requirements WG (NASREQ).
- Roaming Operations WG (ROAMOPS).
- Telecommunications Industry Association (TIA).

The final Diameter protocol is actually split into two parts: The Diameter base protocol and the Diameter applications. The base protocol is needed for delivering Diameter data units, negotiating capabilities, handling errors and providing for 1 The name is derived from geometry, as Diameter = 2 * Radius. Extensibility. A Diameter application defines application-specific functions and data units.

Each Diameter application is specified separately. In addition, the AAA transport profile includes discussions and recommendations on the use of transports by AAA protocols. Third Generation Partnership Project (3GPP) Release 5 has also been allocated a specific set of Diameter command codes. The Diameter base protocol uses both the Transmission Control Protocol and the Stream Control Transmission Protocol (SCTP) as transport. However, SCTP is the preferred choice, mostly due to the connection-oriented relationship that exists between Diameter peers. It is beneficial to be able to categorize several independent streams to a single SCTP association, instead of keeping all streams open as independent TCP connections. Both Internet Protocol Security (IPsec) and Transport Layer Security (TLS) are used or securing the connections.

2. Protocol components

Diameter is a peer-to-peer protocol, since any Diameter node can initiate a request.
Diameter has three different types of network nodes: clients, servers and agents. Clients are generally the edge devices of a network that perform access control. A Diameter agent provides either relay, proxy, redirect or translation services. A Diameter server handles the authentication, accounting and authorization requests for

a particular domain, or realm. Diameter messages are routed according to the network access identifier (NAI) of a particular user.

3. Diameter services

The Diameter base protocol provides two types of services to Diameter applications: authentication and/or authorization, and accounting. An application can make use of authentication or authorization only or it can combine the two by requesting authentication with authorization. The accounting service can be invoked irrespective of whether authentication or authorization was requested first. Each individual Diameter application defines its own authentication and authorization Command-Codes and AVPs. The accounting application described by the base protocol is shared among the applications-only the accounting AVPs are specific to an application.

- ### Authentication and authorization

Authentication and authorization services are interlinked in Diameter. An auth request is issued by the client to invoke a service and, depending on the AVPs carried in the auth request, either authentication or authorization (or both) are performed on it.
Authentication clearly either succeeds or fails, whereas the Diameter base protocol provides authorization services in either stateless or statefull mode. In statefull authorization, the server maintains a session state and the authorization session has a finite length. The authorization session can of course be terminated by the client or aborted by the server and, at the end of the authorization lifetime, it can also be re-authorized. These functions are provided by the Diameter base protocol. The two authorization modes of operation correspond to a state full authorization FSM and a stateless authorization FSM, with which all Diameter nodes that support authentication and authorization services have complied.

- ### Accounting

The Diameter base protocol provides accounting services to Diameter applications. When an accounting session is not active, there are no resources reserved for it in either the Diameter client or the Diameter server. A successful accounting request (ACR) activates an accounting session, in which the accounting records exchanged fall into two categories, based on the accounting service type:

1. Measurable length services have clearly defined beginnings and ends. An accounting record is created when the service begins and another is sent when the service ends. Optionally, interim accounting records can be produced at certain intervals within the measurable length session.
2. One-time events are services without a measurable service length. In a one-time event accounting record, the beginning of the service and the end of the service actually coincide. Therefore, a one-time event only produces a single accounting record. The accounting server or the server dictates the accounting

strategy of a session authorizing a user session: this is called the server-directed model for accounting. The accounting server directs the client to use either measurable length service accounting or one-time event accounting. It also optionally specifies the time interval to use when generating interim accounting records. The Diameter accounting protocol has built-in fault resilience to overcome small message loss and temporary network faults, as well as real-time delivery of accounting information. Accounting records are correlated with the Session-Id AVP, which is a globally unique identifier and present in all AAA messages. Alternatively, if a service consists of several different sessions each with a unique Session-Id AVP, then an Accounting-Multi-Session-Id AVP is used for correlation of accounting records [1].

2.4.2. Remote Authentication Dial-In User Service (RADIUS)

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

2.4.3. H.323

- H.323 - first call control standard for multimedia networks. Was adopted for VoIP by the ITU in 1996

- H.323 is actually a set of recommendations that define how voice, data and video are transmitted over IP-based networks.

- The H.323 recommendation is made up of multiple call control protocols. The audio streams are transacted using the RTP/RTCP.

- In general, H.323 was too broad standard without sufficient efficiency. It also does not guarantee business voice quality.

2.4.4. SIP - Session Initiation Protocol, IETF (Internet Engineering Task Force):

1. Background:

SIP is an application layer protocol that is used for establishing, modifying and terminating multimedia sessions in an IP network. It is part of the multimedia architecture whose protocols are continuously being standardized by the Internet Engineering Task Force (IETF). Its applications include, but are not limited to, voice, video, gaming, messaging, call control and presence. The idea of a session signaling protocol over IP dates back to 1992 where multicast conferencing was in mind. SIP itself originated in late 1996 as a component of the IETF Mbone (multicast backbone), an experimental multicast network on top of the public Internet. It was used by the IETF for the distribution of multimedia content, including IETF meetings, seminars and conferences. Due to its simplicity and extensibility, SIP was later adopted as a Voice Over Internet Protocol (VoIP) signaling protocol, finally becoming an lETF-proposed standard in 1999. SIP was further enhanced to take into account interoperability issues, better design and new features [1].

- SIP works in the Session layer of IETF/OSI model. SIP can establish multimedia sessions or Internet telephony calls. SIP can also invite participants to unicast or multicast sessions.
- SIP supports name mapping and redirection services. It makes it possible for users to initiate and receive communications and services from any location, and for networks to identify the users wherever they are.
- SIP – client-server protocol, Rq from clients, Rs from servers. Participants are identified by SIP URLs. Requests can be sent through any transport protocol, such as UDP, or TCP.
- SIP defines the end system to be used for the session, the communication media and media parameters, and the called party's desire to participate in the communication.
- Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

The Session Initiation Protocol is specified in IETF Request for Comments (RFC) 2543 [8].

2. Design principles

SIP, as part of the IETF process, is based on the Hyper Text Transfer Protocol (HTTP) and the Simple Network Management Protocol (SNMP). Figure 4.1 shows where SIP fits into a protocol stack.
SIP was created with the following design goals in mind:

- Transport protocol neutrality—able to run over reliable (TCP, SCTP) and unreliable (UDP) protocols.

- Request routing—direct (performance) or proxy-routed (control).
- Separation of signaling and media description—can add new applications or media.
- Extensibility.
- Personal mobility.

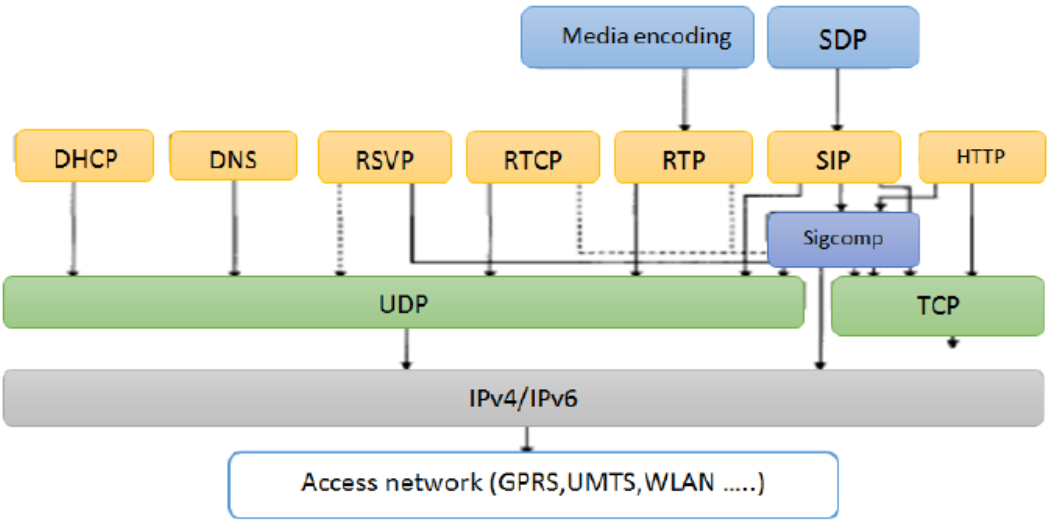


Figure 2.5: SIP fit into a protocol stack

3. SIP architecture

Elements in SIP can be classified into user agents (UAs) and intermediaries (servers). In an ideal world, communications between two ends (or UAs) happen without the need for intermediaries. However, this is not always the case as network administrators and service providers would like to keep track of traffic in their network.
Figure 4.2 depicts a typical network set-up, which is referred to as the "SIP trapezoid". A SIP UA or terminal is the end of dialogs: it sends and receives SIP requests and responses, it is the end of multimedia streams, and it is usually the user equipment (UE), which is an application in a terminal or a dedicated hardware
appliance. The UA consists of two parts:

•User Agent Client (UAC)—the caller application that initiates requests.
• User Agent Server (UAS)—accepts, redirects, rejects requests. Sends responses for incoming requests on behalf of the user. Gateways are special cases of USs.

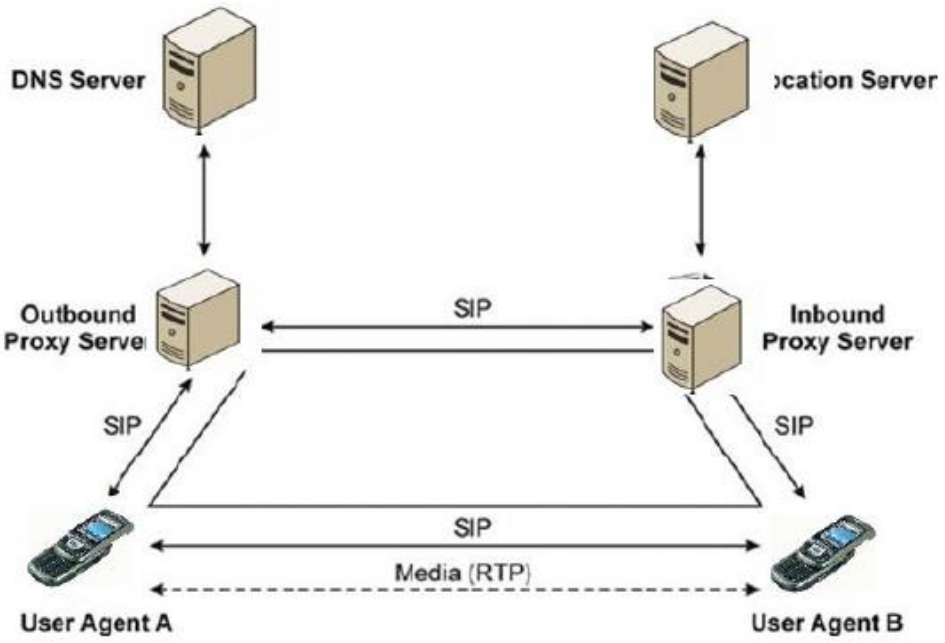


Figure 2.6: The "SIP trapezoid"

SIP intermediaries are logical entities where SIP messages pass through on their way to their final destination. These intermediaries are used to route and redirect requests. These servers include:

- Proxy server—receives and forwards SIP requests. It can interpret or rewrite certain parts of SIP messages that do not disturb the state of a request or dialog at the end points, including the body. A proxy server can also send a request to a number of locations at the same time. This entity is labelled as a forking proxy.

Forking can be parallel or sequential. There are three proxy server types:

- Dialog-state full proxy—a proxy is dialog-state full if it retains the state for a dialog from the initiating request (INVITE request) to the terminating request (BYE request).
- Transaction-state full proxy—maintains client and server transaction-state machines during the processing of a request.
- Stateless proxy—forwards every request it receives downstream and every response it receives upstream.
- Redirect servers—maps the address of requests into new addresses. It redirects requests but does not participate in the transaction.
- Location server—keeps track of the location of users.
- Registrars—a server that accepts REGISTER requests. These servers are used to store explicit binding between a user's address of record (SIP address) and the address of the host where the user is currently residing or wishing to receive requests on.

Two more elements that are used to provide services for SIP users:

- Application server—an AS is an entity in the network that provides end users with a service. Typical examples of such servers are presence and conferencing servers.

- Back-to-back-user-agent—as the name depicts, a B2BUA is where a UAS and a UAC are glued together. The UAS terminates the request as a normal UAS. The UAC initiates a new request that is somehow related to requests received at the UAS side, but not in any protocol-specific link. This entity is almost like a proxy, but it breaks all the rules that govern the way a proxy can modify a request.

2.4.5. SDP (Session Description Protocol)

The Session Description Protocol (SDP) is an application-layer protocol intended to describe multimedia sessions. It is a text-based protocol. When describing a session, the caller and callee indicate their respective "receive" capabilities, media formats and receive address/port.
Capability exchange can be performed during session set-up or during the session itself (while the session is in progress).
At the time of writing, a new SDP specification is in the process of being finalized.

SDP message contents

An SDP message contains three levels of information:

1. Session-level description—this includes the session identifier and other session level parameters, such as the IP address, subject, contact info about the session and/or creator.
2. Timing description—start and stop times, repeat times, one or more media-level descriptions.
3. Media type and format—transport protocol and port number, other media-level parameters. Note that the media address may be different from the signaling address.

2.4.6. RTP (Real-time Transport Protocol)

The Real-time Transport Protocol (RTP) as a protocol for end-to end delivery for real-time data. It also contains end-to-end delivery services for real-time data: payload-type (codec) identification, sequence numbering, time stamping and delivery monitoring. RTP does not provide quality of service (QoS); it does, however provide QoS monitoring using the RTP Control Protocol (RTCP). RTCP also conveys information about media session participants.

2.4.7. RTCP (RTP Control Protocol)

RTP Control Protocol (RTCP) packets are transmitted periodically to all participants in a session. There are four RTCP functions:

- To provide feedback on the QoS of real-time data distribution.
- To carry a persistent identifier of the RTP source (called a CNAME).
- To permit an adjustable RTCP packet distribution interval (the report interval).
- To convey session control information.

1. RTCP packet types

There are five types of RTCP packets:

- SR—a sender report, providing transmission and reception statistics, sent by active media senders.
- RR—a receiver report, providing reception statistics, sent by non-active senders.
- SDES—source description items, such as CNAME.
- BYE—indicates end of participation.
- APP—application-specific functions (defined by a profile).

2. RTCP report transmission interval

Every participant is required to send RTCP packets. If there are many participants (say, a conference), then there is a scalability problem as further users join in. To control the scalability problem, the rate at which RTCP packets are sent must be scaled down by dynamically calculating the interval between RTCP packet transmissions.
A certain percentage of session bandwidth should be dedicated to RTCP; this percentage and the interval between report transmissions are profile-defined.
Timestamp is used to allow the receiver to play packets at the right time and, therefore, minimize distortion.

3. RTP profile and payload format specifications

When conventional protocols are designed, they are generalized to accommodate the additional functionality of their applications. For RTP, this is achieved through modifications and additions to the existing headers as needed by an application. Therefore, RTP for a particular application, like audio, requires 1 or more companion documents: namely, a profile specification document and a payload format specification document.

4. RTP profile and payload format specification for audio and video (RTP/AVP)

An application using RTP must specify a profile and the payload formats used for it. In this section the profile and payload formats for audio and video applications are identified.

2.4.8.Transport layer security (TLS)

1. TLS Introduction

TLS provides transport layer security for Internet applications. It provides for confidentiality and data integrity over a connection between two end points. TLS operates on a reliable transport, such as TCP, and is itself layered into the TLS Record Protocol, and the TLS Handshake Protocol. One advantage of TLS is that applications can use it transparently to securely communicate with each other. Another is that TLS is visible to applications, making them aware of the cipher suites and authentication certificates negotiated during the set-up phases of a TLS session; whereas, with the Internet Protocol Security (IPsec), security policies are usually not visible to each application individually, which makes it difficult to assess whether there is adequate security in place. TLS allows for a variety of cipher suites to be negotiated, for the use of compression and for a TLS session to span multiple connections. This reduces the overhead of having to perform an expensive TLS handshake for each new parallel connection between the applications. It is also possible to resume a session: this means that the client and server can agree to use a previously negotiated session- if one exists in their session cache-instead of performing the full TLS handshake [1].

2.4.9. Common Open Policy Service (COPS)

1 Introduction

The COPS protocol is an Internet Engineering Task Force (IETF) protocol used for the general administration, configuration and enforcement of policies. It defines a simple query and response protocol for exchanging policy information between a policy server and its clients. The clients are denoted as policy enforcement points (PEPs) and the server as a policy decision point (PDP), respectively. The protocol employs a client/server model in which a PEP sends requests, updates and deletes to the PDP, which in turn returns policy decisions back to the PEP. A special type of PDP is the local policy decision point (LPDP), which is used by PEPs to request local policy decisions when there is no available PDP to communicate with. Figure illustrates the model.

There are two main models for COPS policy control:

- Outsourcing-the PEP assigns (outsources) responsibility of authorizing certain events at the PEP to an external entity (PDP). This model assumes a one-to-one correlation between events at a PEP and decisions from a PDP.

- Configuration-unlike the previous model, there exists no direct mapping between events at the PEP and decisions from the PDP.

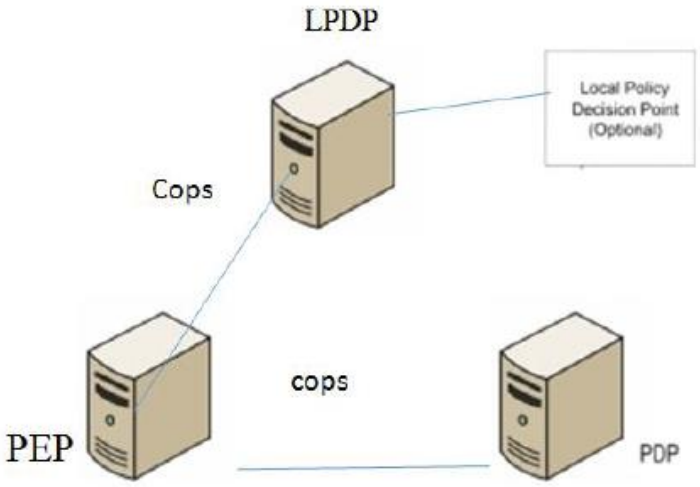


Figure 2.7: A special type of PDP is the local policy decision point (LPDP)

Originating at the PEP. This may be performed by the PDP in bulk or in portions, but the overall timing is more flexible than the outsourcing model's. The COPS protocol uses persistent Transmission Control Protocol (TCP) connections between the PEPs and the PDP for reliable transport of protocol messages. The COPS protocol is statefull since the request/decision state is shared between the client and the server. Also, unlike many other client/server protocols, the state of a given request/decision pair can be associated with another request/decision pair. The server is also able to push state to the client and remove it once it is no longer valid. COPS has a built-in extensibility: policy objects are self-identifying and support vendor-specific objects. Extensions may describe the message formats and objects that carry the policy data without requiring any changes to the protocol itself.

2.4.10. Signaling Compression

Signaling compression (SigComp) is a mechanism that application protocols use to compress messages before sending to the network. It is presented to applications as a layer between application protocols and transport protocols. SigComp uses a universal decompressor virtual machine (UDVM) to decompress messages. A message that is compressed using SigComp is referred to as a SigComp message.

1. SigComp architecture

SigComp's architecture can be broken down into five entities (see Figure 4.17). The entities are described as follows:

- Compressor dispatcher-this is the interface between the application and the SigComp system. It invokes a compressor, indicated by the application using a compartment identifier. The compressor dispatcher forwards the returned compressed message to its destination.
- Decompressor dispatcher-this is the interface between the SigComp system and the application. It invokes a UDVM that decompresses the message. The decompressor dispatcher then passes the decompressed message to the application. If the application wishes the decompressor to retain the state of the message, it returns what is called a compartment identifier.
- Compressors-this entity compresses the application message. It uses a compartment that is identified using the compartment identifier. The compressed message is passed to the compressor dispatcher. DEFLATE is an example of a compression algorithm.

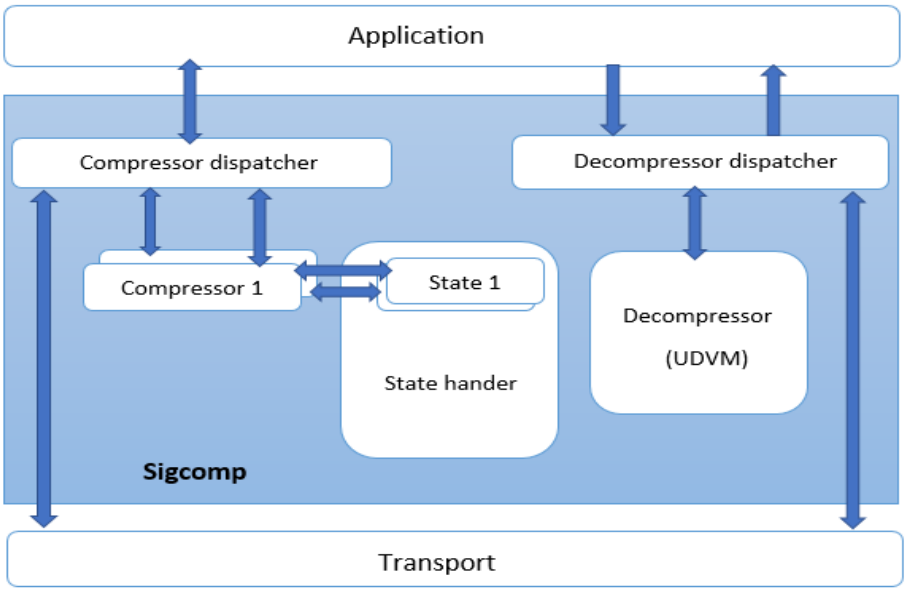


Figure 2.8: SigComp's architecture

- UDVM-this entity decompresses a compressed message. A new instance is invoked for every new SigComp message. UDVM uses the state handler to create a state for a new message or make use of an existing state.
- State handler-this holds information that is stored between SigComp messages (referred to as the state of the messages). It can store and recover the state.

2.4.11. DHCPv6 (Dynamic Host Configuration Protocol for Internet Protocol Version 6)

- The Dynamic Host Configuration Protocol for Internet Protocol Version 6 (DHCPv6), as defined in, is a client-server protocol that allows devices to be configured with management configuration information. DHCP specifically provides clients with dynamically assigned IP addresses using a DHCP server.

It also provides other configuration information carried as options: options are extensions to DHCP. "Extending DHCP" means defining a new option.

- DHCP messages are exchanged between clients and servers using User Datagram Protocol (UDP) as the transport protocol. Clients listen on port 546 for messages, while servers listen on port 547. A client uses a link-local address for transmitting and receiving DHCP messages. A client sends DHCP messages to servers using the link-scoped multicast address "FF02::1:2", also known as All_DHCP_Relay_Agents_and_Servers. DHCP relay agents on the client's link allow a DHCP client to send a message to a DHCP server that is not attached to the same link.
- A client needs, first, to locate a DHCP server before requesting an IP address and other configuration information. It does so by sending a DHCP solicit message to the multicast address identified earlier. A server willing to answer the request answers with a DHCP advertise message. The client then chooses one of the servers and a DHCP request message. The server responds with a relay message confirming the assigned IP addresses and other configuration information. Because assigned IP addresses expire, the client needs to send a DHCP renew message to the server in order to extend the assigned IP address lifetime [1].

2.4.12. Extensible Markup Language Configuration Access Protocol (XCAP)

In many services today the service provider needs-in order to carry out a request-to have access to information that can only be set by users. Such services include presence, messaging and conferencing. In XCAP a user is able to upload information to an XCAP server, which provides this uploaded information to application servers that use this information to satisfy a request demanded by the user. With XCAP, the user is also allowed to manipulate, add and delete such data. An example of the data that a user can upload is the user's resource list for presence. XCAP uses the Hyper Text Transfer Protocol (HTTP) to upload and read the information set by users and the Information is represented using XML (Extensible Markup Language).

- XCAP application usage

Applications, like presence, need to define an XCAP application usage, which defines the way that a unique application can make use of XCAP. It defines the XML document for the application, along with the following:

- Application usage ID (AUID)-this ID uniquely identifies an application usage.
- Additional constraints-these cover data constraints that are not possible to represent using an XML schema.
- Data semantics-the semantics for each element and attribute in an application usage XML document.

- Naming convention-defines how an application constructs the URI (uniform resource identifier) representing the document that is to be read or written by the application so that it can carry out its tasks.

2.4.13. CPCP (Conference Policy Control Protocol)

The Conference Policy Control Protocol (CPCP) is a client-server protocol that can be used by users to manipulate the rules associated with the conference. These rules include directives on the lifespan of the conference, who can and cannot join the conference, definitions of roles available in the conference and the responsibilities associated with those roles, and policies on who is allowed to request which roles. The conference policy is represented by a URI (uniform resource identifier). There is a unique conference policy URI for each conference, which points to a conference policy server where a user can manipulate that conference policy. Note that CPCP is not the only mechanism to manipulate conference policy—other mechanisms exist as well, such as the Web interface. CPCP allows clients to manipulate the conference policy at the conference policy server (CPS), which is able to inform the focus about changes in conference policy, if necessary: for example, if new users are added to the dial-out list, then the conference policy server informs the focus, which makes the invitations as requested. CPCP can specifically be used to create conferences, terminate conferences, define start and stop times, define the dial-out and dial-in lists, bring about conference security and give out general conference information. A conference policy also includes the conference media policy and floor control.
CPCP allows the creator of a conference to:

- determine the lifespan of the conference;
- decide who can and who cannot join the conference;
- define the dial-out and dial-in lists;
- define the roles available in the conference and the responsibilities associated with those roles;
- give out general conference information;
- set up media policy;
- set up conference security [1].

Media Gateway Control Protocol(MGCP) /Megaco/H.248 .2.4.13 .2.4.14

- MGCP - Media Gateway Control Protocol , IETF.
- MGCP – control protocol that specifically addresses the control of media gateways
- Megaco/H.248 (IETF, ITU) - standard that combines elements of the MGCP and the H.323, ITU (H.248).

- The main features of Megaco - scaling (H.323) and multimedia conferencing (MGCP)

2.4.15. SIGTRAN (Signaling Transport)

- SIGTRAN (for Signaling Transport) is the standard Telephony Protocol used to transport Signaling System 7 signals over the Internet. SS7 signals consist of special commands for handling a telephone call.
- Internet telephony uses the IP PS connections to exchange voice, fax, and other forms of information that have traditionally been carried over the dedicated CS connections of the public switched telephone network (PSTN). Calls transmitted over the Internet travel as packets of data on shared lines, avoiding the tolls of PSTN.
- A telephone company switch transmits SS7 signals to a SG. The gateway, in turn, converts the signals into SIGTRAN packets for transmission over IP to either the next signaling gateway.
- The SIGTRAN protocol is actually made up of several components (this is what is sometimes referred to as a protocol stack):

    - standard IP common signaling transport protocol (used to ensure that the data required for signaling is delivered properly), such as the Streaming Control Transport Protocol (SCTP) adaptation protocol that supports "primitives" that are required by another protocol.
    - The IETF Signaling Transport working group has developed SIGTRAN to address the transport of packet-based PSTN signaling over IP Networks, taking into account functional and performance requirements of the PSTN signaling. For interworking with PSTN, IP networks will need to transport signaling such as Q.931 or SS7 ISUP messages between IP nodes such as a Signaling Gateway and Media Gateway Controller or Media Gateway. Applications of SIGTRAN include Internet dial-up remote access and IP telephony interworking with PSTN.

2.4.16.Stream Control Transmission Protocol (SCTP)

- TCP transmits data in a single stream (sometimes called a byte stream) and guarantees that data will be delivered in sequence to the application or user at the end point. If there is data loss, or a sequencing error, delivery must be delayed until lost data is retransmitted or an out-of-sequence message is received. SCTP's multi-streaming allows data to be delivered in multiple, independent streams, so that if there is data loss in one stream, delivery will not be affected for the other streams. For some transmissions, such as a file or record, sequence preservation is essential. However, for some applications, it is not absolutely necessary to preserve the precise sequence of data. For example, in signaling transmissions, sequence preservation is only necessary for

messages that affect the same resource (such as the same channel or call). Because multi-streaming allows data in error-free streams to continue delivery when one stream has an error, the entire transmission is not delayed [8].

Chapter 3

3.1 Services of IMS

3.2 Application of IMS

3.1 Services of IMS

3.1.1 Presence

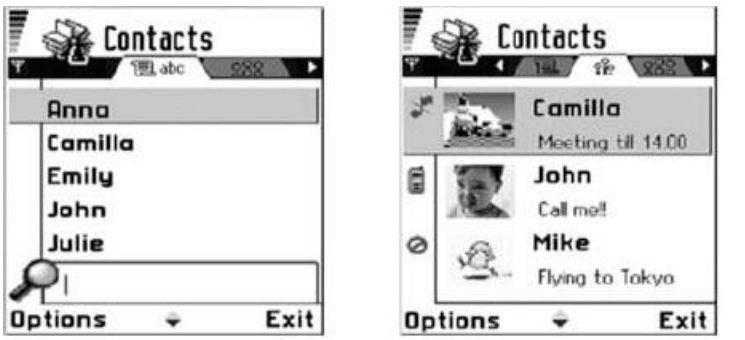
With an ever increasing penetration of Internet Protocol (IP) technologies, the wireless industry is evolving the mobile core network towards all-IP network. The IP Multimedia Subsystem (IMS) is a standardized Next Generation Network (NGN) architectural framework defined by the 3rd Generation Partnership Project (3GPP) to bridge the gap between circuit-switched and packet-switched networks and consolidate both sides into on single all-IP network for all services. In this section, we provide an insight into the limitation of the presence service, one of the fundamental building blocks of the IMS.

The IMS presence service:

Presence is in essence two things: it involves making my status available to others and the statuses of others available to me. Presence information may include:

- Person and terminal availability
- Communication preferences;
- Terminal capabilities;
- Current activity;
- Location.

It is envisioned that presence will facilitate all mobile communication, not only instant messaging, which has been the main driver for presence. Instant messaging has been the main interactive, almost real time communication service in the Internet and presence is a great compliment in that you know if a friend is online before you begin a chat session with her. However, in the mobile environment, it is envisioned that presence information will not only support instant messaging, it will also be used as an indicator of the ability to engage in any session, including voice calls, video and gaming: all mobile communications will be presence- based. Presence-specific and presence-enhanced applications and services will be available in the near future. A typical example of a presence-specific application will be a phonebook with embedded presence information, making it dynamic. Dynamic presence (Figure 5.1) will be the initial information the user sees before establishing communication. This information affects the choice of communication method and timing [1].



Contacts Today Presence Enhanced Contacts

Figure 3.1: Dynamic presence

3.1.2 Messaging

There are currently many forms of messaging services available. In general, messaging entails sending a message from one entity to another. Messages can take many forms, include many types of data and be delivered in various ways. It is usual to have messages carry multimedia as well as text and be delivered either in near-real time as in many instant messaging systems or into a mailbox as in email today. In this section we give some details about messaging in the Internet Protocol Multimedia Subsystem (IMS) context.

1. Overview of IMS messaging

IMS messaging takes three forms:

- Immediate messaging;
- Session-based messaging;
- Deferred delivery messaging.

Each form of IMS messaging has its own characteristics; so, even though messaging in its simplest form can be thought of as a single service—after all, all forms of messaging are really about sending a message from *A* to *B*—the fact that these characteristics differ makes them each a service on their own. However, the way in which applications are built on top of these services may well hide the fact that these are different forms of messaging. In fact, one of the key requirements for IMS messaging is easy interworking between different messaging types.

5.1.3 Conferencing

A conference is a conversation between multiple participants. There are many different types of conferences, including loosely coupled conferences, fully distributed multiparty conferences, tightly coupled conferences. In this chapter only the latter is described since it is the only one that is of interest to the Internet Protocol Multimedia Subsystem (IMS). Conferencing is not just limited to audio; the popularity of video and

text conferencing, better known as chatting, has been growing rapidly over the past few years. This popularity is due to conferencing's ability to simulate a face-to face meeting in so many realistic ways: for example, by enabling file and whiteboard sharing and conveying emotions using video, all in real time.

3.2 Applications of IMS

This chapter shows IP Multimedia Subsystem emerging applications in the field of Telecommunication and Information Technology. We have examined the standard architecture of IMS based on the Third Generation Partnership Project (3GPP) and the basic operation which is being modified for different solutions by different vendors.

The goal is to examine the applications of IMS along with the capabilities and/or benefits IMS brings to the mobile network operators and end users in terms of new services and the overall experience.

3.2.1 IPTV

IPTV is defined as multimedia services such as television, video, audio, text, graphics, data delivered over IP based networks managed to provide the required level of quality of service and experience, security, interactivity and reliability.

With the Nortel IPTV solution for example, telephony meets television, which meets mobility providing the very most advanced features of both technologies, synergized to allow for uninterrupted downtime while fully in touch with the outside world. IPTV allows users to relax on the sofa while onscreen before them is access to instant messaging, caller ID and the ability to accept, reject, initiate or even redirect incoming calls to another number or even to voicemail. This solution applies to video for all access technologies, whether mobile television, cable or IP. A recent survey of end users by Nortel indicates that approximately 30 percent have expressed interest in subscribing to interactive services such as these.

1. IPTV Benefits

- Operates with various levels of communications management and types of phones.
- Enhances the end-user experience and helps afford uninterrupted television viewing by enabling the user to check the caller ID without leaving the couch and then presenting them with the option to answer or ignore the call or redirect it to voicemail.
- Links with other IMS capabilities, such as click-to-call, instant messaging, video on demand and buddy lists.

Before IMS we had Proprietary interfaces and Separate subscriber databases, authentications, etc. but now with IMS, proprietary interfaces are replaced with open standards with an integrated single sign-on for telephony, multimedia, TV, video while a single authentication, QoS, security solution are required for telephony, multimedia and IPTV.

The IPTV solution allows subscribers to stay in touch with friends and family while watching their favorite television shows, to identify who is calling and receive or route calls as they wish. They can go to a voice call with the click-to-call feature or immediately initiate an instant message. Consumers can also receive video photos from a caller on their screens as shown in figure 5.14.

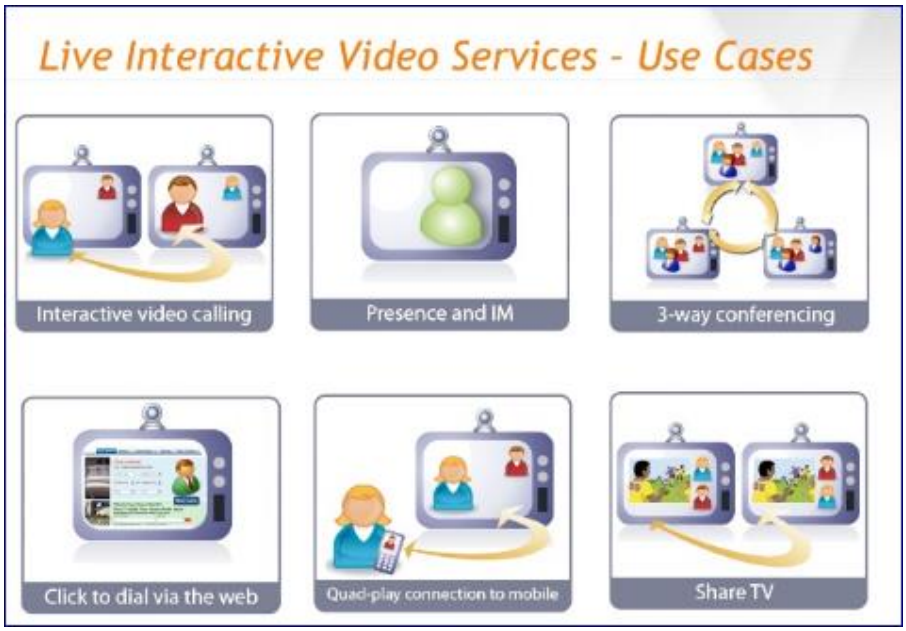


Figure 3.2: Consumers receive video photos from a caller on their screens

3.2.2 Converged Mobility

IMS Converged Mobility untethers communications from physical boundaries, freeing users to roam, seamlessly, with unbroken service. By integrating traditional wireless technologies with new wireless technologies, it seamlessly improves and provides coverage in areas where cellular coverage is poor, while maintaining features across cellular and WLAN — for example, voice features, SMS and instant messaging. Most fundamentally and notably, Nortel Converged Mobility for example allows subscribers to use a single device, a common dial-pad and a common address book in cellular, office WLAN or home WLAN environments.

1. Converged Mobility benefits:

● Improves in-building coverage and increases reachability.

Before IMS, there was no multimedia integration in mobility; but now with IMS, multimedia is integrated which addresses multiple market segments with a single solution. Converged Mobility allows subscribers to be truly mobile and to communicate freely without having to be concerned with specific access types. Communications conform to customers' lifestyles and follow them intelligently as they move. This is shown in the figure 3.3:

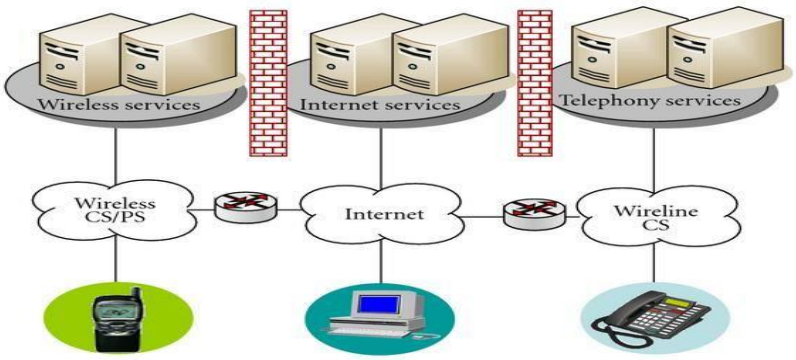


Figure 3.3: Communications conform to customers' lifestyles and follow them intelligently .

2. Identity Management in a Fixed Mobile convergent IMS environment

Today, there are still different technologies used in fixed and mobile networks environment such as cellular technologies (GSM, UMTS, 3G, etc.), wireless network technology like WLAN, wired network technology like ADSL, etc. With the usage of IMS (IP Multimedia Subsystem), all those technologies can be combined together in a fixed mobile convergence environment based on an IP-based infrastructure. Although IMS applies well for a Fixed Mobile convergent environment, there are still issues that need to be solved. First, the IMS central protocol is SIP but there are differences between the 3GPP SIP specifications and the IETF one. This will lead to interoperability problem with different SIP specifications, and the devices between different SIP environments cannot communicate with each other. Second, IMS for a fixed mobile environment should also allow the users to subscribe to any type of services (fixed or mobile), to get access to services on an arbitrary number of registered mobile and fixed devices interchangeably, to dynamically add or remove the number of registered fixed devices. In fact, the general IMS infrastructure is only a high-level scheme and does not support the mentioned requirements.

Therefore, in order to satisfy all the mentioned requirements, it is crucial to have a sound identity management solution. The goal of this thesis work is to propose a sound identity management solution for a fixed mobile convergent IMS environment.

More specifically, the thesis work will be aiming at the following objectives:To provide a concise but clear introduction to Identity Management to provide a comprehensive description on how identities are organized and managed in both fixed and mobile networks To propose an identity management solution for a fixed mobile convergent IMS environment to demonstrate the soundness and feasibility of the proposed solution via the implementation of a prototype. Two Identity Management solutions have been proposed and analyzed as follows:

1. Modified IMS and SSO-enabled SIP system

2. Modified SIP-enabled Client Due to time limitation, only the second solution is selected and a proof-of concept has been successfully designed and implemented. The proof-of-concept has demonstrated the following features: Single-Sign-On between the Mobile and Fixed domain enabling a mobile phone moving from the IMS mobile network to a SIP WLAN network without re-authentication. Identity Federation between the Mobile and Fixed domain enabling the delivery of calls addressed to one domain at the other domain.

3.2.3 Push to Talk

IMS Push to Talk (PTT) is a standards-based, end-to-end solution that offers mobile, half- Duplex voice communication services that combine 'always-on' capabilities with ease-of-use. PTT is a forerunner to peer-to-peer services over IP, for which IMS provides the capabilities and foundation. PoC is the first commercial application based on IMS.

Push-to-Talk is all about ease of use and ease of access, allowing customers to use a single Button to alert a friend or colleague that they'd like to talk, and to then have a conversation without having to dial their phone. It's a personalized "walkie-talkie" experience- personalized in that the Push-to-Talk solution is integrated with other elements of the IMS infrastructure, such as buddy lists and presence features.
An expansion of the Push-To-Talk service is Push to see and eventually push to X (anything) involving content-sharing, location-based services and IMS applications across a number of different devices truly enabling enhanced real-time communications.

1. Push to Talk benefits:

- Increases Average Revenue Per User.
- Enhances end-user convenience with a "walkie-talkie" experience, with the party being Dialed just a single button push away

3.2.4 Voice over IP

Voice over Internet Protocol (VoIP) is a form of transmission that allows any person to make phone calls over a broadband internet connection. VoIP access usually allows the user to call others who are also receiving calls over the internet. Interconnected VoIP connections also allow users to make and receive calls to and from conventional landline numbers, usually for a service charge. A type of adapter is used in some VoIP services which require a computer and a dedicated VoIP telephone. VoIP can also be described as a distinct solution which enables the transmission of voice signals over internet connection rather than the traditional telephone.
In today's VoIP implementations, the voice analog signals are sampled and encoded using codec then encapsulated into an IP packet and carried over data cables or the internet infrastructure in the same way that data packets are carried.

Earlier, VoIP required a headset to be plugged into the computer, and the speaker and receiver could only speak with others who had a similar set up. They had to inform each other ahead of time, in order to signal the user at the other end of the incoming call and the time of call.
In November 1977, the Internet Engineering Task Force published the Specifications for the NVP (network voice protocol). In the abstract to this document, the purpose of the research was elucidated. the development and the demonstration of the feasibility of secure and high-quality as well as low-bandwidth, real-time, full-duplex digital voice-to-voice communications over packet-switched data communications networks.
In the mid-90s, IP networks were growing, the technology had advanced and there has been an extensive use of Personal Computers. The belief that VoIP could make some significant impact on the market resulted in high expectations which resulted in the distribution of the first software package.
In its early stages, the VoIP technology was not fully developed and there were many loopholes. There was a big gap between the marketing structure and the technological reality. This can be concluded that technical shortages stopped any major development or changes in VoIP.
However, lately VoIP has continued to make technological and viable progress. Signaling protocols are used to set up and tear down calls, carry data required to locate users and negotiate capabilities.
One key advantage of VoIP includes making long distance calls at very cheap prices which include calls to other countries with the flexibility of using the same number in different parts of the world.

1. Implementation of VOIP

- Protocols

There are three protocols widely used in the implementation of VoIP

a) H.323 Family of protocols

H.323 protocol is recommended by (ITU) International Telecommunication Union and consists of family of protocols used for setting up calls, terminating calls, registering the calls, authenticating and other functions as shown in figure 3.4. These protocols that belong to the H.323 family are transported over TCP or UDP connections. H.323 family of protocol includes H.225 used for registration of calls, admission, and call signaling. H.245 is used to establish and control the media sessions and T.120 is used for conferencing applications in which a mutual whiteboard application is used. The G.7xx series defines audio codec used by H.323, and the H.26x series defines the video codec. H.323 uses RTP for media transport and RTCP for control of the RTP sessions

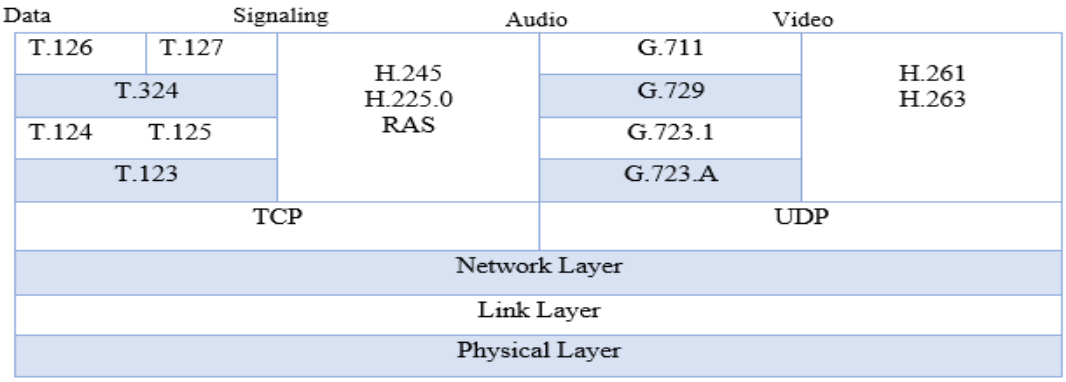


Figure 3.4: H.323 Family Protocol Stack

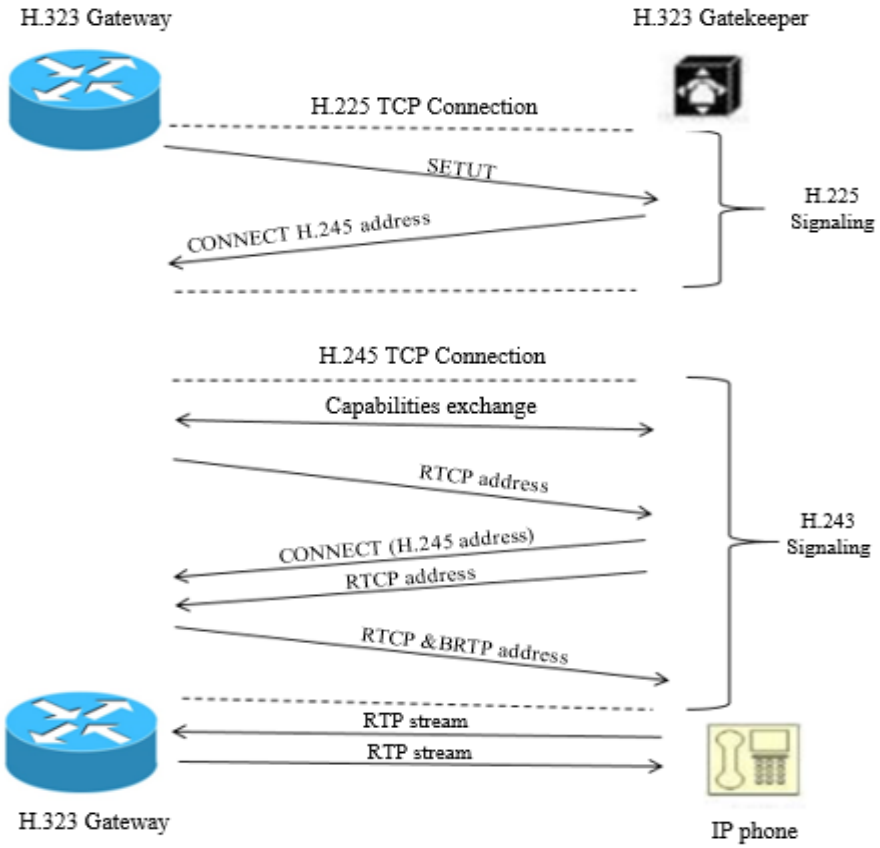


Figure 3. 5: Call flow of H.323

b. Session Initiation Protocol (SIP)

SIP, Session Initiation Protocol is a protocol developed by IETE (Institute of Electronics and Telecommunication Engineering) and is the proposed standard for initiating a user session, modifying and terminating an interactive user session that involves video, voice, instant messaging, online games and other multimedia elements. SIP can establish interactive sessions for audio/video conferencing and interactive

gaming deployed over IP networks. These enabling service providers integrate the basic IP telephone services with Web and chat services.
SIP makes communication possible through two protocols RTP/RTCP used to transport voice data in real time and SDP is used to negotiate participant capabilities, codification type, etc. SIP offers an alternative to the complex H.323 protocols. Due to its simpler nature, SIP has become more popular than the H.323 family of protocols.

c. Media Gateway Control Protocols (MGCP)

MGCP, Media Gateway Control Protocol is used to communicate between the separate components of a decomposed VoIP gateway. It is a complementary protocol to SIP and H.323. Within MGCP the MGC server or more commonly known as "call agent" is mandatory as MGC manages calls and conferences, and supports the services provided. The MG (Media Gateway) endpoint is ignorant of the calls/conferences and does not maintain call states. MGs execute commands that are sent by the call agents. MGCP assumes that call agents synchronize with each other sending coherent commands to MGs under their control. MGCP does not have any mechanism for synchronizing call agents. MG is the slave and MGC acts as the master so MGCP is a master/slave protocol

2. Data Processing in VoIP System

At the sender side, analog voice signals are converted into digital signals, compressed and then set into a prearranged format using voice codec such as G.711, G.729, and G.723 etc. Next the encoded voice is broken down into equal size packets. Furthermore, in each packet, headers from different layers are attached to the encoded voice. The protocol headers added to voice packets are of RTP, UDP, and IP as well as Data Link Layer header.
The packets are then sent over the network (IP) to its destination where the decoding and de-packetizing of the received packets is carried out. During the transmission process, jitter (time variation of packet delivery) may occur. Hence, a playout buffer is used that smoothens the playout at the receiver end which may have a delay caused due to jitter. Packets are queued at the playout buffer for a stipulated time before being played. However, packets that arrive later than the playout time are discarded. VoIP uses the signaling protocols namely Session Initiation Protocol (SIP) and H.323. These signaling protocols are required to establish VoIP calls and to close the media streams between the clients.

3. Quality of Service (QoS) in VoIP

(QoS) is defined as the network's ability to provide good services that satisfy its customers. QoS in VoIP are briefly described in following sections.

1. Delay

Delay can be defined as the total time it takes between a speaker speaking a word from one end and the receiver hearing it in the other line of communication. Delay can be

categorized into: source delay, receiver delay, and network delay. ITU-T suggests that one-way latency should not be more than 150 ms.

2. Jitter

IP network does not give guarantee of packet's delivery time, which may give rise to transmission delay. This variation is known as jitter and it has negative effects on voice quality. Jitter may lead to the loss of voice packets.

3. Packet Loss

Packets transmitted over IP network may be lost in the network or may arrive corrupted or late. Packets are discarded, if they arrive late at the jitter buffer of the receiver Packets may also be discarded in case the jitter buffer or router buffer is full. Therefore, packet loss is the loss which occurs due to network congestion in the network and/or late arrival. G.729 codec a common codec used by VoIP requires a packet loss of less than 1 percent to avoid any audible error.

4. Echo

In VoIP, Echo occurs when caller at the sender side hears a reflection of his voice after he talks at the mouth-piece of the phone (may be a microphone) whereas the callee does not notice the echo. Echo could be electrical echo which exists in PSTN networks or acoustic echo which is an issue in VoIP networks.

5. Throughput

This parameter concerns about the maximum bits received out of the total bits sent during an interval of time. Throughput in VoIP will depend on number of concurrent users and the codec used. Usually voice packets are given higher priority so the throughput of voice packets over data packets in a channel is higher.

- CONFIGURATION OF VOIP

1. Adapters (USB)

VoIP phone adapters allow us to use any traditional telephone to place VoIP calls. They usually look like USB adapters. These USB adapters have a typical modular telephone phone port to which one can connect a regular phone line. Once attached, your phone operates as if connected to normal phone service.

2. Software controlled VoIP applications: softphones

Softphones are phones that allow us to make VoIP phone calls directly from a computer that has an internet connection. Softphones make call with the help of a PC headset and a sound card. A softphone is just like a normal phone just with the difference that the connection is coming from your PC. VoIP providers give away softphones for free in

exchange of availing their service. Software controlled VoIP application allows users to talk to other people using these services at no extra cost.

3. Dedicated VoIP phones

A VoIP phone seems like a regular telephone (can be cordless as well). A dedicated VoIP phone connects directly to a computer network rather than a conventional telephone line. A dedicated VoIP phone may work in two ways 1) a phone and base station that connects to the internet 2) it may function on a local wireless network. Dedicated VoIP phones require a provider as well as a service plan.

4. Dedicated routers

These routers in VoIP allow user to connect conventional phones to the internet to place VoIP calls where the router is connected to an ADSL/Cable modem and allow users to attach a traditional telephone. VoIP routers have the additional functionality of an IP router as which allows us to connect to the PC as well. VoIP providers configure these routers under a specific plan for a service fee. These routers can also perform their functions independent of any computer or any software [4].

Chapter 4
Long-Term Evolution
(LTE Technology)
And VOLTE

4

4.1 LTE Technology

Long-Term Evolution (LTE) is a standard for high-speed wireless communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface together with core network improvements.

The term LTE is actually a project name of the Third Generation Partnership Project (3GPP). The goal of the project, which started in November 2004, was to determine the long-term evolution of 3GPP's Universal Mobile Telephone System (UMTS). UMTS was also a 3GPP project that studied several candidate technologies before choosing Wideband Code Division Multiple Access (W-CDMA) for the Radio Access Network (RAN). The terms UMTS and W-CDMA are now interchangeable; although that was not the case, before the technology was selected.

Because LTE is the evolution of UMTS, LTE's equivalent components are thus named Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN). These are the formal terms used to describe the RAN. The system, however, is more than just the RAN Since there is also a parallel 3GPP project called System Architecture Evolution (SAE), which is defining a new all-IP packet-only Core Network (CN) known as the Evolved Packet Core (EPC). The combination of the EPC and the evolved RAN (E-UTRA plus E-UTRAN) is the Evolved Packet system (EPS). Depending on the context, any of the terms LTE, E-UTRA, E-UTRAN, SAE, EPC and EPS may get used to describe some or all of the System. Although EPS is the only correct term for the overall system, the name of the system will often be written as LTE/SAE or even simply LTE [9].

4.1.1 LTE architecture:

The general LTE / EPC architecture is defined from a physical and a functional point of view. From a physical point of view, the LTE / EPC architecture is composed of the following domains:

- The EU
- The access network, called LTE or E-UTRAN (Evolved-UTRAN);
- The core network, called EPC.

The general LTE / EPC architecture is shown in the following figure.

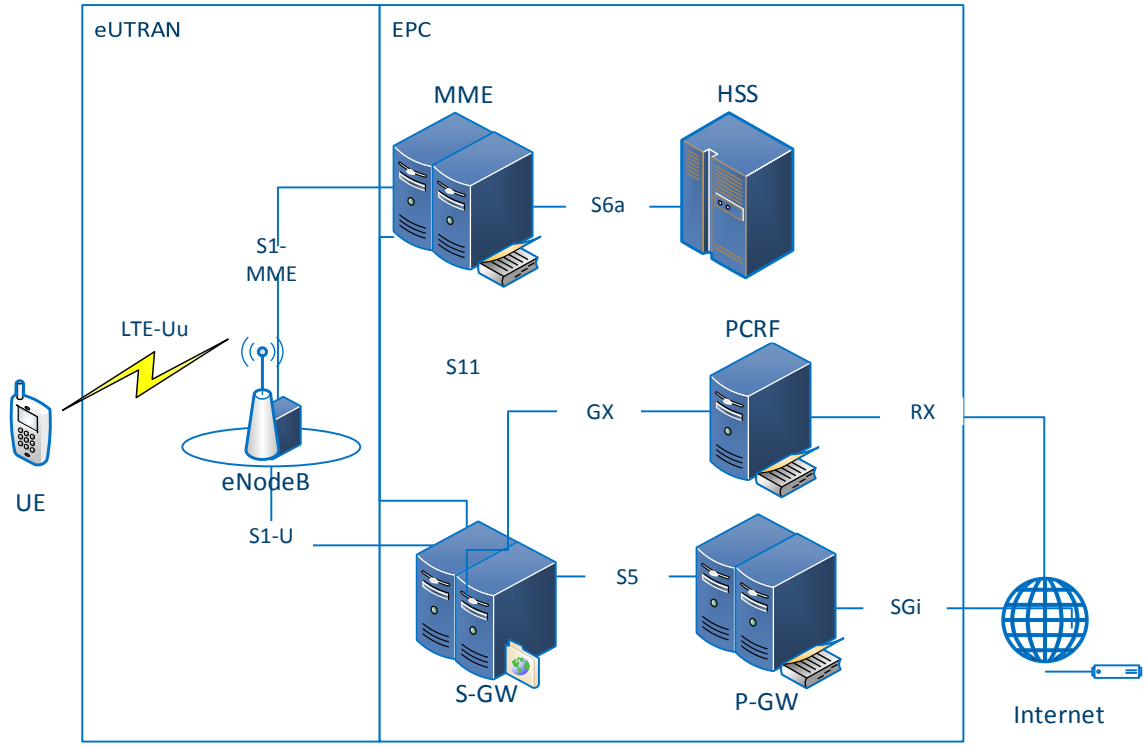


Figure 4.1: LTE Architecture.

1) The core network

The core network (called EPC) is responsible for the overall control of the UE and establishment of the bearers. The main logical nodes of the EPC are:

- PDN Gateway (P-GW)
- Serving Gateway (S-GW)
- Mobility Management Entity (MME)

In addition to these nodes, EPC also includes other logical nodes and functions such as the Home Subscriber Server (HSS) and the Policy Control and Charging Rules Function (PCRF). Since the EPS only provides a bearer path of a certain QoS, control of multimedia applications such as VoIP is provided by the IP Multimedia Subsystem (IMS), which is considered to be outside the EPS itself.

The logical CN nodes are discussed in more detail below:

- PCRF

The Policy Control and Charging Rules Function is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF), which resides in the P-GW. The PCRF provides the QoS authorization (QoS class identifier [QCI] and bit rates) that

decides how a certain data flow will be treated in the PCEF and ensures that this is in accordance with the user's subscription profile.

- HSS

The Home Subscriber Server contains users' SAE subscription data such as the EPS-subscribed QoS profile and any access restrictions for roaming. It also holds information about the PDNs to which the user can connect. This could be in the form of an access point name (APN) (which is a label according to DNS naming conventions describing the access point to the PDN) or a PDN address (indicating subscribed IP address (es)). In addition, the HSS holds dynamic information such as the identity of the MME to which the user is currently attached or registered. The HSS may also integrate the authentication center (AUC), which generates the vectors for authentication and security keys [9,10] .

- P-GW

The PDN Gateway is responsible for IP address allocation for the UE, as well as QoS enforcement and flow-based charging according to rules from the PCRF. It is responsible for the filtering of downlink user IP packets into the different QoS-based bearers. This is performed based on Traffic Flow Templates (TFTs). The P-GW performs QoS enforcement for guaranteed bit rate (GBR) bearers. It also serves as the mobility anchor for interworking with non-3GPP technologies such as CDMA2000 and WiMAX networks [9,10].

- **S-GW**

All user IP packets are transferred through the Serving Gateway, which serves as the local mobility anchor for the data bearers when the UE moves between eNodeBs. It also retains the information about the bearers when the UE is in the idle state (known as "EPS Connection Management — IDLE" [ECM-IDLE]) and temporarily buffers downlink data while the MME initiates paging of the UE to reestablish the bearers. In addition, the S-GW performs some administrative functions in the visited network such as collecting information for charging (for example, the volume of data sent to or received from the user) and lawful interception. It also serves as the mobility anchor

for interworking with other 3GPP technologies such as general packet radio service (GPRS) and UMTS [10].

- MME

The Mobility Management Entity (MME) is the control node that processes the signaling between the UE and the CN. The protocols running between the UE and the CN are known as the Non Access Stratum (NAS) protocols.

The main functions supported by the MME can be classified as:

- Functions related to bearer management*:* This includes the establishment, maintenance and release of the bearers and is handled by the session management layer in the NAS protocol.
- Functions related to connection management: This includes the establishment of the connection and security between the network and UE and is handled by the connection or mobility management layer in the NAS protocol layer [10].

2) The access network

- The access network of LTE, E-UTRAN, simply consists of a network of eNodeBs. For normal user traffic (as opposed to broadcast), there is no centralized controller in E-UTRAN; hence the E-UTRAN architecture is said to be flat.
- The eNodeBs are normally interconnected with each other by means of an interface known as "X2" and to the EPC by means of the S1 interface, more specifically, to the MME by means of the S1-MME interface and to the S-GW by means of the S1-U interface.

The protocols that run between the eNodeBs and the UE are known as the "AS protocols."

The E-UTRAN is responsible for all radio-related functions, which can be summarized briefly as:

- **Radio resource management (RRM):** This covers all functions related to the radio bearers, such as radio bearer control, radio admission control, radio mobility control, scheduling and dynamic allocation of resources to UEs in both uplink and downlink.
- **Header Compression:** This helps to ensure efficient use of the radio interface by compressing the IP packet headers that could otherwise represent a significant overhead, especially for small packets such as VoIP.
- **Security:** All data sent over the radio interface is encrypted.
- **Connectivity to the EPC:** This consists of the signaling toward MME and the bearer path toward the S-GW.

4.2 Different scenarios & mechanisms for carrying voice traffic in LTE networks:

Scenario 1: Where the entire network is LTE network but it is does not have the capability to make voice calls on LTE.

In such cases the voice calls are handled by the legacy networks like CDMA/UMTS(2G/3G). Here it is important to note that the deployment strategy for

CDMA operators, who adopt their next generation mobile network as LTE, will be different from the network operators who migrate their network from legacy 3GPP (UMTS) networks to LTE. The deployment strategies for these two category of TSPs, over a period of time has been shown in the Figure4.2. Below

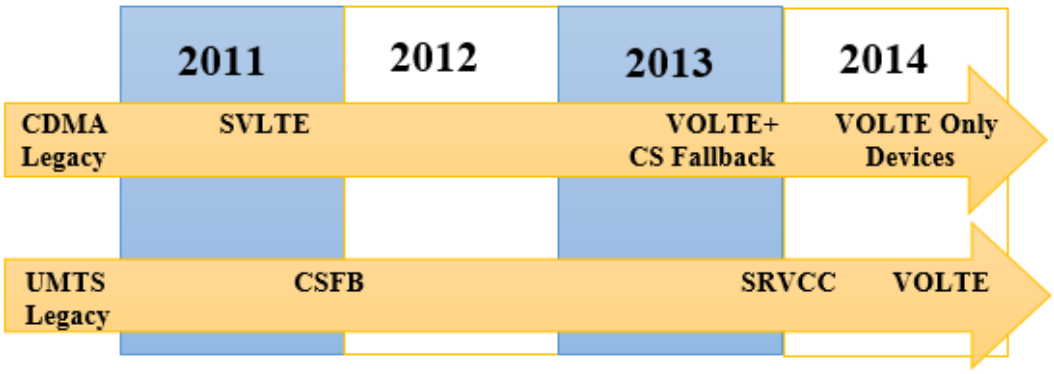


Figure 4.2: VoLTE deployment strategy

The two different techniques of carrying voice calls in this scenario are SVLTE and CSFB.
These techniques are described below.

(i) Simultaneous Voice and LTE (SVLTE)

SVLTE allows a phone to use both voice and data networks at the same time. When LTE is used with the legacy CDMA network, SVLTE uses two different radios to simultaneously communicate with:

- Legacy CDMA network for 1x RTT circuit switched services like voice call, SMS and emergency call
- LTE network to get better packet switched (PS) data throughput SVLTE is important because LTE networks were initially deployed to handle data only.

Therefore, without SVLTE such networks will not be able to carry voice traffic as the LTE data network is as good as not unavailable for voice traffic.
Though this approach helps for rapid deployment and makes the data and voice available simultaneously but using two radio antennae is not a cost effective solution for mobile manufacturers. Also two radios may create some interference which can result in high power output. This in some cases may even exceed the permitted levels. Moreover, high power
output also has direct adverse impact on battery life.

(ii) Circuit Switched Fall back (CSFB)

Circuit Switched Fall back is another feasible intermediate solution for LTE deployment voice traffic i.e. without the VoLTE solution. Due to absence of a clear voice solution in LTE during the initial phases of deployment, it was decided to opt for CSFB (CS Fall Back) as an intermediate solution. In case of CSFB if a voice call is initiated in the LTE network it is handled by the legacy networks only. When an LTE

device is used to make or receive a voice call or SMS text messages, the device "falls back" to the 3G or 2G network to complete the call or to deliver the SMS text message. And thereafter when the call is released, UE reregisters back to LTE network. However, in this solution, the user experience may be an issue due to reasons which have been mentioned in subsequent paragraphs.
The biggest advantage of CSFB is that, unlike SVLTE, only one antenna is used. But with this advantage come certain drawbacks as well. For example, when UE is registered with the legacy network during the voice call it does not have access to fast services. And in some cases e.g GSM (2G), the complete PS bearer is teared down and hence the user will not be able to avail any significant data services because of the limitation of GSM network.
As an interim solution, several TSPs use CSFB for providing voice service in LTE networks prior to deployment of VOLTE solution as the preferred method. The TSPs who use CSFB as an interim solution should migrate to VOLTE at the earliest for the following reasons:

- Innovation is limited: New services that rely on all-IP networks cannot be implemented. These include video calling.
- Customer experience is compromised:

(a) During voice calls, CSFB subscribers actually lose their LTE data service, falling back to 3G or 3G HSPA+ rates or even lose data service altogether during a fall back to 2G.
(b) In CSFB, one of the major disadvantage is higher call setup time as UE registers to 2G/3G radios networks. For example, the call set up time in CSFB on 3G is greater than 4 seconds (approximately 1 second more than the call set up time in 3G). And the call set up time in CSFB is noticeably longer than that in case of Volte's.

- High maintenance cost and increased business risk; TSPs have the burden to maintain and expand two networks in parallel.

Scenario 2: Where the LTE network exists along with VoLTE solution, however there may be patches where LTE coverage is not there.

In such cases the voice calls are handled by the LTE network, but if the LTE network coverage is not there at a particular place, then the calls are handled by the legacy networks. In case where there is full LTE coverage, the voice calls are carried on the VOLTE solution. In the patches where there is no LTE coverage, SRVCC technique is used to carry voice traffic.
These two solutions are discussed below.

(i) VOLTE

LTE is an all IP network. The implementation of VoLTE solution to deliver voice over internet protocol in LTE network is totally dependent on IMS (IP Multimedia Subsystem).
IMS brings together voice features such as authentication, server authorization, call control, routing, interoperability with PSTN, billing etc. These elements do not exist in Evolved Packet Core (EPC), that's why pure EPC cannot process a voice call without IMS in LTE network. In other words, in VoLTE solution, the access network is deployed via eUTRAN and EPC, while voice lies in IMS.

(ii) Single Radio Voice Call Continuity (SRVCC)

SRVCC solution is used when the VoLTE calls cannot be continued due to non-coverage of LTE network. In such cases SRVCC allows a PS/IMS-based (VoLTE) Voice Call to transition to a legacy CS network.
Basically, SRVCC is a call transfer method (handover), implemented in a simplified and reliable manner used when an LTE user has an active voice session in IMS and is moving to areas which have legacy 2G/3G coverage and does not have LTE coverage. The main advantage of this solution is that the call will not drop but will only be transferred to the CS
domain of the legacy networks. Further SRVCC uses a single radio, and allows an operator to provide uniform voice service, even when LTE coverage is not available. However, the signalling required is very complicated in such scenarios [1].

4.3 VOLTE

Voice over Long-Term Evolution (VoLTE) is a standard for high-speed wireless communication for mobile phones and data terminals. It is based on the IP Multimedia Subsystem (IMS) network, with specific profiles for control and media plans of voice service on LTE defined by GSMA in PRD IR.92. This approach results in the voice service (control and media planes) being delivered as data flows within the LTE data bearer. This means that there is no dependency on (or ultimately, requirement for) the legacy circuit-switched voice network to be maintained. VoLTE has up to three times more voice and data capacity than 3G UMTS and up to six times more than 2G GSM. Furthermore, it frees up bandwidth because VoLTE's packets headers are smaller than those of unoptimized VoIP/LTE**.**

4.1.1 VOLTE Architecture

The VoLTE logical architecture is based on the 3GPP defined architecture and principles for VoLTE UE, Long Term Evolution (LTE), Evolved Packet Core network (EPC), and the IMS Core Network. It consists of the following: -

- VoLTE UE:

The VoLTE UE contains functionality to access the LTE RAN and the EPC to allow mobile broadband connectivity. An embedded IMS stack and VoLTE IMS application are required to access VoLTE services.

- **Radio Access Network**:

  The Evolved Universal Terrestrial Radio Access Network (E-UTRAN); this is often referred to as Long Term Evolution (LTE). LTE radio capabilities for FDD LTE only, TDD LTE only, or both FDD and TDD LTE are applicable for VoLTE.

- **Core Network**. The Evolved Packet Core (EPC).
- IMS Core Network.

The IMS Core Network within the VoLTE architecture provides the service layer for providing Multimedia Telephony.

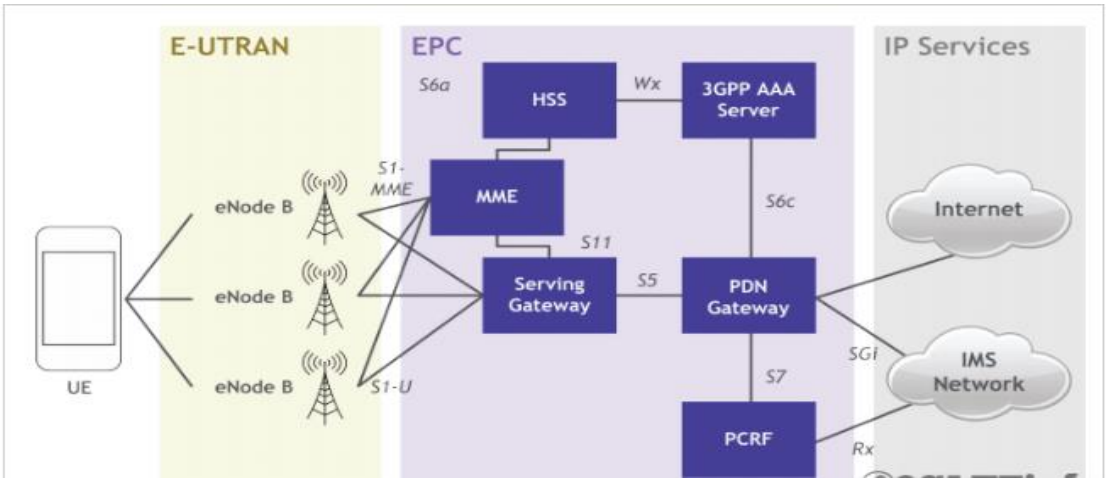


Figure 4.3: VOLTE architecture

1. VoLTE UE (User Equipment)

The User Equipment that is used to connect to the EPC, in the figure above this is an LTE capable UE accessing EPC via the LTE-Uu radio interface. Other access technologies may also be supported by the UE.

2. Evolved Universal Terrestrial Access Network (E-UTRAN)

- **eNodeB**

The EUTRAN consists of a single node, the eNodeB that interfaces with the UE. The eNodeB hosts the Physical (PHY), Medium Access Control (MAC), Radio Link Control (RLC), and Packet Data Convergence Protocol (PDCP) layers that include the

functionality of user-plane header-compression and encryption. It also offers Radio Resource Control (RRC) functionality corresponding to the control plane. It performs many functions including radio resource management, admission control, scheduling, enforcement of negotiated UL QoS, cell information broadcast, ciphering/deciphering of user and control plane data, and compression/decompression of DL/UL user plane packet headers.

3. Evolved Packet Core

- **MME (Mobility Management Entity)**

The Mobility Management Entity (MME) is the key control-node for the LTE access network. It is responsible for idle mode UE tracking and paging procedures including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the SGW for the UE at the initial attach and at the time of intra-LTE handover involving Core Network node relocation. It is responsible for authenticating the user (in conjunction with the HSS). The NAS (Non-Access Stratum) signaling terminates at the MME which is also responsible for the generation and allocation of temporary identities to the UEs. The MME validates the permission of the UE to camp on the service provider's PMN and enforces UE roaming restrictions. The MME is the termination point in the network for ciphering/integrity protection for NAS signaling and handles security key management. Lawful interception of signaling is also a function provided by the MME. The MME provides the control plane function for mobility between LTE and 2G/3G access networks and interfaces with the home HSS for roaming UEs.

- **SGW (Serving Gateway)**

The SGW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating the S4 interface and relaying

the traffic between 2G/3G systems and PGW). For idle state UEs, the SGW terminates the DL data path and triggers paging when the DL data arrives for the UE. It manages and stores UE contexts and performs replication of the user traffic in case of lawful interception. The SGW and PGW functions could be realized as a single network element.

- **PGW (Packet Data Network Gateway)**

The PGW provides connectivity between the UE and external packet data networks. It provides the entry and exit point of traffic for the UE. A UE may have simultaneous connectivity with more than one PGW for accessing multiple Packet Data Networks. The PGW performs policy enforcement, packet filtering for each user, charging

support, lawful interception and packet screening. The SGW and PGW functions could be realized as a single network element.

- **HSS (Home Subscriber Server)**

The HSS is a network database that holds both static and dynamic data elements related to subscribers. The HSS provides user profile information to the MME and IMS core during UE attach and IMS registration.

- **PCRF (Policy Charging and Rules Function)**

The PCRF provides policy control decisions and flow based charging controls. The PCRF determines how a service data flow shall be treated in the enforcement function (PGW in this case) and ensure that the user plane traffic mapping and treatment is in accordance with the user's profile.

3. IMS Core

IMS core is responsible for session management and media control. IMS core as shown in the Figure4.4 bellow

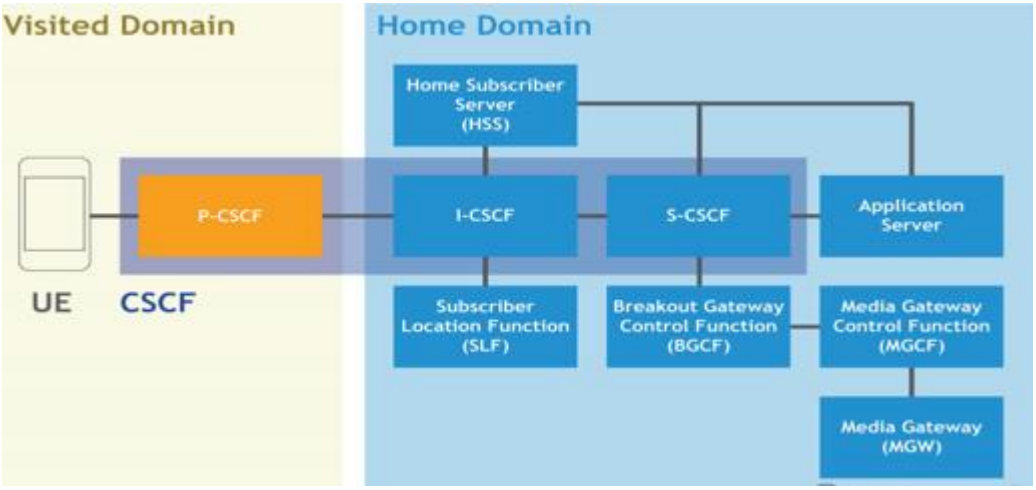


Figure4.4: IMS Core

IMS core has the following important nodes.

- Call Session Control Function (CSCF)

CSCF is responsible for establishing, monitoring, supporting and releasing multimedia sessions. It has three different functional elements which may or may not be separate physical entities.

- **Proxy CSCF:** P-CSCF is seen as the initial point of contact from any SIP User Agent. It handles all requests from the UE and is, from the UE's point of view, the "SIP proxy" to the entire subsystem.
- **Serving CSCF:** S-CSCF has knowledge about the user and what applications are available to the user. It acts as a decision point and its main job is to decide whether or not the user's SIP messages will be forwarded to the application servers.
- **Interrogating CSCF:** I-CSCF is the entity that initiates the assignment of a user to an S-CSCF (by querying the HSS) during registration.

- Home Subscriber Server (HSS)

HSS is a database that maintains user profile and location information and is responsible for name/address resolution. HSS is also responsible for authentication and authorization.

- Subscriber Location Function (SLF)

  SLF is responsible for assigning HSS to user in home network. To achieve this function SLF keeps track of all HSSes.

- Media Gateways

Media Gateway resides at the interface between SIP based IMS network and traditional PSTN network. More details are found in RFC 3372 (Session Initiation Protocol for Telephones (SIP-T): Context and Architectures)

- Media Gateway Control Function(MGCF)

Media Gateway Control Function controls media gateways, converts codecs where necessary and may serve as a breakout to a circuit-switched network.

In the case when MGCF works as a breakout to CS network it is also responsible for managing the conversion of signaling messages, converting SIP messaging to the Bearer Independent Call Control (BICC) and ISDN User Part (ISUP) protocols used in legacy systems.

- Breakout Gateway Control Function (BGCF)

When Media Gateway Control Function does not include breakout to circuit-switched network, BGCF takes care of this functionality.

4.4 Benefits of having voice through VoLTE

VoLTE offers a number of benefits both for the subscribers as well as the TSPs. An independent research has been done by study by ABI (a Signals Research Group) to

analyses VoLTE performance in a commercially deployed network. The research evaluated the parameters like call setup time, reliability, quality, network resource requirements, battery life etc. The significant findings are as under:

- VoLTE call quality greatly exceeded that of 3G circuit-switched voice and was measurably higher than the HD voice service offered by Skype.
- VoLTE supports the wideband advanced multirate codecs that enable the next level of evolution of the phone call, that is, high-definition (HD) voice
- With network loading i.e., lots of competing traffic, and in particular with background applications running on the mobile phone exchanging data with the network, the VoLTE results were considerably better than Skype
- VoLTE call setup time was nearly twice as fast as 3G Circuit Switched Fallback (CSFB) call setup
- VoLTE used substantially fewer network resources than Skype voice, which in turn resulted in longer estimated device battery life for the subscriber and a more efficient network for TSPs
- When leaving LTE coverage, VoLTE calls were successfully handed over to 3G or 2G circuit switched voice, ensuring call continuity without interruption. Whereas this was not the case with VoIP on other OTT Applications. Therefore, with VoLTE while the subscribers benefit from better Quality of Service and improved device battery life, the TSPs enjoy greater delivery efficiency.

So deploying VoLTE in LTE network offers a number of benefits for both, the Customers as well as the TSPs. These are summarized as under:

4.4.1 Advantages of VoLTE from customer's point of view

For the Customers, VoLTE offers a number of benefits. Some of these benefits are mentioned below:

- Call set-up time: In case of VoLTE call set-up time is 1-2 seconds, while in case of circuit switching, the UMTS/GSM layer typically takes 5-10 seconds.
- Sound quality: The highest possible bit rate can be defined in VoLTE. Currently, the global voice standard supports AMR-WB codec at 23.85 kbps, which is HD voice.
- Battery life: VoLTE sessions require significantly less power because the processing happens on the baseband processor or modem rather than on the application processor.
  Moreover, as the call set-up time is less with VoLTE, the battery life of the user device is increased by 15-20 per cent on this account only.
- Sessions: Simultaneous voice and data connections are achieved through the shift to VoLTE. It also has the potential to be combined with rich media services.
- Multimedia services: VoLTE enables multimedia content sharing during voice calls, SMS over IP, video calls and video sharing.

4.4.2 Advantages of VoLTE from TSPs point of view

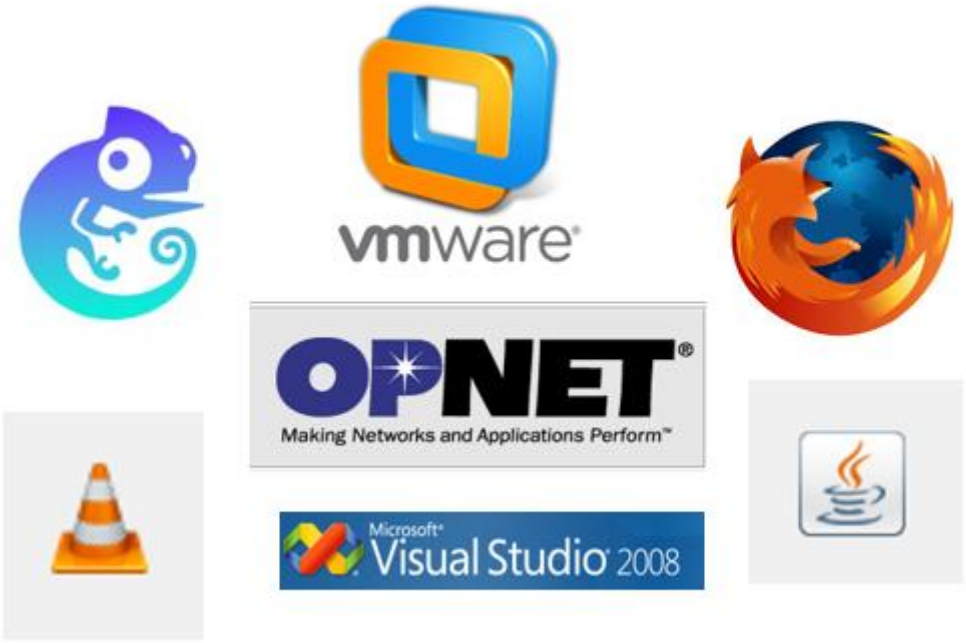
For the TSPs, VoLTE offers a host of marketing and operating advantages. Some of these are enumerated below:

- Reduced cost and complexity of network because a single all IP network carries voice, video and other data services.
- Enhanced user experience which could lead to ARPU augmentation.
- Capability to support rich multimedia applications like HD voice which can help TSPs market the services in a better manner.
- Efficient spectrum utilization provides opportunities for Opex savings from consolidation and optimization.
- The rich communication suite support in VoLTE, enables TSPs to compete with OTT Service Providers as they can offer a host of services like rich voice and messaging services including SMS, Instant Messaging, group chat, live video sharing and file transfer etc... [5].

Part II

Simulation and Emulation

- VOIP Emulation on : Chapter 5
- VOLTE Simulation on : Chapter 6



Chapter 5
VOIP & IPTV

5

5.1 VOIP

Voice over IP is an important service of IP multimedia subsystem. this project is focused on how amazing are the services and the applications that IP multimedia subsystem would offer for us as subscribers, network providers, and telecommunication carriers. One of them is making a voice over IP call using emulation programs they are CUCM, GNS3, Cisco IP communicator and media5 phone application for cellphones. CUCM acts as a server to control the calling process. GNS3 is used to implement the network. Cisco IP communicator and media5 phone application are installed just to provide making VoIP calling.

5.1.1 CUCM Simulation (Programs Description and Interfaces)

Cisco Unified Communications (UC) is an IP-based communications system integrating voice, video, data, and mobility products and applications. It enables more effective, secure communications and can transform the way in which we communicate. Cisco IP Communications represents a new way of delivering UC functionality to enterprise customers. Instead of delivering a collection of disjointed products with individual release dates, testing methodology, and documentation, Cisco UC is a coordinated release of an *integrated* set of products that are tested, documented, and supported *as a system*. This project was simulated by different program to show as many as possible features for UC system. Those programs can be summarized as following

1. VMware and CUCM

CUCM was installed in a VMware 10 as a UC simulation. It has a Command Line Interface (CLI) as any other cisco product. This interface is shown in Figure 5.1

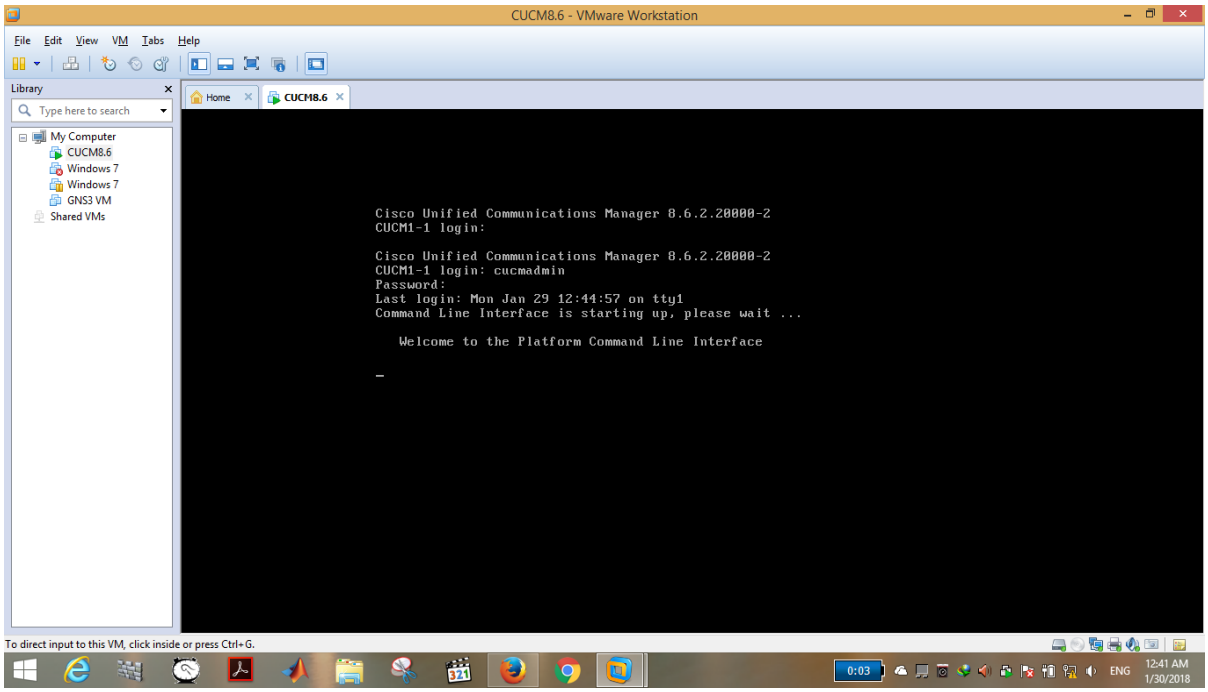


Figure 5.1: CUCM CLI in VMware

2. Web Browser

CUCM Graphical User Interface (GUI) can be used at any web browser connected to the server. It used to have a full and easy control to CUCM and can be opened at the browser by writing its IP. CUCM website home page shown in Figure 5.2. Also, user home page is shown in Figure 5.2

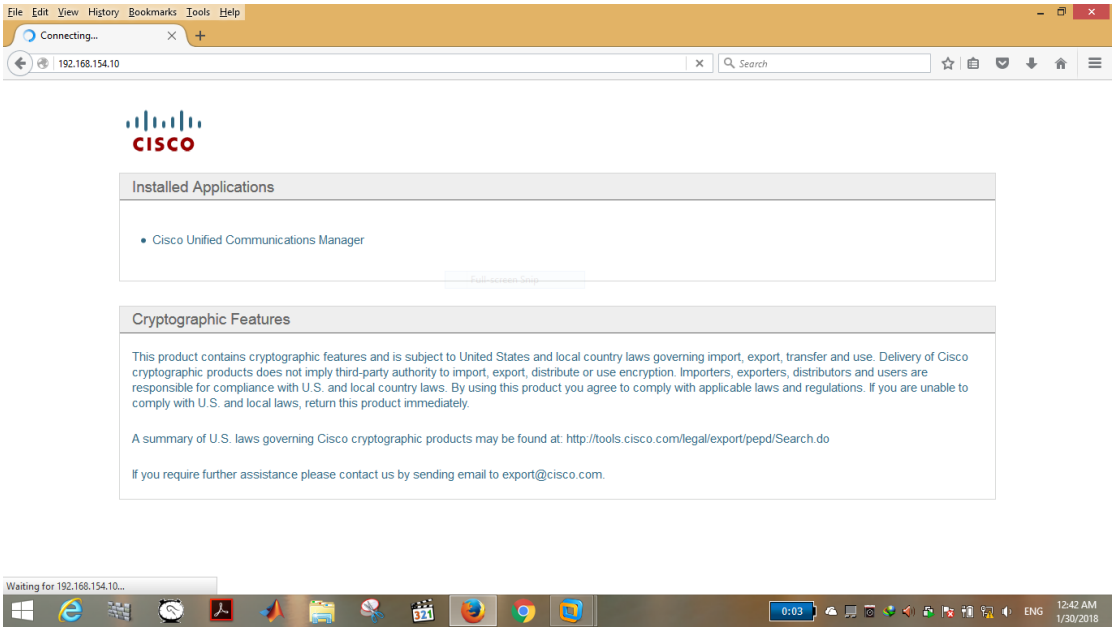


Figure 5.2:. CUCM website home page

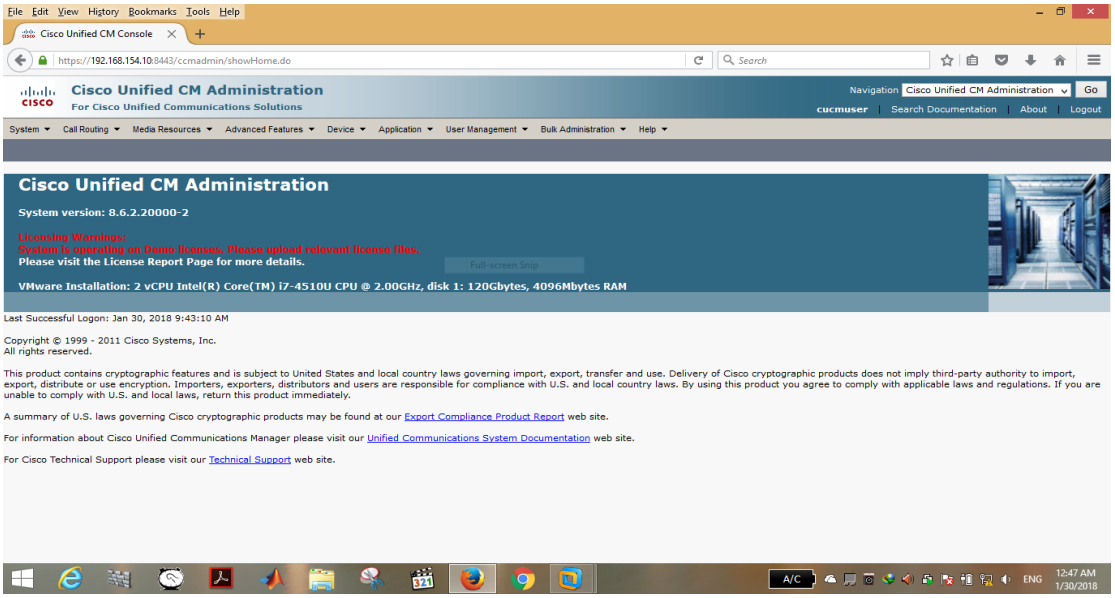


Figure 5.3: User home page

3. Cisco IP Communicator

The Cisco IP Communicator is a software - based phone that delivers the capabilities of the 7900 Series phones through a PC running Microsoft Windows and Vista. This solution is perfect for travelers who require advanced telecommuting features. Using the IP Communicator gives users all the features of a 7970 IP hardware phone through a PC. In fact, the interface looks exactly like a 7970 hardware phone, so end users will immediately be familiar with how it works. All the features are available, including up

to eight separate lines, direct access to voice mail, and XML services. Most third - party microphones and headsets are fully compatible with the IP Communicator. Figure 5.4 shows an image of the Cisco IP Communicator running on Windows.

Figure 5.4: Cisco IP phone

Media5-Fone .5

Media5-Fone is another IP phone program. It is a dependent program works by adding the phones MAC address to its system to make a contact list. However, it was connected to the CUCM in this project to show the SIP features. Figure 5.5 next page shown media5 Fone program

Figure 5.5: media-5 Fone

5. GNS3

GNS3 is a simulation program for network. It was use in this project to make a virtual network diagram and connect it to the CUCM. The virtual network that made in GNS3 shown in Figure5.6

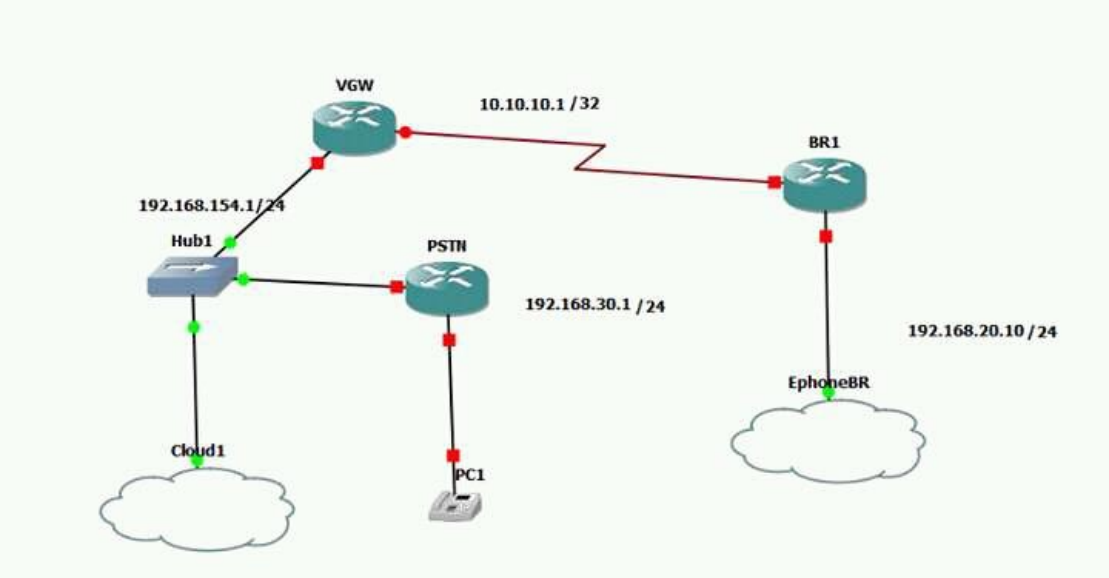


Figure 5.6: Virtual network for the project

5.2 CUCM Configuration

Those configurations applied to be download from the TFTP server to the phones while they registry to the CUCM. Those configurations are

1. Time zone

From System tab select Date/Time Group as shown in Figures 5.7, then add the zone information that the phones will work on it as shown in Figure 5.8, after saving the zone information, the date/time group will be shown in Figure 5.9This information will be specified for a specific group and all the phones in the same zone will be part of this group, if there is another time zone for anther phones, anther time group should be created. This project used only one group for the phones' simulation but three more groups with different time zones were created for more explanation.

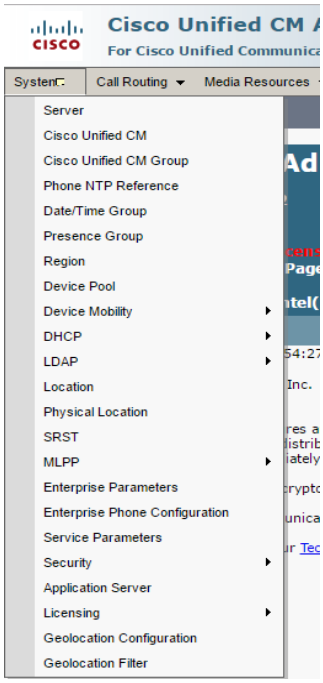


Figure 5.7: System tab's options

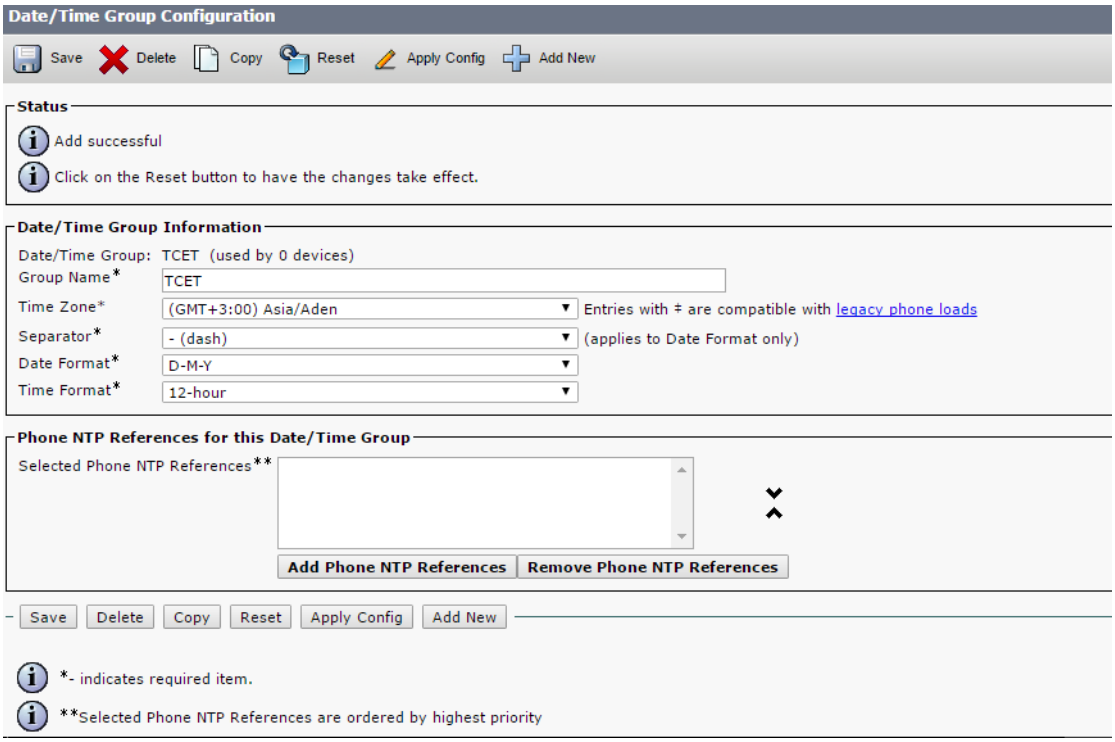


Figure 5.8: Date/Time group configurations' interface

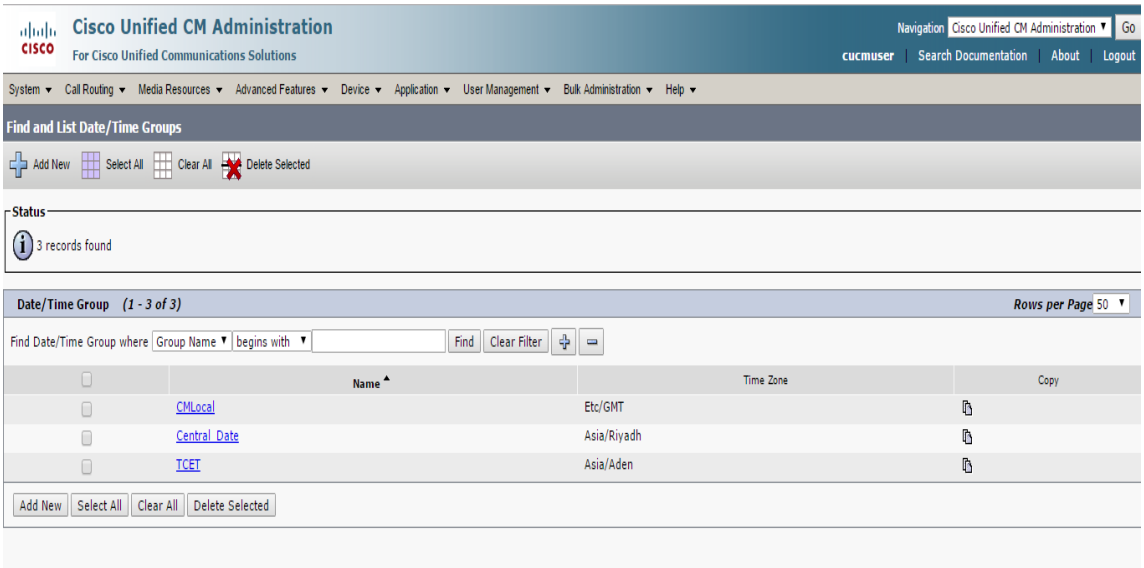


Figure 5.9: Existing Date/Time groups

2. Network Time Protocol (NTP)

NTP for the server was applied while the instillation. NTP configurations for windows which is the NTP server that the phone software will installed time zone information from it, and it configured like that:

In the services' window in Figure 5. 11 (part of Administrative Tools Figure 5.10) stop the 'Windows Time' service if already running. Start the 'Windows Time'; the 'Startup Type' could be set as manual or automatic depending on the user needs as shown in Figure 5.12.

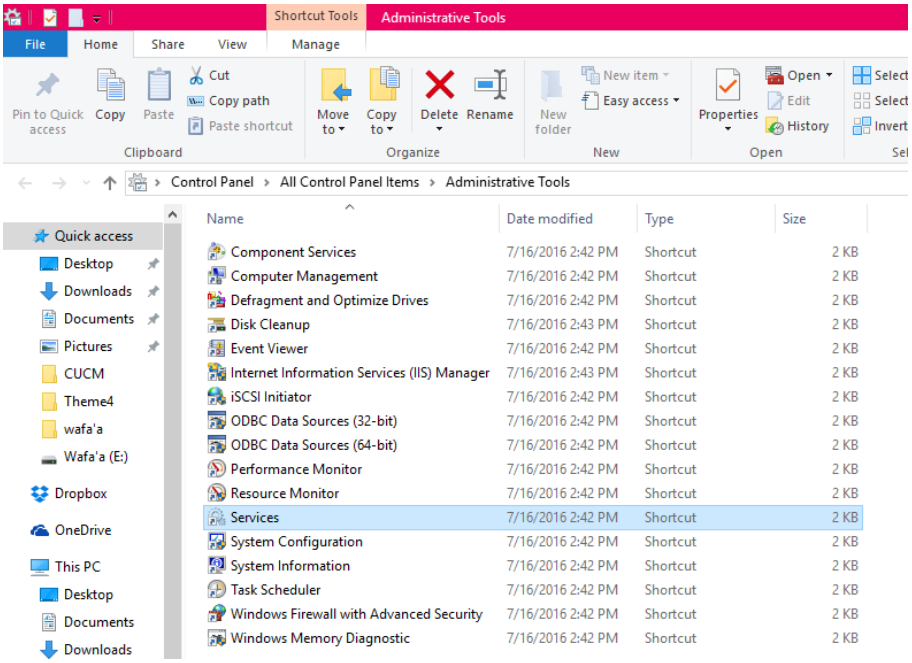


Figure 5.10: Administrative tools' list

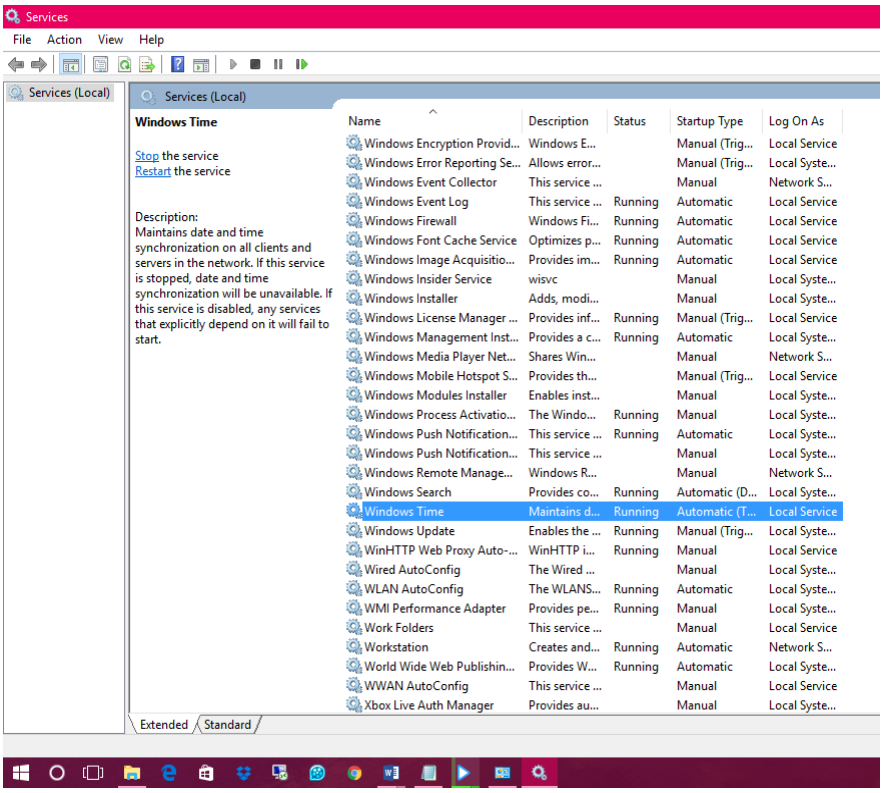


Figure 5.11: Services' list

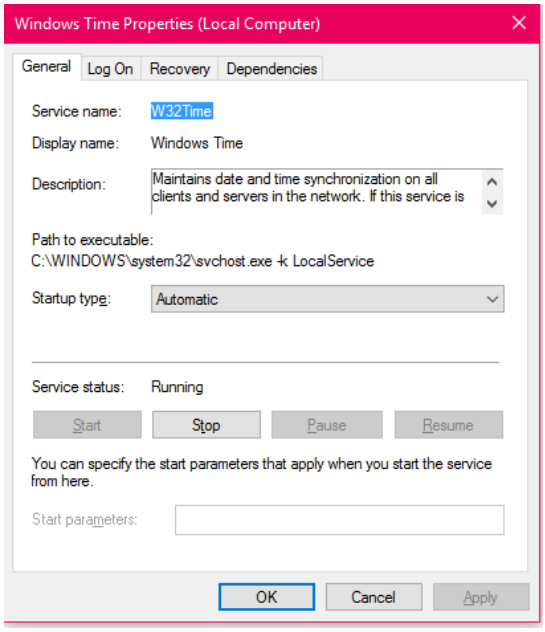


Figure 5.12: Windows time properties

3. CO configurations

CO has been connected with VMware that contains CUCM server and the main windows of the device that has been configured as NTP server for the CO. The main windows contain two phones. The first Cisco IP Communicator phone that has been worked by SCCP protocol, and the second X-Lite phone that has been worked by SIP protocol. The VGW has four step of configurations which is:

a. Dial Peer.
b. Codec.
c. Signaling.
d. QoS.

Those configurations can be explained in details as following

a) Dial Peer

In order to route voice traffic properly from one point to another point using H.323 or SIP voice gateways, dial peers' configurations are needed. A dial peer is a device that can make or receive a call in a voice network. With VoIP networks, there are two types of dial peers:

- POTS dial peers
- VoIP dial peers

Those points can be review to see how they function in IP and PSTN network

- **POTS Dial Peers**

POTS dial peers are considered to be traditional telephony devices such as analog phones, cellular phones, and fax machines. From a voice gateway perspective, the POTS dial peer is a simple dial - string - to - port mapping. Figure 5.13 illustrates a POTS dial - peer scenario. A single POTS dial peer runs from the analog phone located on the PSTN to the local voice gateway.

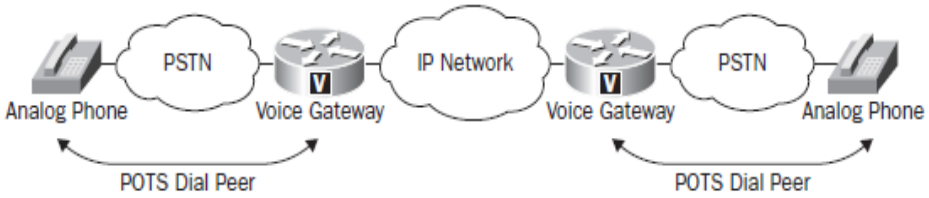


Figure 5.13: POTS dial peers

- **VoIP Dial Peers**

These dial peers include any VoIP - capable endpoint, router, and gateway within the IP network. Just like POTS dial peers, VoIP dial peers use a dial string for mapping purposes. The difference is that instead of mapping the dial string to a physical interface, the VoIP dial peer maps the dial string to a remote IP network device. Figure 5.14 helps to explain VoIP dial peers.

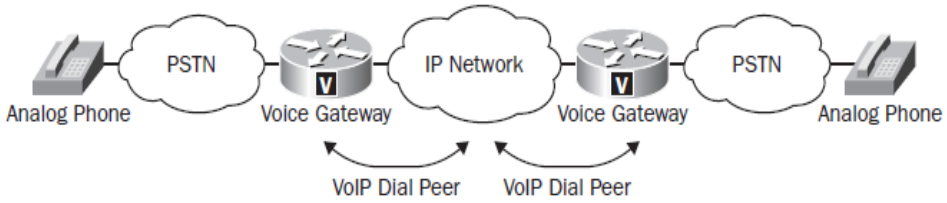


Figure 5.14: VoIP dial peers

In this example, there is a VoIP dial peer for each side of the IP network. They are needed because each voice gateway requires a dial - peer configuration in order to identify the call source and destination endpoints.

In this project three dial peers were configured in the GW which is dial peer to the CME which is any call with directory number of 2XXX, the two others are to the PSTN which is any call with the directory number of 77XXX for any call goes from the GW to the PSTN or to the BR during the PSTN link, and 77XXX for any call goes back from the PSTN or BR to the GW. This is shown in Figure 5.15

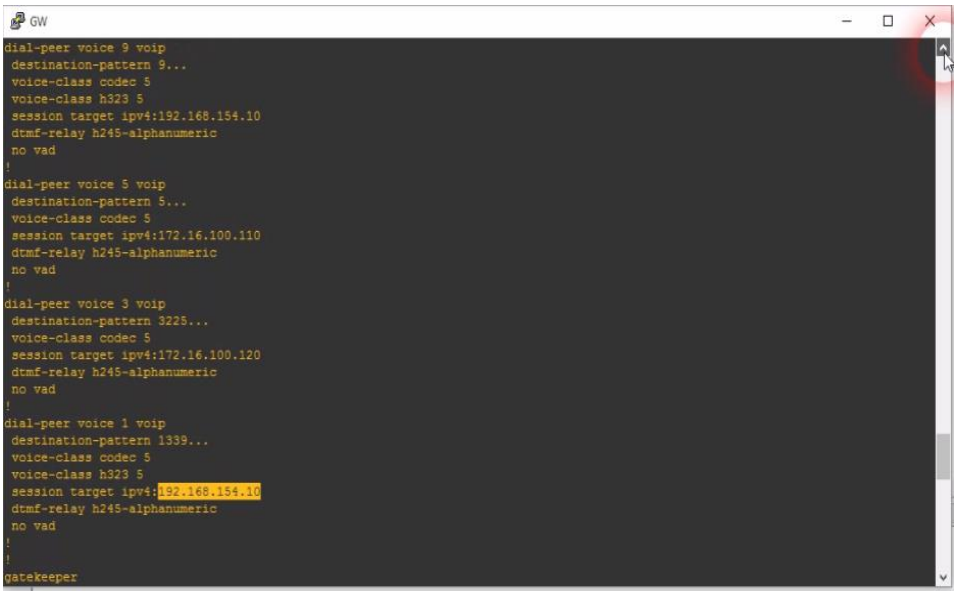


Figure 5.15: GW dial peers

b) Codec and Signaling

Codec and protocols' signaling were explained in chapter 2. In this project, researchers configured the GW to codec any packet comes to it to G.711 to communicate. The signaling used here is H323, so any packet comes to the CUCM will be transmitted by H323. That's shown in figure 5.16.

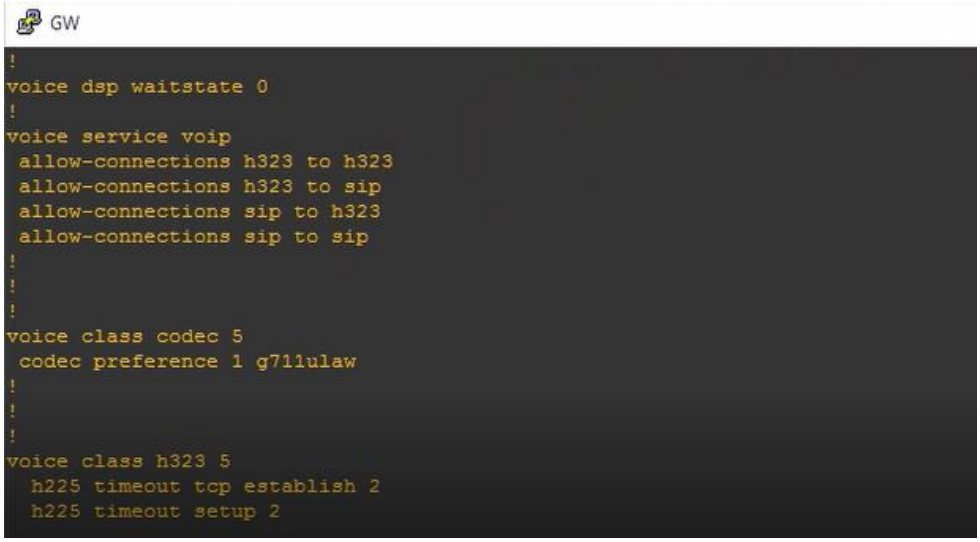


Figure5.16: GW signaling and codec

4. BR Configurations

BR has been connected to the VMware at another device that contains Windows XP. Windows XP contains Cisco IP communicator phone and connected the router with the main windows of the device. The main Windows has been configured as NTP, and contains a phone from the same type. The router has been configured as CME and segregation it as independent system for reduce the problem of WAN. Where the call from any branch has been converted to the CUCM directory and the call has been configured from there. That make compression on the link. also for keep the internal connected in the branch when the link cut off between the branch and CUCM. The configurations have done as fallowing

1. Dial peer

Dial peer to the VGW and PSTN as shown in Figure 5.17

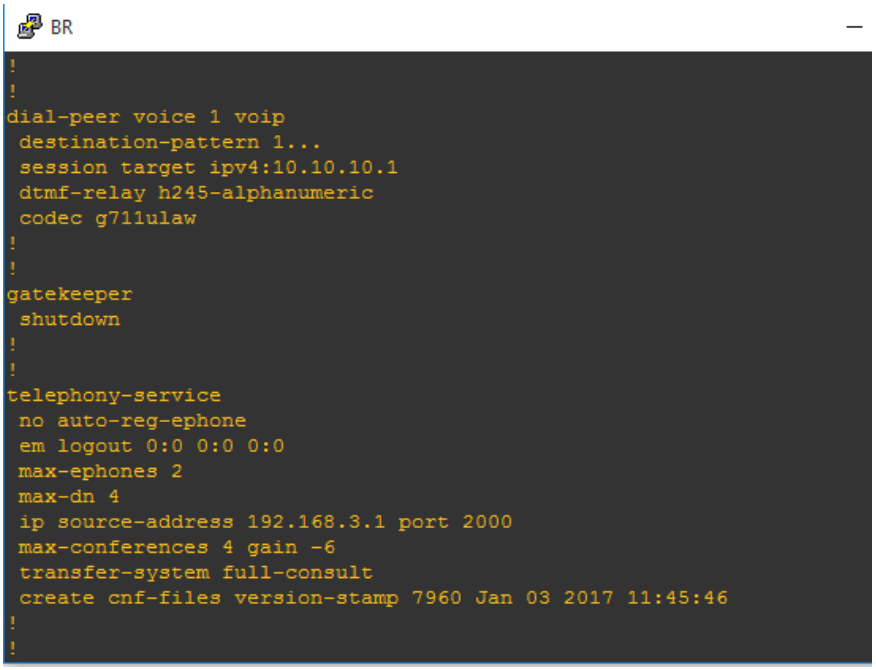


Figure 5.17: BR dial peer

2. A telephony service setup

One configuration method that is often brought up is the telephony - service setup script command. The telephony service setup script is a command - line script that walks an administrator through a series of DHCP and voice questions to automatically configure IP phones and IP phone' DN settings. The CUCM Express CME is then set up for auto - assign so that it hands out extension numbers automatically when phones begin to add to the network. At the same time, it grabs the phone' s MAC address and puts it into the IP phone configuration so it will continue to receive the same extension from that point on. To demonstrate this functionality, researchers used telephony-services

commands shown in the index, and this is the result of the command show run for this service shown in Figure 5.18

BR

```
!
!
dial-peer voice 1 voip
 destination-pattern 1...
 session target ipv4:10.10.10.1
 dtmf-relay h245-alphanumeric
 codec g711ulaw
!
!
gatekeeper
 shutdown
!
!
telephony-service
 no auto-reg-ephone
 em logout 0:0 0:0 0:0
 max-ephones 2
 max-dn 4
 ip source-address 192.168.3.1 port 2000
 max-conferences 4 gain -6
 transfer-system full-consult
 create cnf-files version-stamp 7960 Jan 03 2017 11:45:46
!
!
```

Figure 5.18: BR telephony services

3. PSTN Configurations

PSTN has only dial peer configurations to the GW as shown in Figure 5.19

PSTN

```
!
!
!
control-plane
!
!
!
mgcp fax t38 ecm
!
!
!
dial-peer voice 3 voip
 destination-pattern 3225...
 voice-class codec 5
 session target ipv4:172.16.100.110
 dtmf-relay h245-alphanumeric
 no vad
!
dial-peer voice 1 voip
 destination-pattern 1339...
 voice-class codec 5
 session target ipv4:172.16.100.100
 dtmf-relay h245-alphanumeric
 no vad
```

Figure 5.19: PSTN dial peer

- Add Telephone settings

To use any IP phone within the CUCM it must be added and configured at the CUCM first. The steps of adding a phone is as explained in the coming steps:

1- From the device bar chose Phone as shown in Figure 5.20

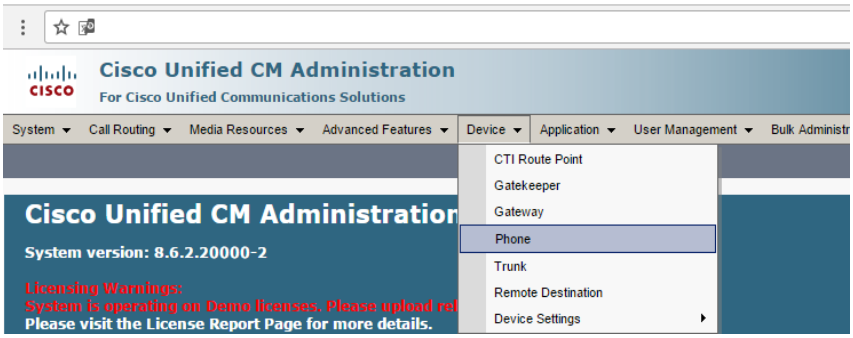


Figure 5.20: The selection for the phone from device bar

2- At the second window Click on add new to add new phone as shown in Figure 5.21

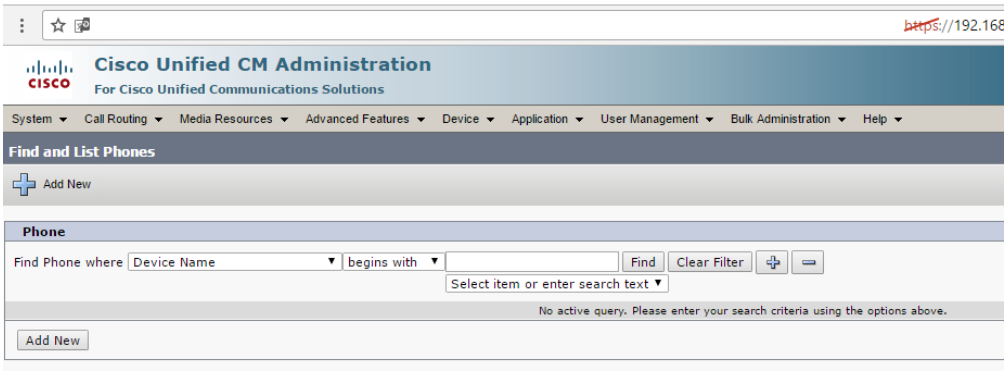


Figure 5.21: Find and list phones page

3- Choose the type of the phone that has been used. Here Cisco IP communicator has been used just as shown in Figure 5.22.

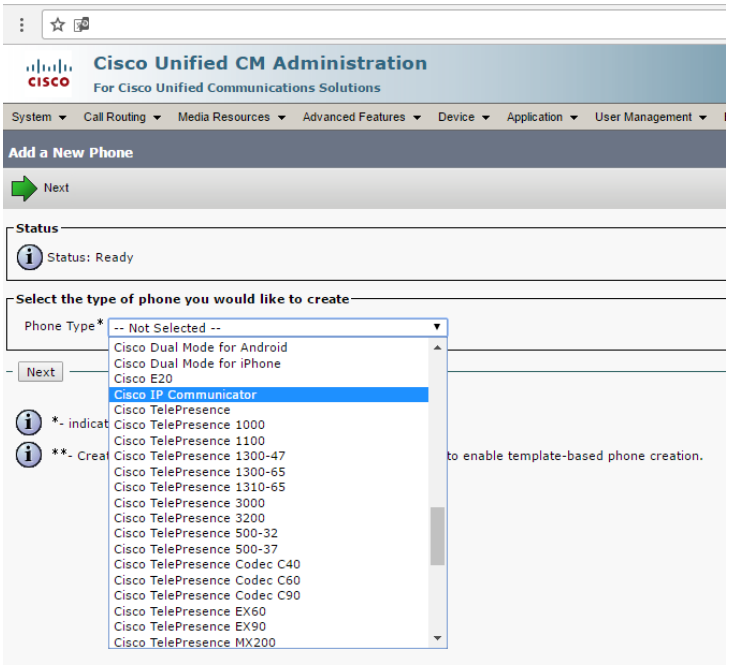


Figure 5.22: Select the phone type

4- Determine the protocol type if it's Cisco type should be use SCCP protocol. All another phone types used SIP protocol. This is shown in Figure 5.23.

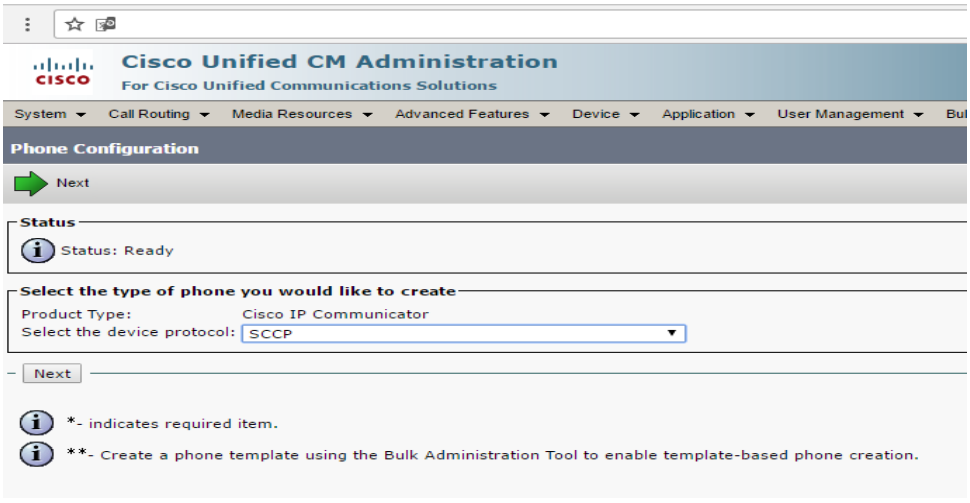


Figure 5.23: Select protocol type

5. After choosing the type of protocol. The following Window opens, adding all the phone information isn't necessary because some information was added to

the system by default, just focus on the parts marked by a (*). As shown in Figures 5.24and 5.25

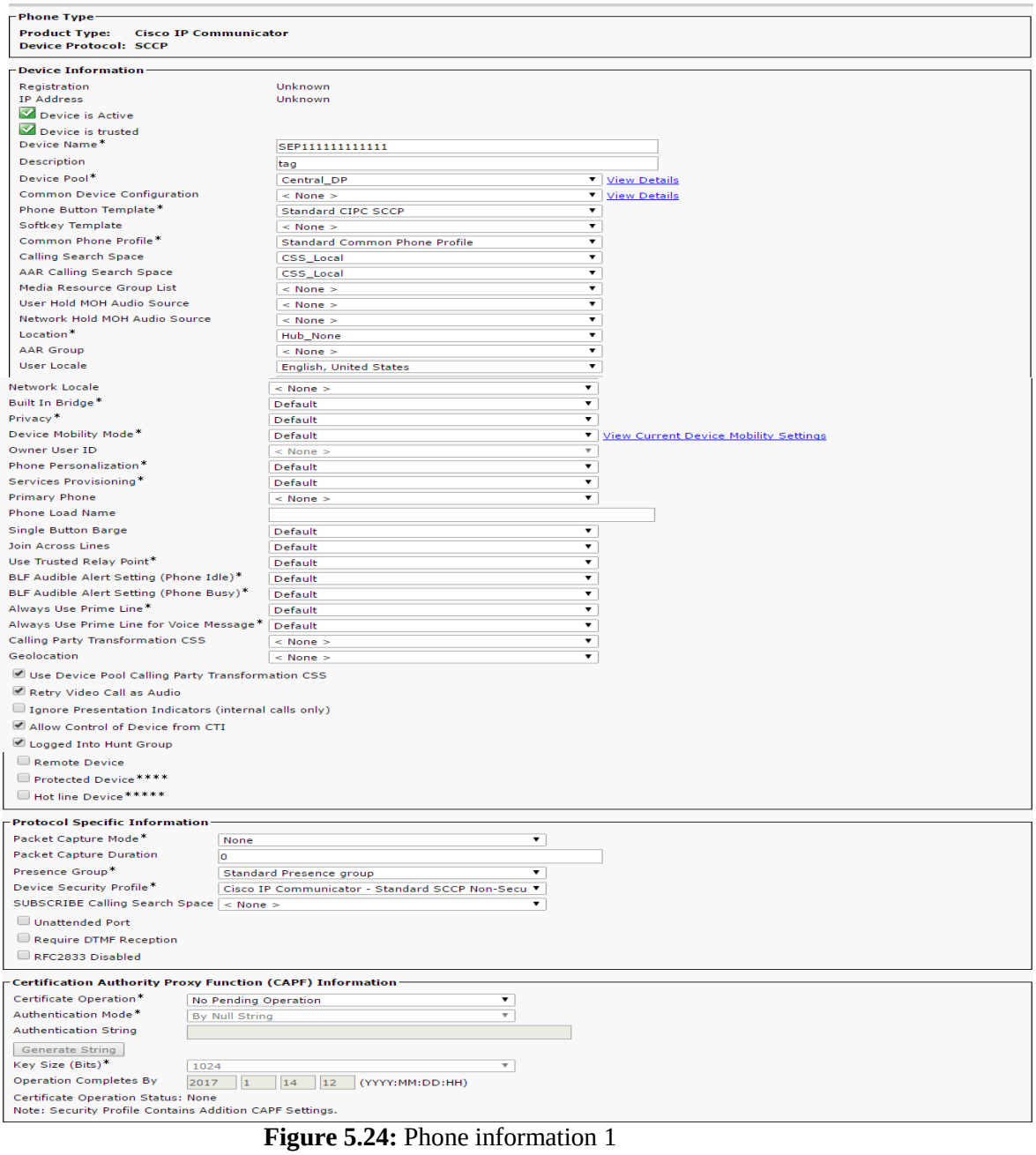


Figure 5.24: Phone information 1

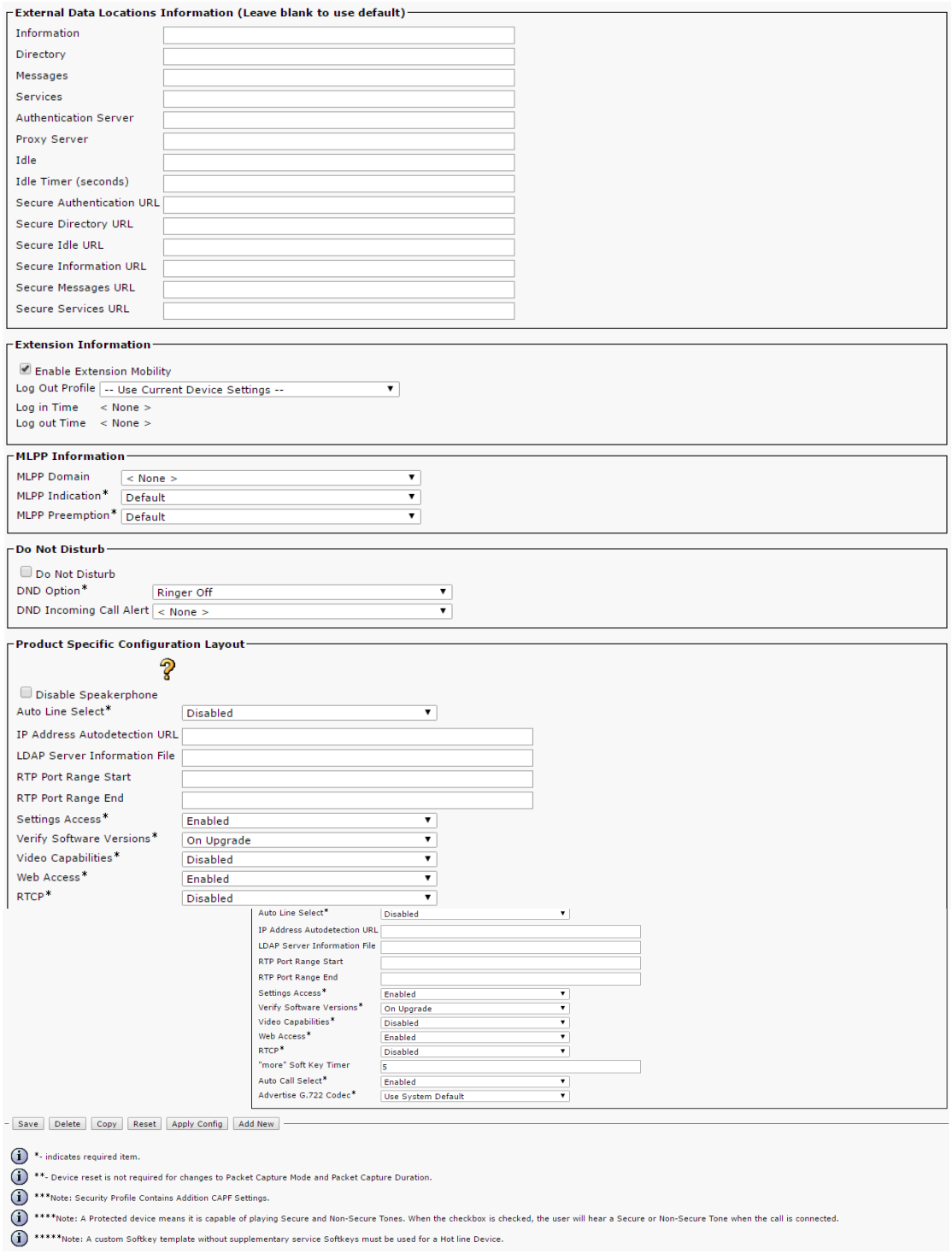


Figure 5.25: Phone information 2

5- At the end click on save to keep the changes

6- To show phones added to the system. Device → phone → find as shown down in Figure 5.26

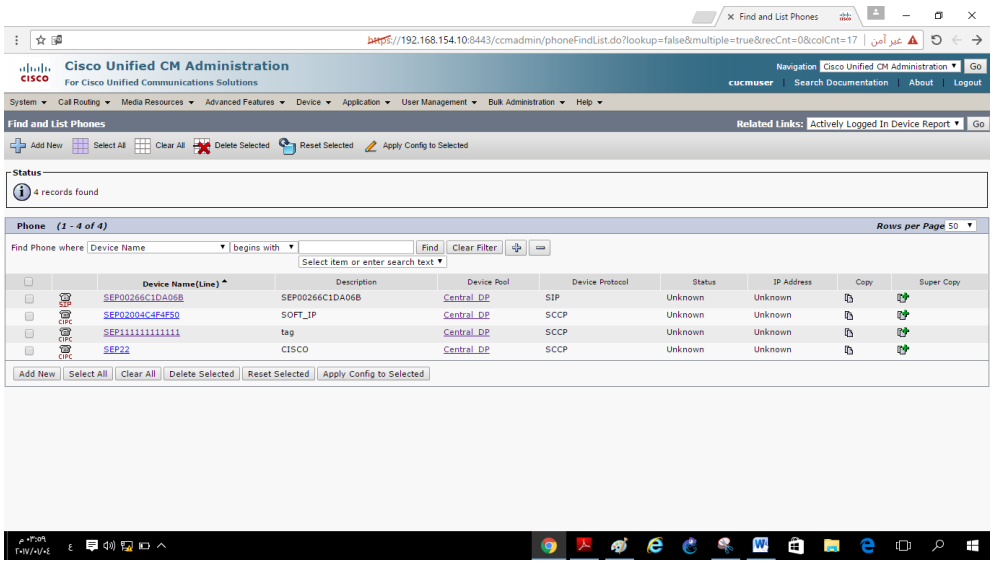


Figure 5.26: Phones in CUCM

5.2 IPTV

5.2.1 VLC

The building has contracted for IPTV services as well as high speed internet access. IPTV (Internet Protocol Television) is accessible by any laptop/computer or cellphone wired to the network, which has a specialized VLC (Video LAN Client) installed.

VLC includes a fairly easy-to-use streaming feature that can stream music and videos over a local network or the Internet.

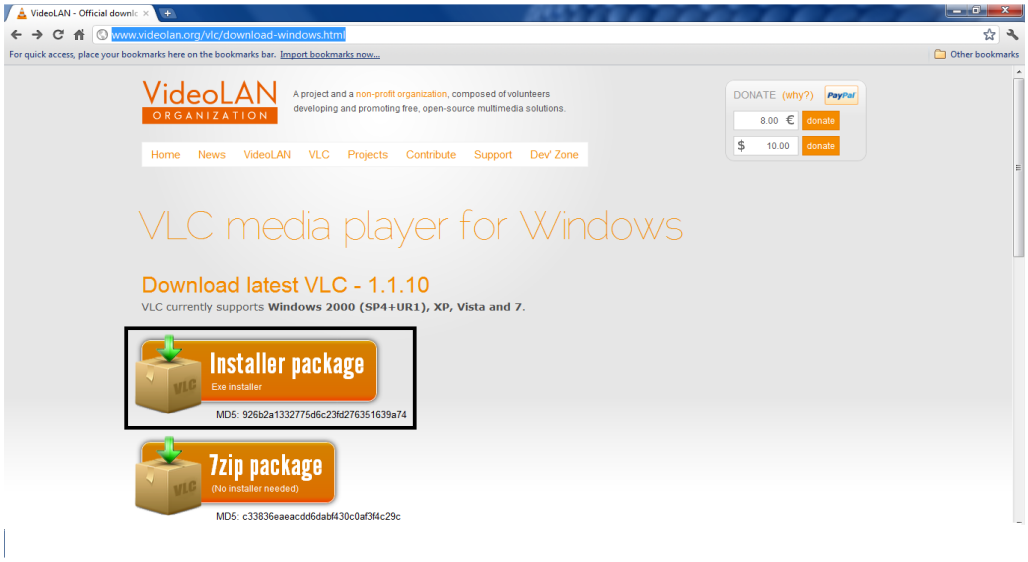


Figure 5. 27: VLC media player for windows

First, we have to connect the laptop with a unique IP of the same network of a voice gateway. As shown in figure 5.28

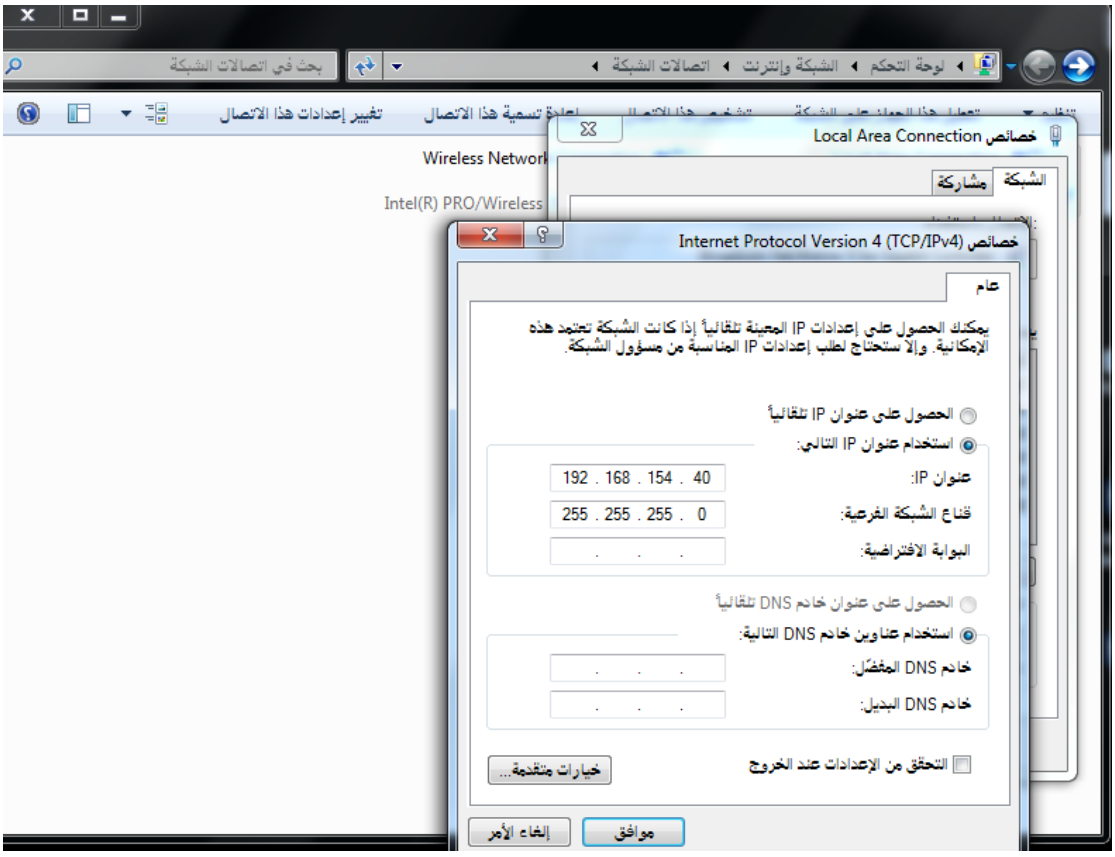


Figure 5.28: IP Address of the IPTV

How to stream videos and music over the network using VLC

1- To start broadcasting a network stream, click the Media menu in VLC and select Stream.

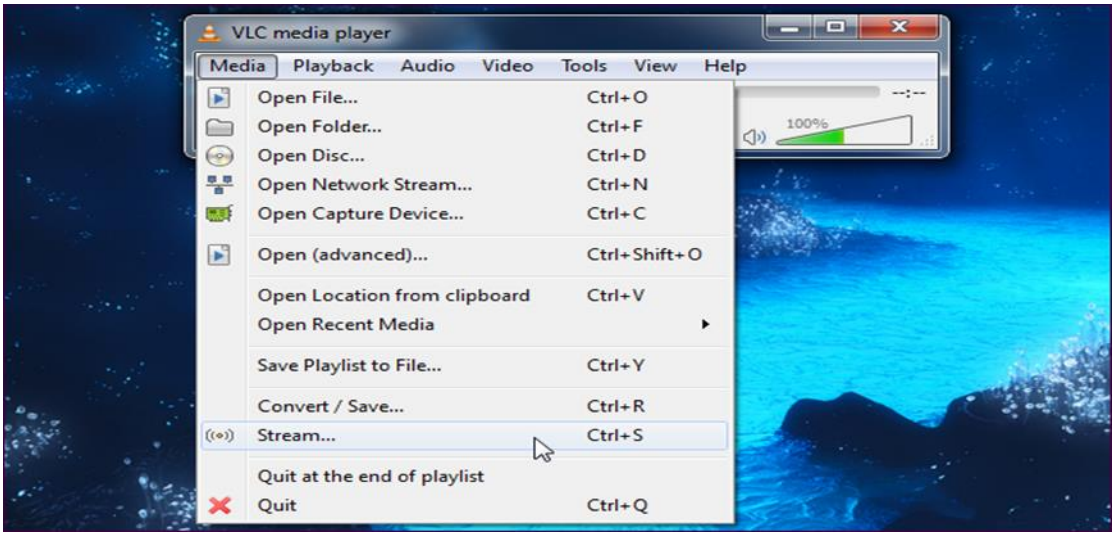


Figure 5.29: broadcasting a network stream.

Step 1

Click the Stream button after selecting your media.2

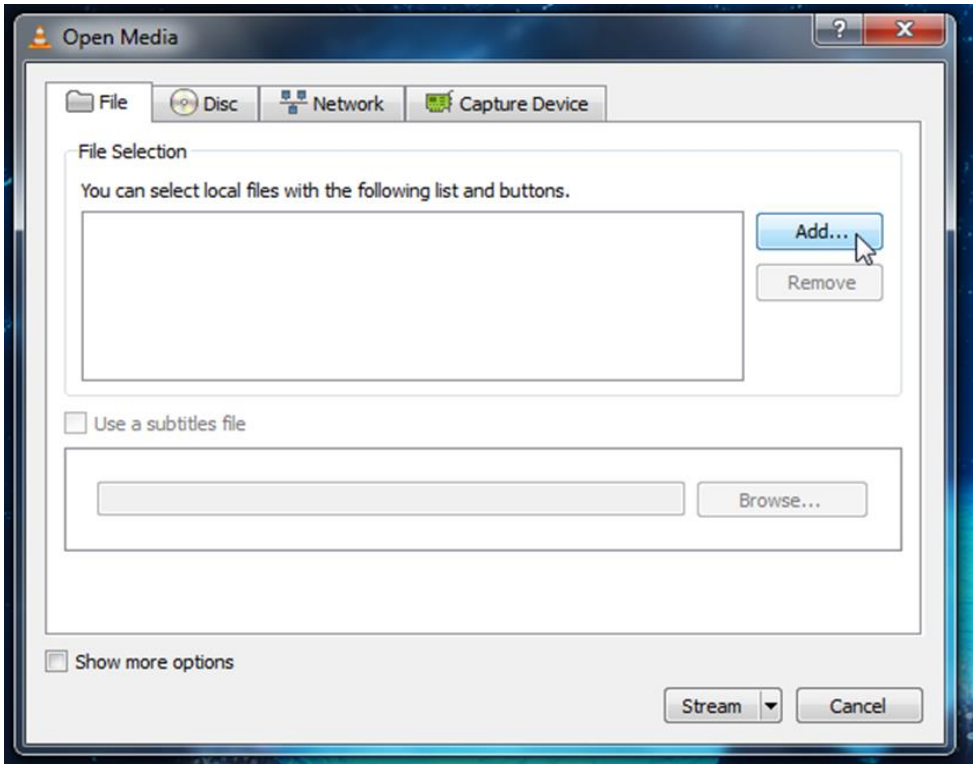


Figure 5.30: step 2

The Stream Output window will appear. The first pane just lists the media source you selected – click Next to continue.

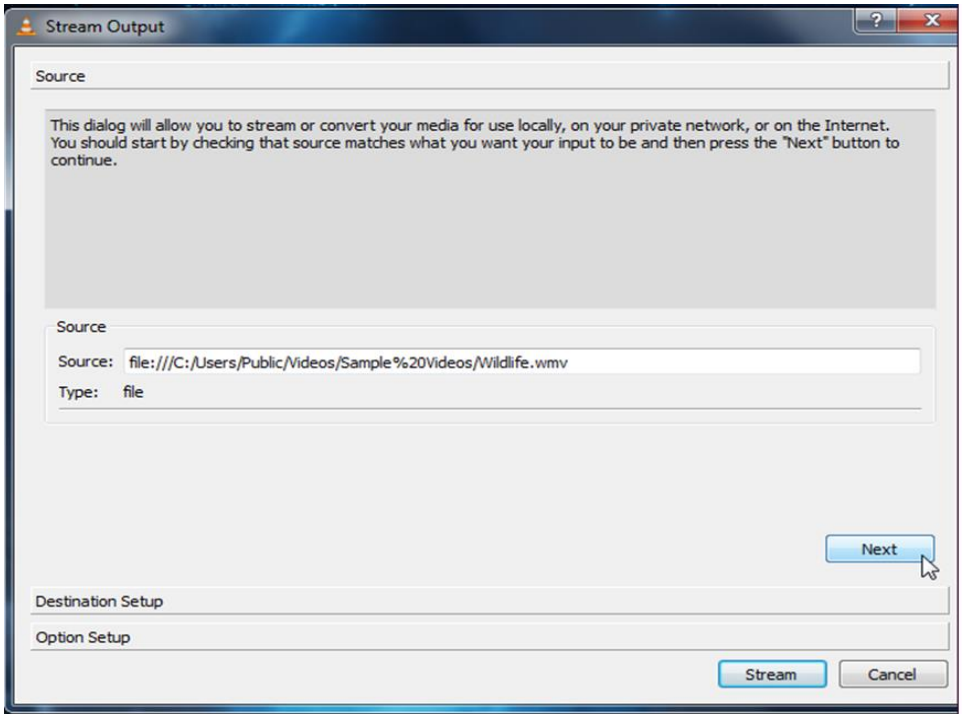


Figure 5.31: step 3

On the Destination Setup pane, you'll need to choose a destination for your stream. For example, you can select HTTP to listen for connections – other computers can connect to your computer and watch the stream. You can also select UDP to broadcast to a specific IP address or range of IP addresses.

After selecting your destination, click the Add button. You may also want to activate the Display locally check box – if you do, you'll see and hear the media being streamed on your local computer, so you'll know it's playing correctly.

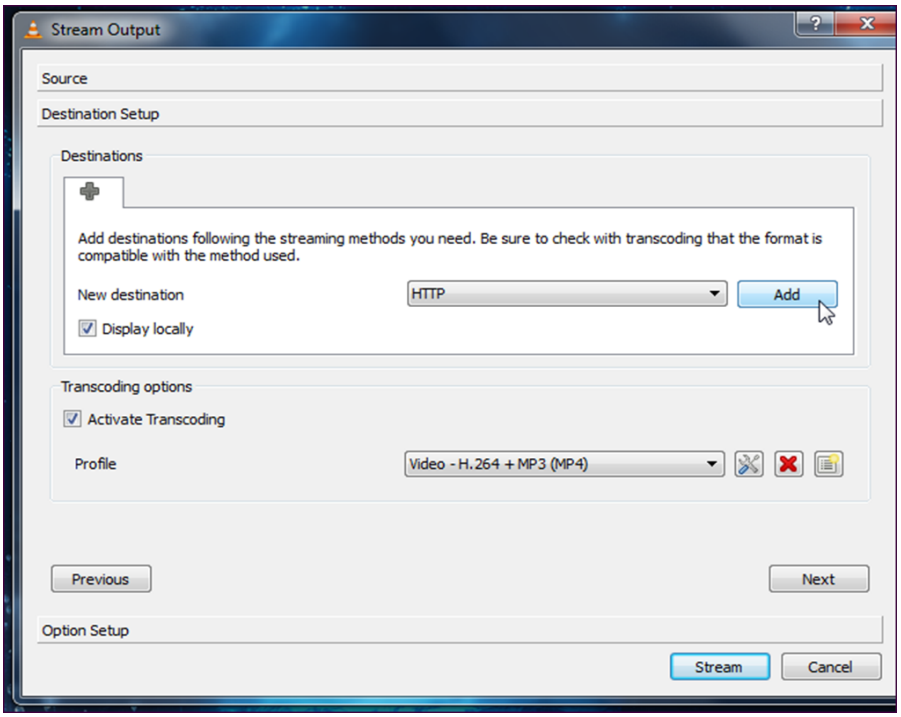


Figure 5.32: step 4

After adding a destination, you'll be able to customize its settings. With the HTTP destination, you could specify a custom path – but the default one will work fine.

You can also tweak the transcoding settings – by transcoding to a lower quality, VLC can save network bandwidth.

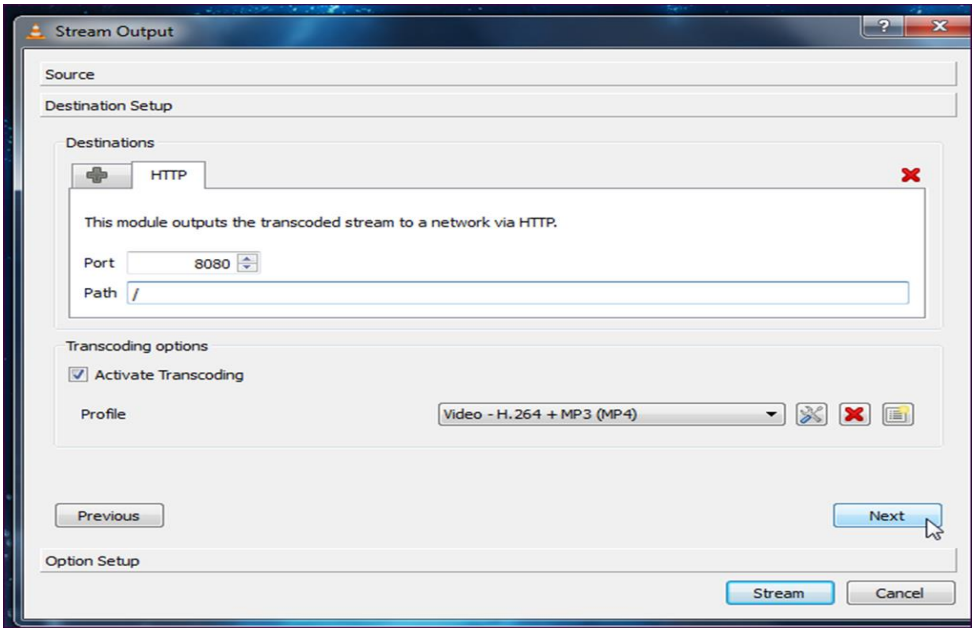


Figure 5.33: step 5

Click Next to continue to the Option Setup pane – you probably don't need to tweak any of the advanced options here. To start streaming, click the Stream button.

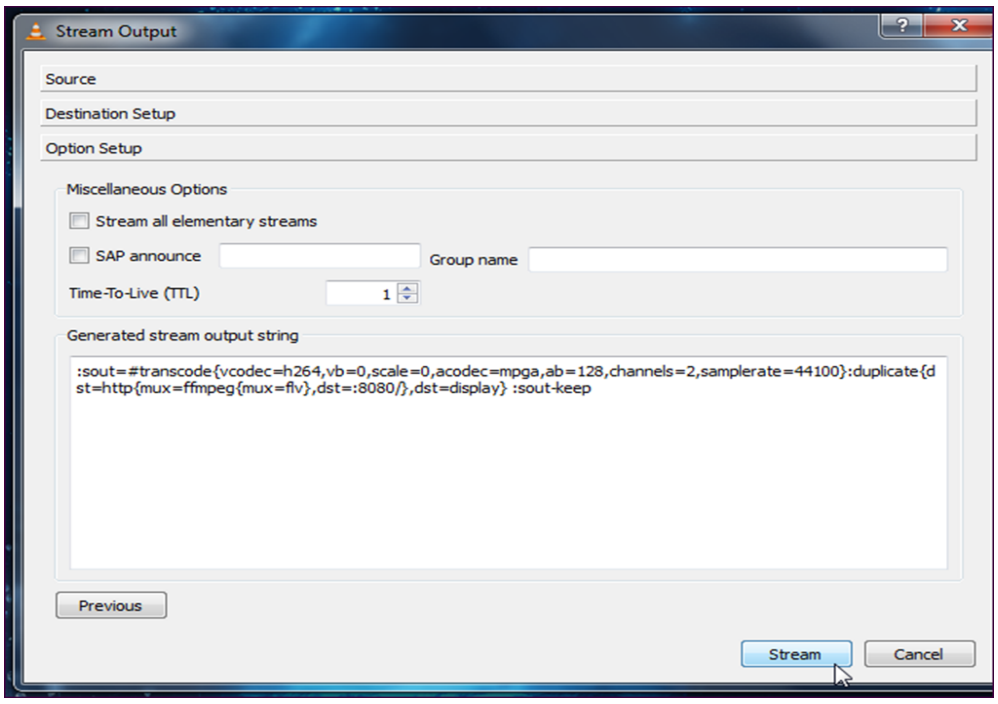


Figure 5.34: step 6

If you selected the Display locally option, the media will start playing locally on your computer.

If you have a firewall enabled, ensure that VLC is an allowed program or no computers will be able to connect. If you're trying to stream over the Internet, you may also need to forward ports on your router.

VLC Streaming is ready now.

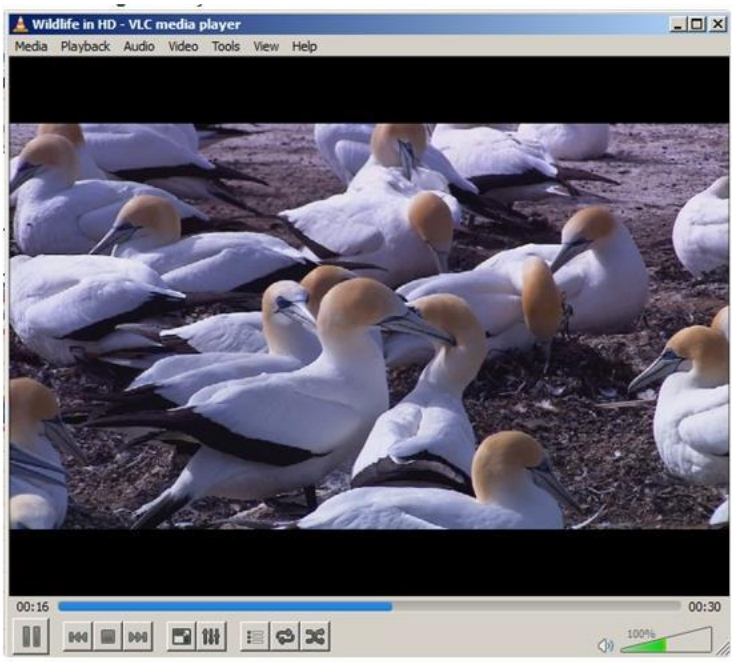


Figure 5.35: VLC streaming

Finally, connect any laptop or cellphone with IP address as shown in Figure 5.43

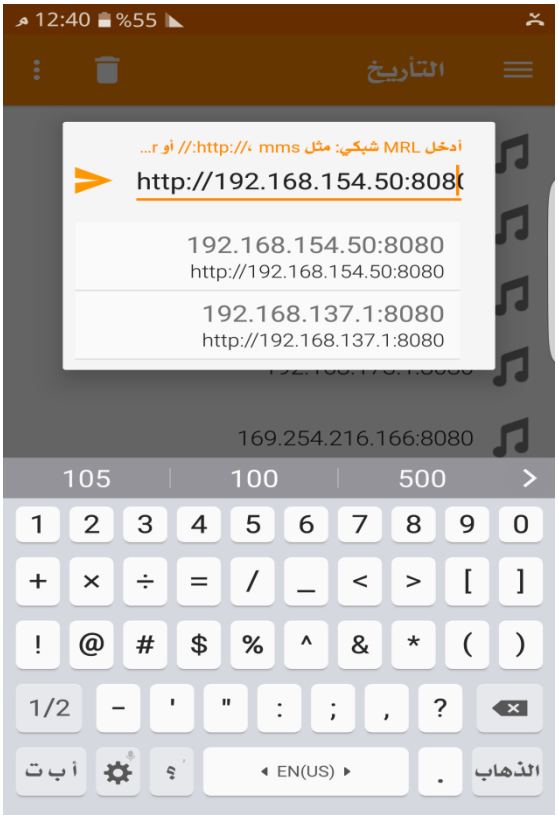


Figure 5.36: The connection for cellphone with IPTV network

In conclusion, there were many obstacles that had faced us.one of them is that our devices did not support installation for the required software that we should use to make voice over IP call ,because their systems were windows 8 . So we upgrade windows 8 to 10 to install the program that support VOIP call. After solving this problem, VOIP calling was passed successfully. then IPTV and VOIP have been connected at the same network,

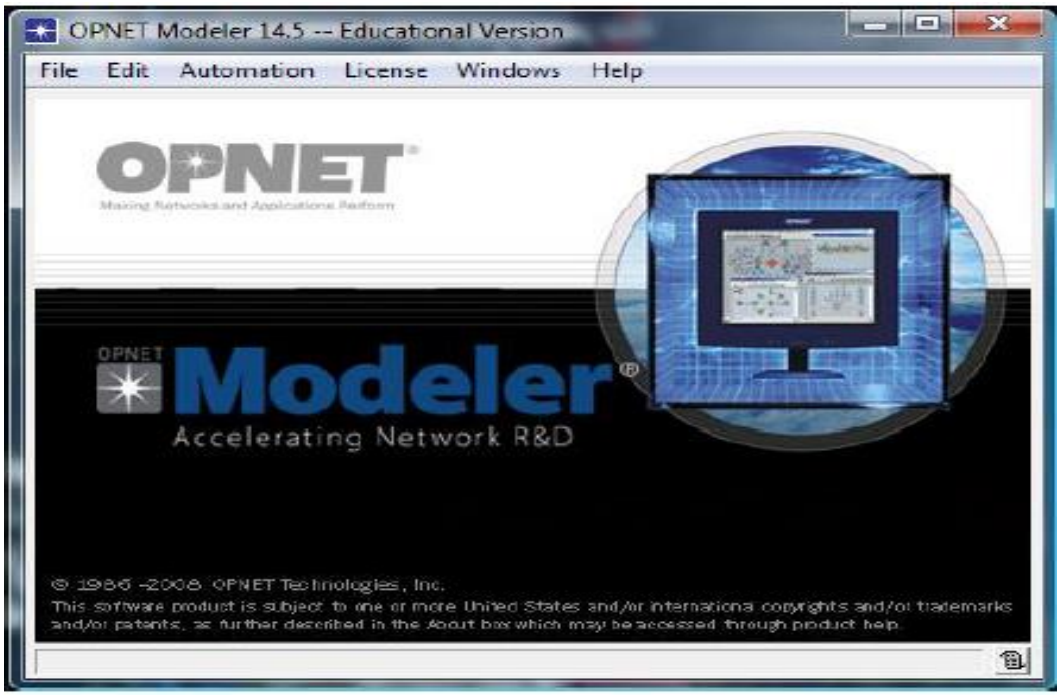
The result of passing VOIP calling and IPTV had low delay, And multimedia (voice and video) had good quality.

Chapter 6
VOLTE

6

6.1 OPNET simulator:

OPNET simulator is a tool to simulate the behavior and performance of any type of network. The main difference with other simulators lies in its power and versatility. This simulator makes possible working with OSI model, from layer 7 to the modification of the most essential physical parameters.
This chapter will show how can we simulate the projects by using opnet modeler 14.5.



6.1.1 Scenarios:

Two scenarios utilize tow cases.

1) Connection between ims core network and volte
2) Connection between ims full network and volte

Both simulations utilized the following variation:

- Throughput:

  Throughput is a measure for computing the actual speed of sending data through a network.

- Delay (latency):

Delay is a measure for computing the time consumed in transferring an entire message to its destination, starting from the time that the first bit is sent out from the source.

- Jitter:

Jitter is a variation of the delay time of sequent packets. Jitter significantly affects real-time, delay-sensitive applications, such as voice and video. A small amount of jitter may be acceptable, but if its amount increases, then delay-sensitive applications will be adversely affected and will become useless. Jitter is measured by computing the difference in the delay of packets over a certain period.

- Voice application:

Voice application is variation of voice during the transition from cell to another.

6.2 Opnet LTE simulation:

Opnet lte simulation mobile communication systems are deployed as a natural evolution of GSM (Global system for mobile communications) and UMTS (Universal Mobile Telecommunications System). LTE is a 4G wireless technology that Verizon Wireless and numerous leading wireless carriers have chosen as their upgrade path beyond 3G technologies. Verizon Wireless will operate LTE in the 700 MHz spectrum, which translates to unprecedented performance and data access.Voice over LTE (VoLTE) has emerged as the leading solution for delivering voice services. In this project, we simulated voice calls with varying amounts of network congestion, and analyzed the impact this had on packet loss, end-to-end delay, jitter, and mean opinion score. We found that only extreme amounts of congestion caused significant amounts of packet loss, that delay increases exponentially with congestion, that jitter is practically unaffected by congestion, and that mean opinion score suffers significantly with increased congestion.Simulation of VoLTE services is performed utilizing OPNET Simulator 14.5 software tool, depending on Discrete Event Simulation (DES) method. However, aim of this work is to examine only effect of several voice coded on end-to-end performance of VoLTE, Type of Service (ToS) assumed is only Best Effort (BE). Volte cannot be shown by opnet 14.5 modeler so the simulation will be deliberated as voice over wimax and the parameters will be altered as volte [15].

6.2.1 Requirements of LTE opnet simulation:

- Enhanced multimedia broadcast multicast service
- Less than 5 ms user-plane latency
- Peak data rate-100 mbps DL/ 50 mbps UL within 20 MHZ bandwidth
- Spectrum flexibility is up to 1.25 ~20 MHZ.
- Up to 200 active users in a cell

- Enhanced support for end-to-end QoS

6.2.2 Features of LTE opnet simulation:

- Support for both FDD and TDD
- Use multiple access scheme like SC-FDMA and OFDMA with CP
- H-ARQ, mobility support, rate control, security etc
- Use adaptive modulation and coding
- Advanced MIMO spatial multiplexing techniques etc[17].

6.2.3 Advantages of LTE opnet simulation:

- Reduces cost per bit through improved spectral efficiency
- Offers easier access and use with greater security and privacy
- Supports real-time applications due to its low latency
- Dramatically improves speed and latency
- Creates a platform upon which to build and deploy the products and services of today and those of tomorrow

Delivers enhanced real-time video and multimedia for a better overall experience[16].

6.2.4 Simulation goals:

The mean goalmouth of the simulation is to essence about the connection between YM and PTC by VOLTE and to study the sending and receiving voice calls, throughput ,delay and jitter between BSs and SS.

Opnet modeler 14.5 does not support VOLTE. So Voice over LTE will be configured as voice over wimax as shown below .

6.3WiMAX Modulation Techniques

The main objective of this work is to study and analyze the performance of VoIP over WiMAX networks. A second objective is to study the WiMAX (IEEE 802.16e) standard with QoS features. Accordingly, we briefly reviewed VoIP technology and its main features to identify the best methodology for designing a model. Furthermore, we simulated the WiMAX network model by using different scenarios that addressed QoS classes, number of users, and voice codecs.

6.3.1 Experimental Network Configuration

The configuration details of the simulation components are described in this section. These components include the WiMAX network model, BSs, and SSs. The network consists of seven coverage cells that are controlled by a WiMAX node. Each cell

contains one BS and five SSs, as indicated in Table 6. The BSs are linked to the core network via an IP backbone. The cell radius in the simulated network is 1 km and voice calls with public switched telephone network quality are configured among mobile nodes. Transmission power is set to 0.5 W, with reference to the subscriber node.

-The network can be done as following:

- Topology
- Deploy wireless wizard
- Then you can follow these steps:

6.4 Voice over LTE simulation scenario:

The scenario will explain the case of connection between YM and PTC.

The connection includes the core of IMS that can be provided by PTC, and wimax network as LTE network that can be provided by YM as shown in figure 9.1.

Component	Value
Network	4 cells
Cell Radius	1 km
No. of Base Stations	4 station
Simulation time	240 s
No. of Subscriber Stations per BS	1 station
Base Station Model	wimax_bs_atm_router_adv
Subscriber Station Model	wimax_ss_wkstn_mobile
Voice Server Model	sip server
Link Model (BS-router)	ppp_adv
Link Model (server – router)	1000base t

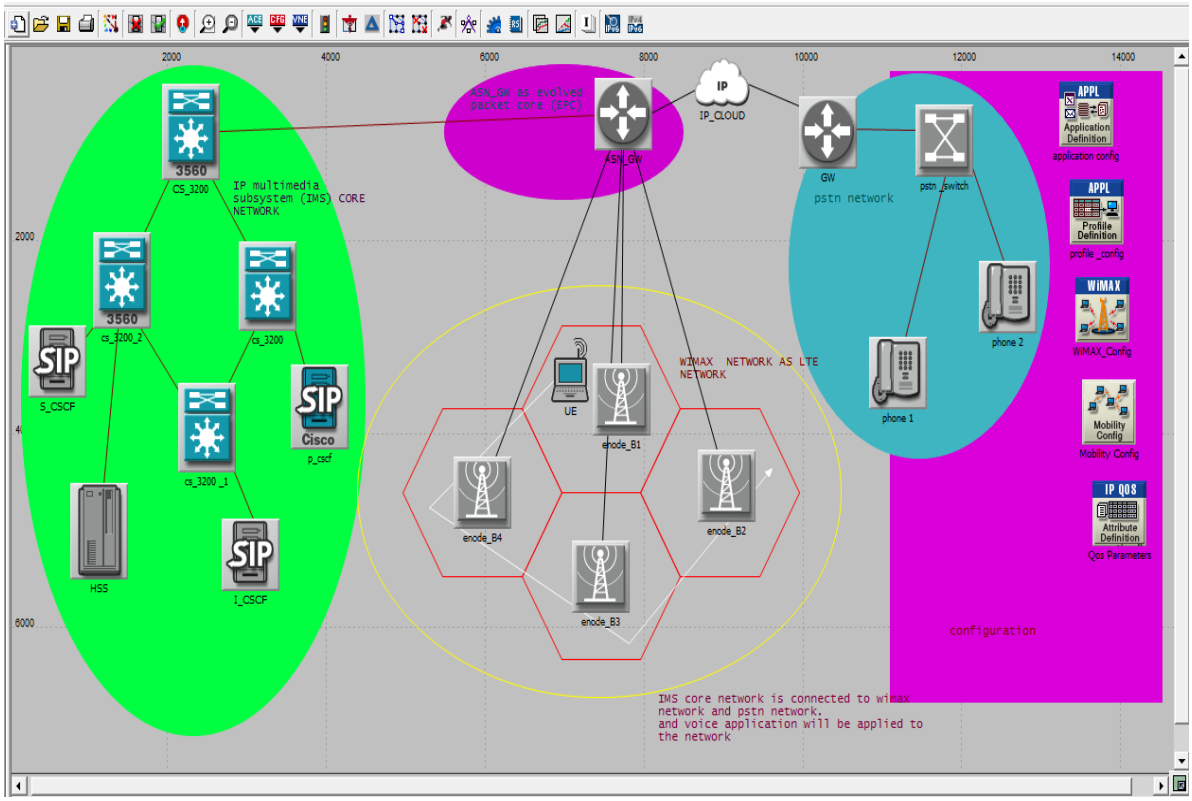


Figure 6.1: The core of ims and wimax network (as LTE network) and pstn .

For PSTN network as example consist from PSTN switch and two phones.
The configuration for phones will be in profile and application configuration.
The trajectory path will be calculated and it is Accum Time=46m19.39**.**that will show in the following figure 6.2:

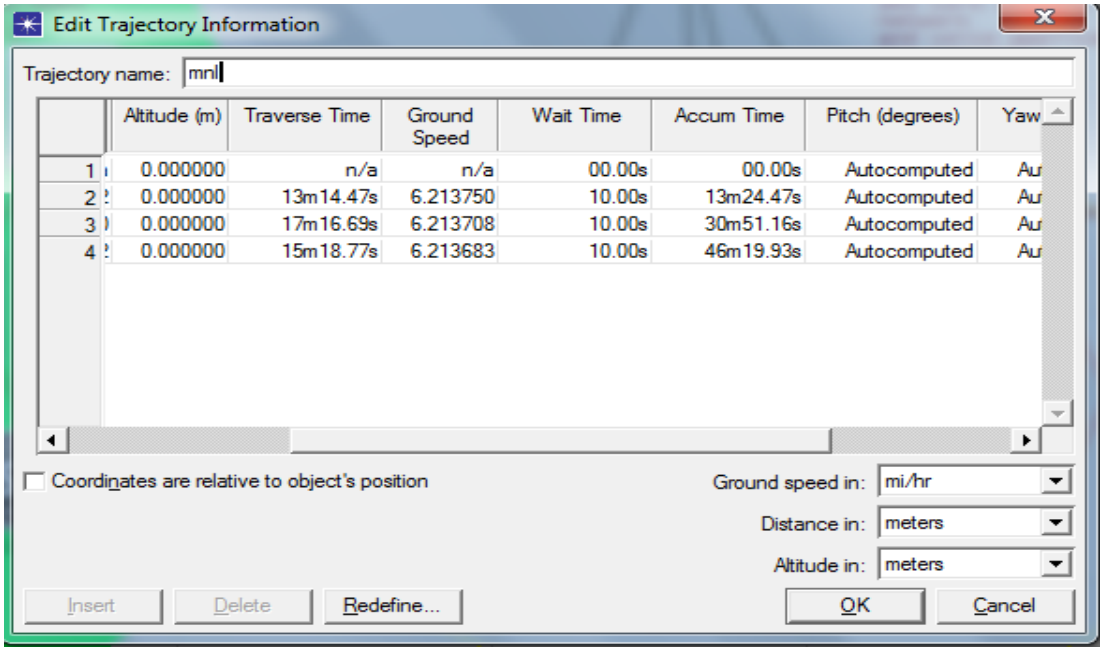


Figure 6.2: The trajectory path**.**

The application configuration: describe the application that can be applied to the network. Figure 6.3 shows the application is voice, the description will be PCM Quality Speech, it can be configured as following:

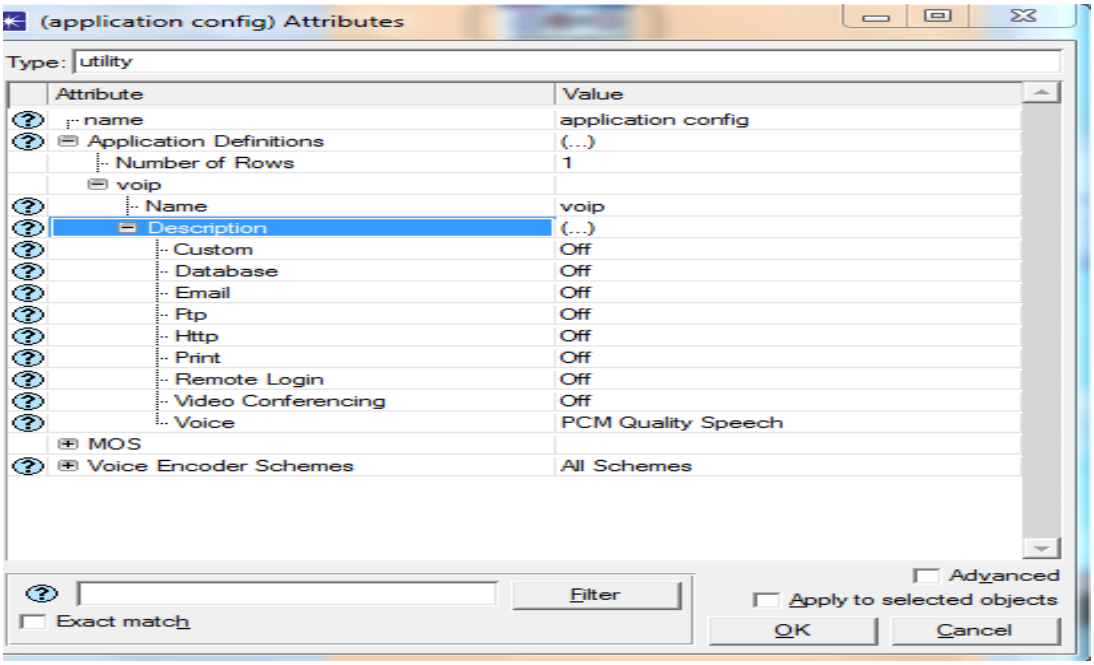


Figure 6.3: The application is voice, the description will be PCM Quality Speech

The profile configuration will indicate to voice application as following:

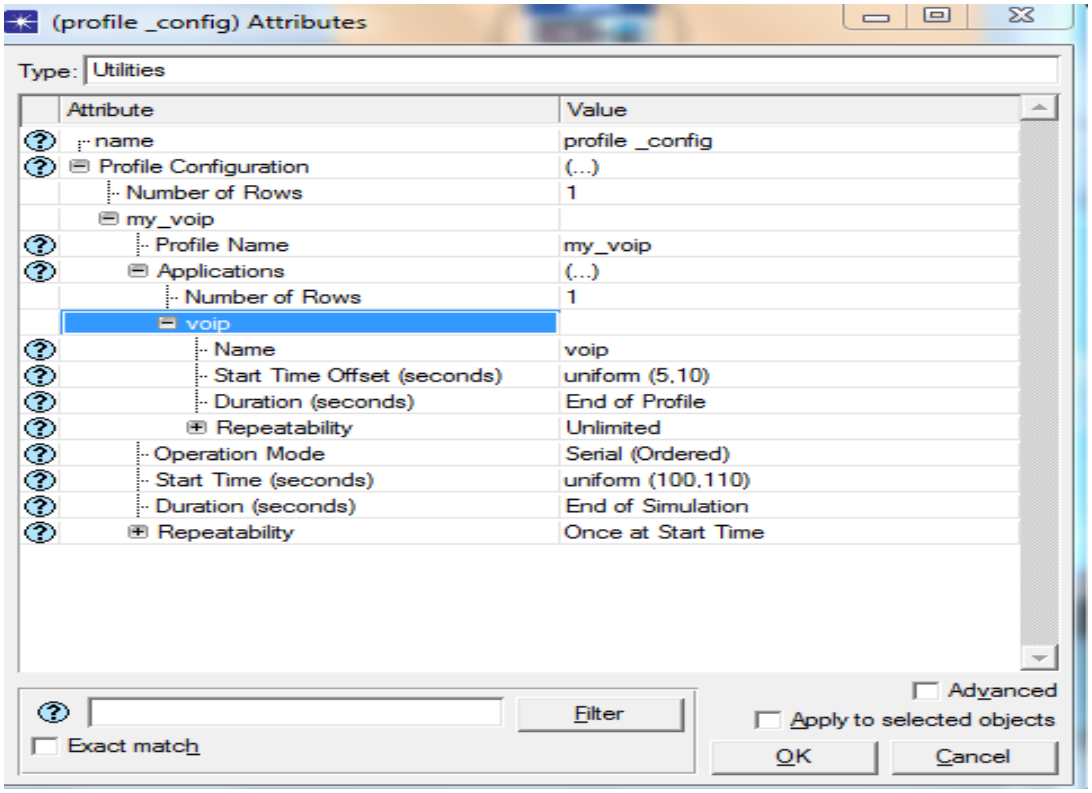


Figure 6.4: The profile configuration

Wimax configuration will be as following:
the service class name will be Gold as shown in figure 6.5, that means all the enode_Bs and UEs should have the same name .

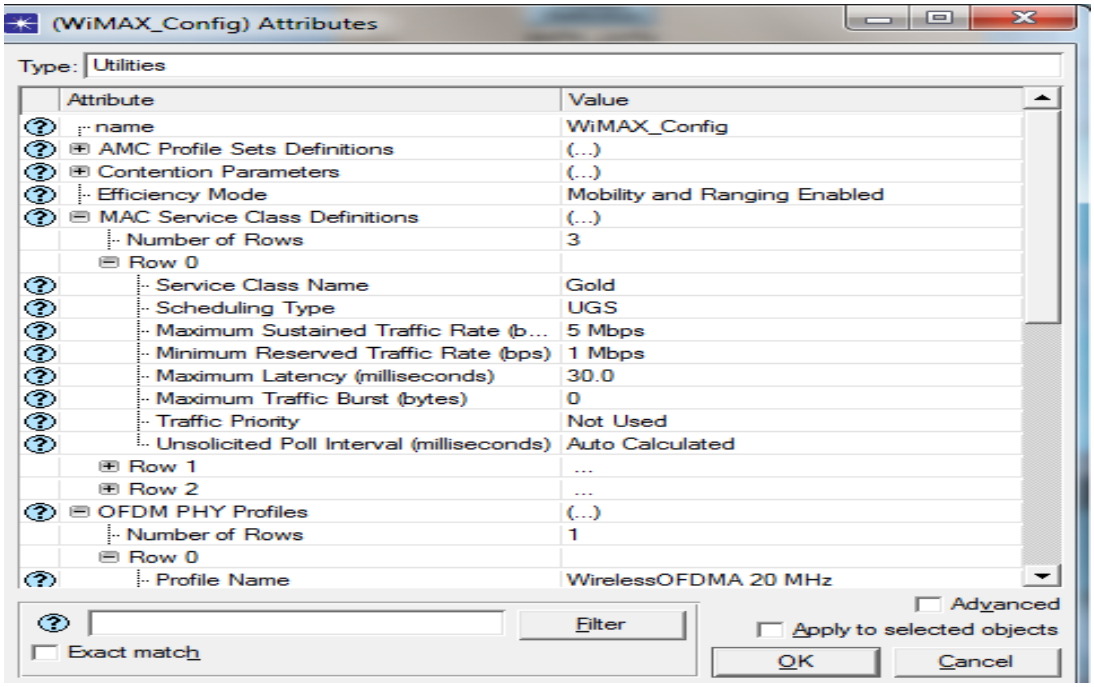


Figure 6.5: The service class name will be Gold.

As shown in figure 6.6 base frequency will be 10 GHz, and the bandwidth will be 50MHz in order to transform the wimax in to LTE. In addition, the duplexing technique will be FDD.

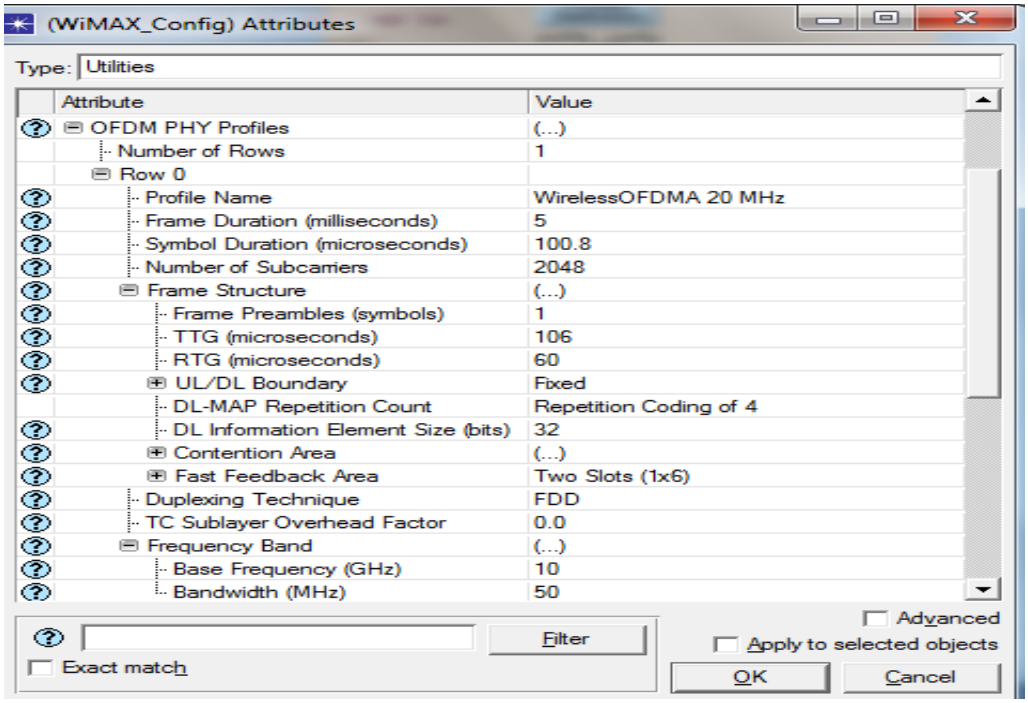


Figure 6.6: Base frequency will be 10 GHz, and the bandwidth will be 50MHz .

ASN _GW router for wimax will be configured as following:
From the IP routing parameters, select the interface IF0 and put IP address and the class as shown in figure 6.7. All eNodeBs should have the same gateway of the ASN_gw router.

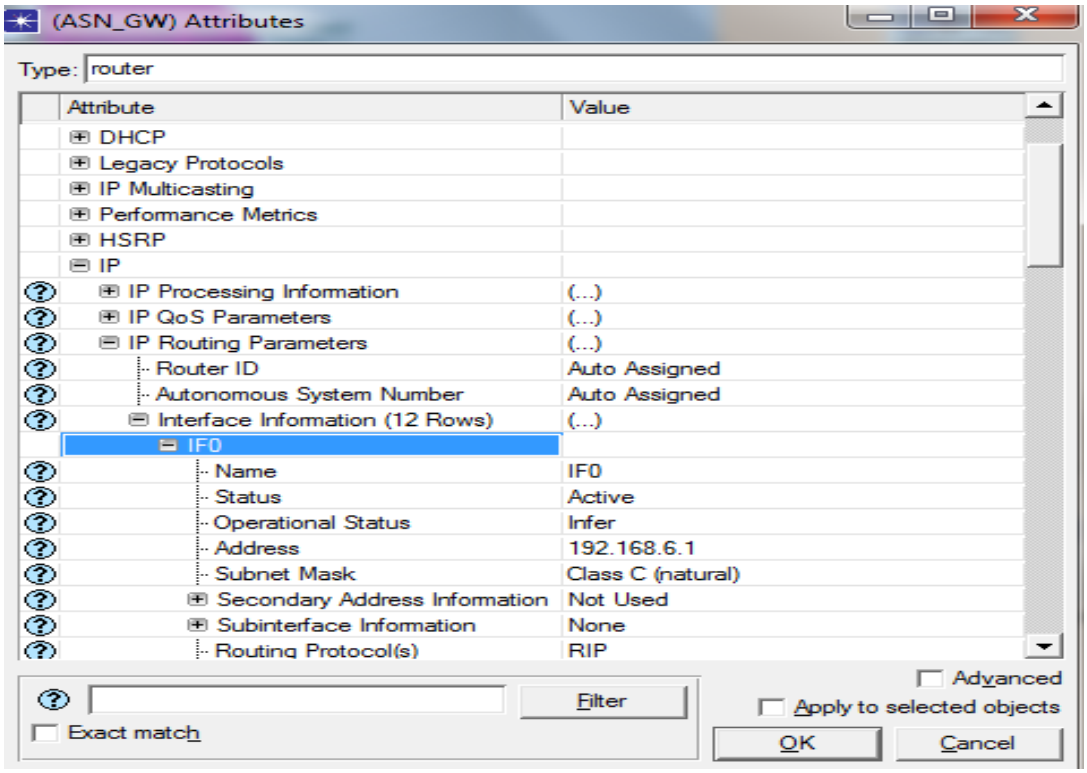


Figure 6.7: ASN_GW router (Ip address and the class) .

The eNodeB will be configured as following:
The number of transmitters STC&MIMO, and the gateway is ASN-GW IP address as shown in figure 6.8.

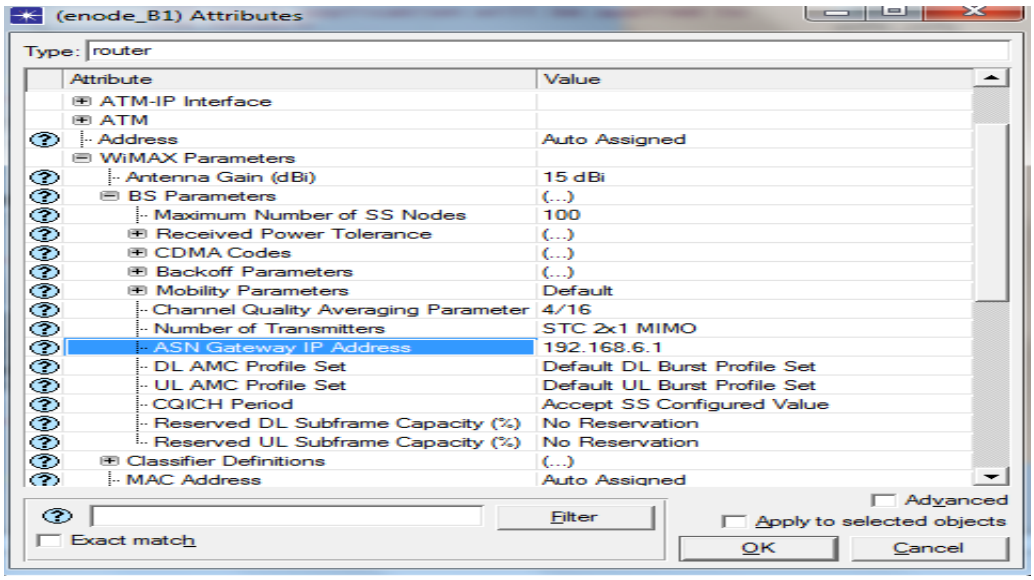


Figure 6.8: Number of transmitters STC&MIMO, and the gateway is ASN-GW ip address

As shown in figure 6.9 For The classifier defination the class name will be Gold.

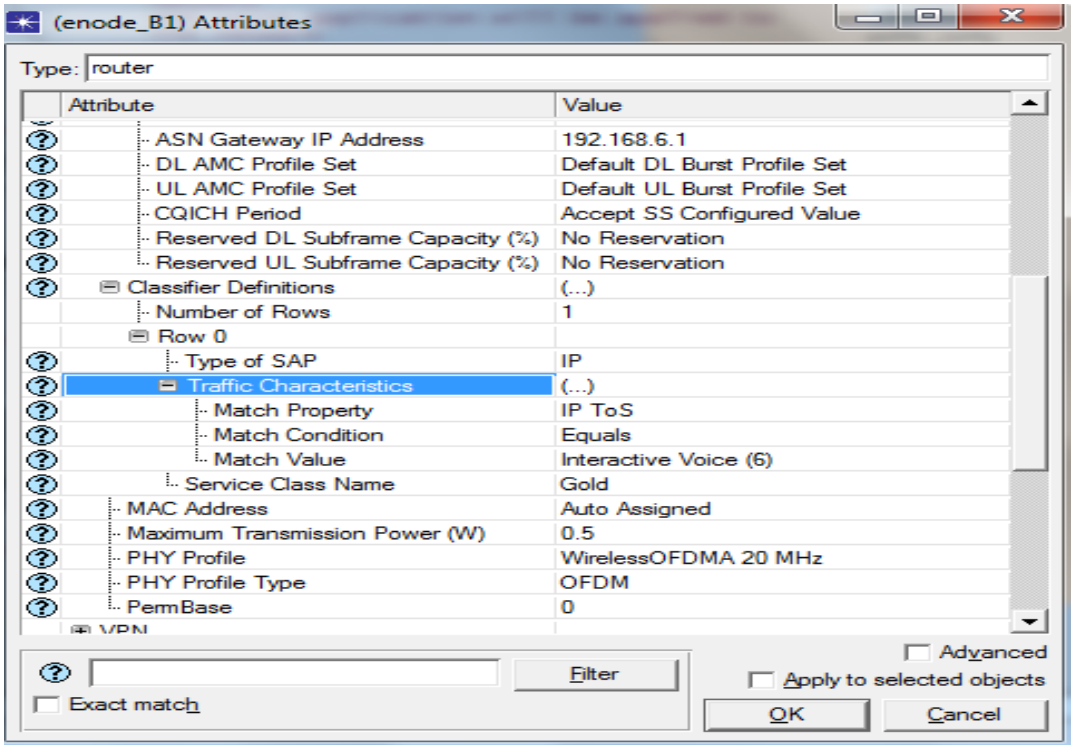


Figure 6.9: For The classifier defination the class name will be Gold

User equipment configuration will as following:
The class name will be Gold and the match value will be interactive voice as shown in figure 6.10. Also this can be done for both uplink and downlink.

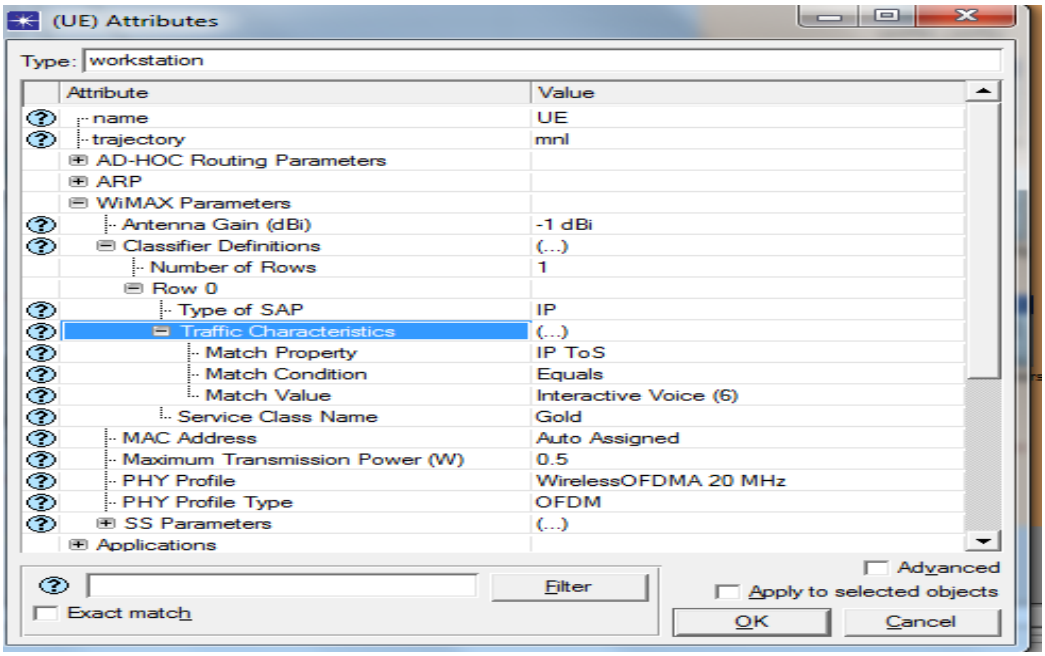


Figure 6.10: The class name will be Gold and the match value will be interactive voice

Figure 6.11 shows the application configuration voip and profile configuration my_voip.

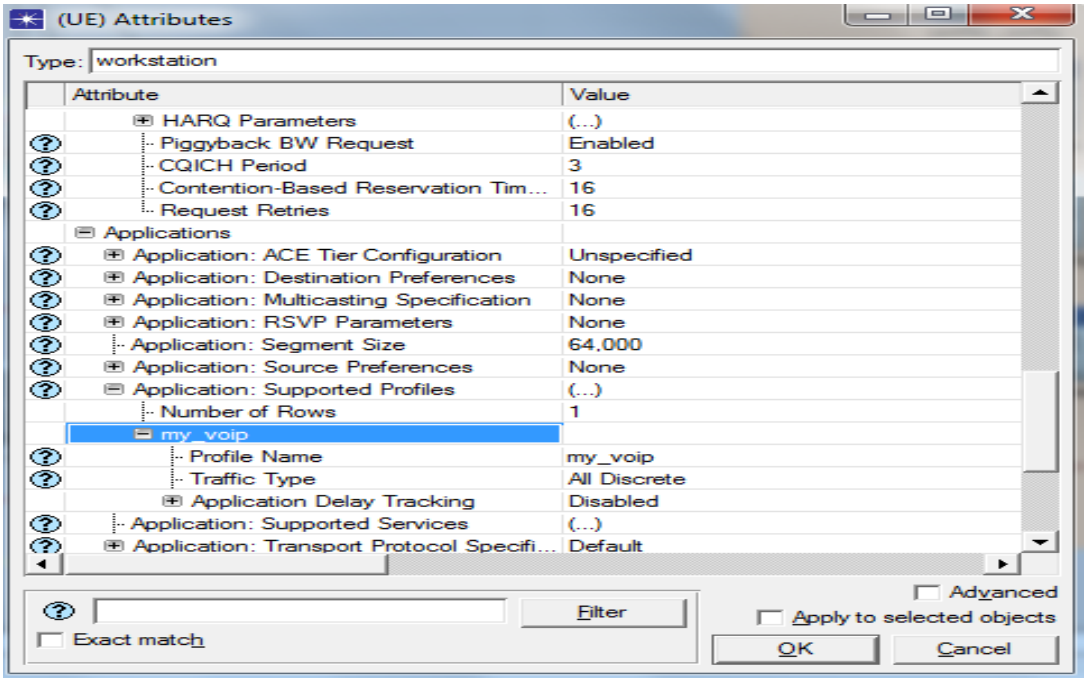


Figure 6.11: The application configuration voip and profile configuration my_voip**.**

Choose result:

Choose result will be according to the voice application and wimax as shown in figure 6.12 , you can choose result according to your studying search .

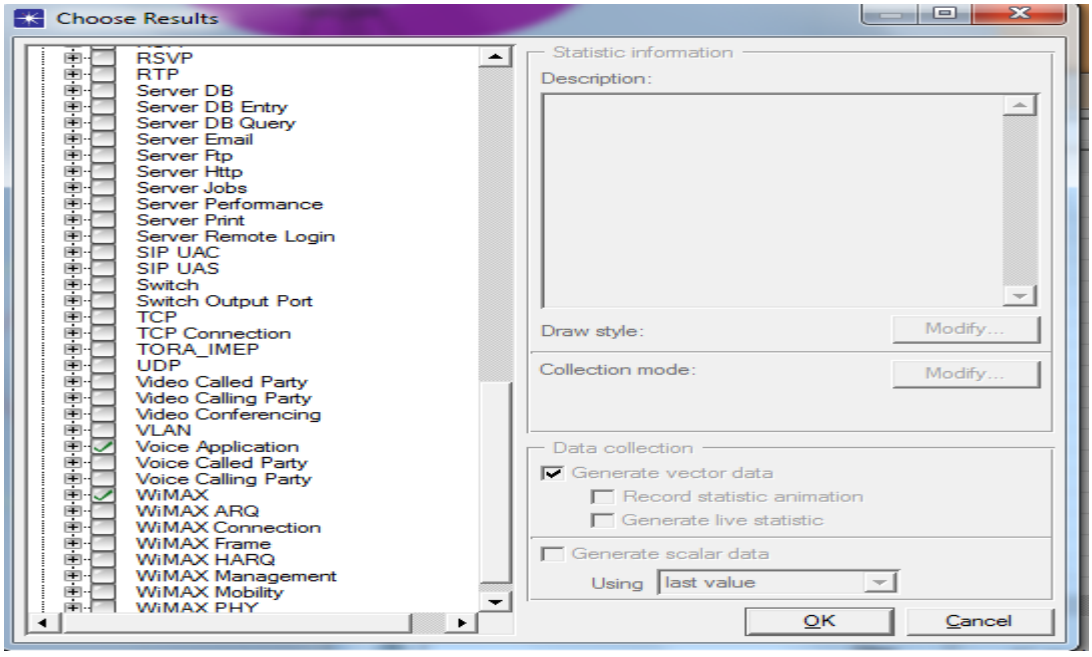


Figure 6.12: The choosing result will be according to the voice application and wimax

*For IMS core network, SIP servers will be configured as following:
Choose the sip type, and configured the application as voice as shown in figure 6.13.

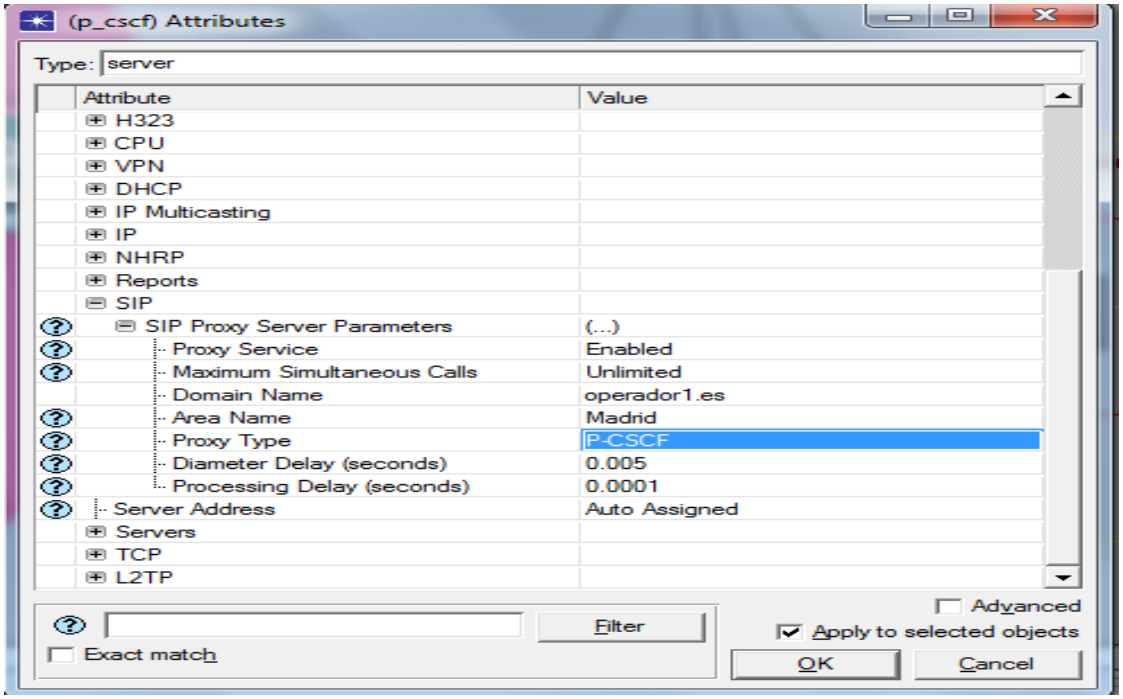


Figure 6.13: Sip type

The first scenario's packets stream will be as shown in the figure:

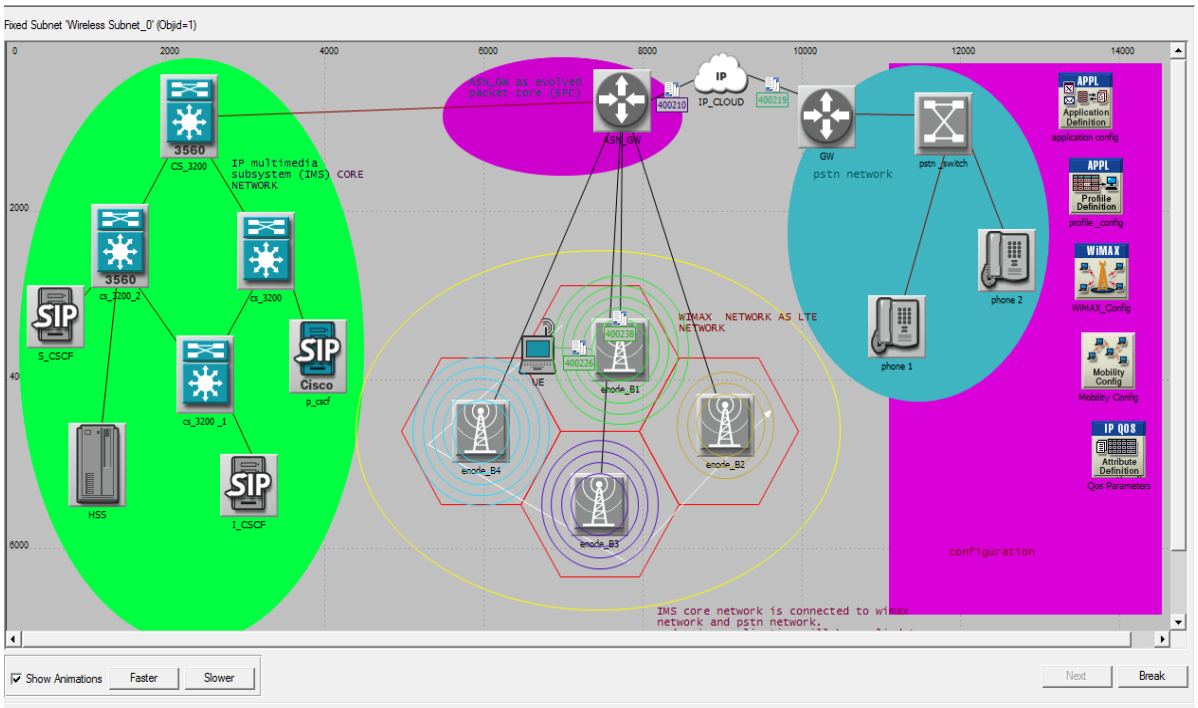


Figure 6.14: The packet stream.

The reasult for the simulation of first scenrio will be as following :

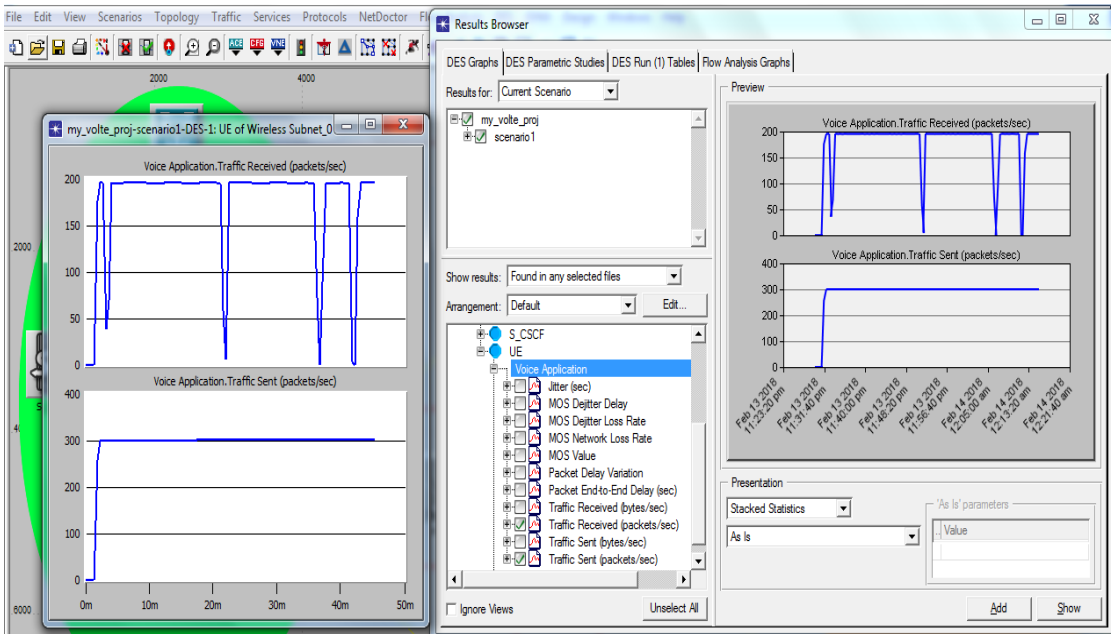


Figure 6.15: The transition between the cells, from cell to another cell.

The simulation shows in figure 6.15 the transition between the cells, from cell to another cell. For the voice application traffic received (packet/bits) the drop of signaling indicates to handover .That means the voice will be low at this moments.

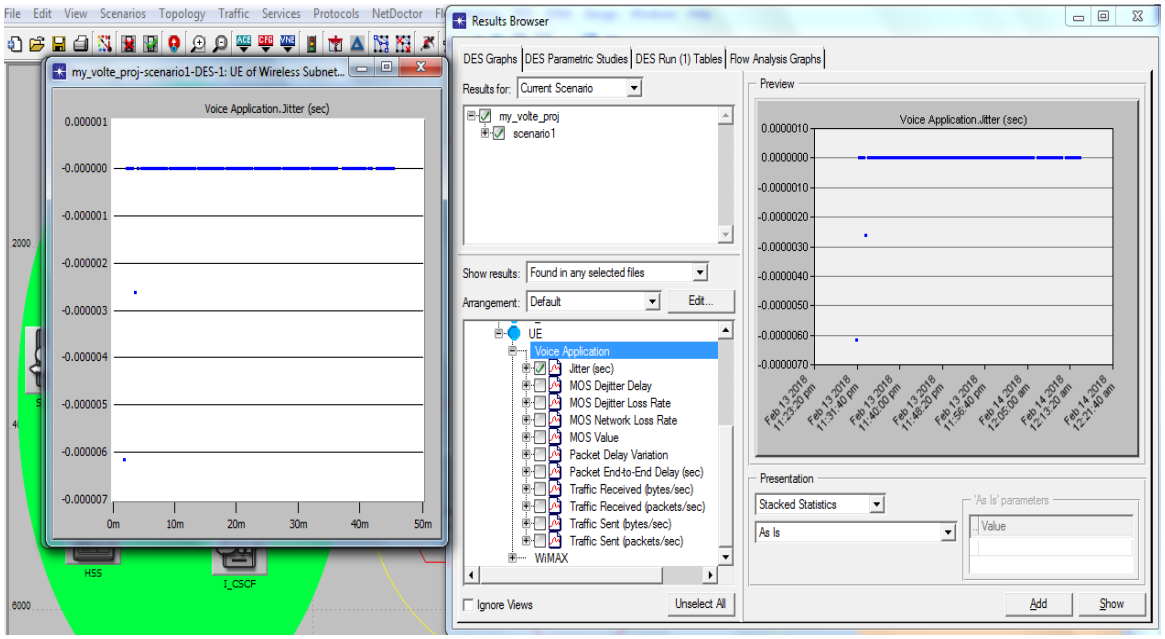


Figure 6.16: The jitter.

From the figure 6.16 the jitter will be low**.** From the figure 6.17 the packet delay will be at very low and that indicate at the following distances 7m, 23m, 38m, and 43m.

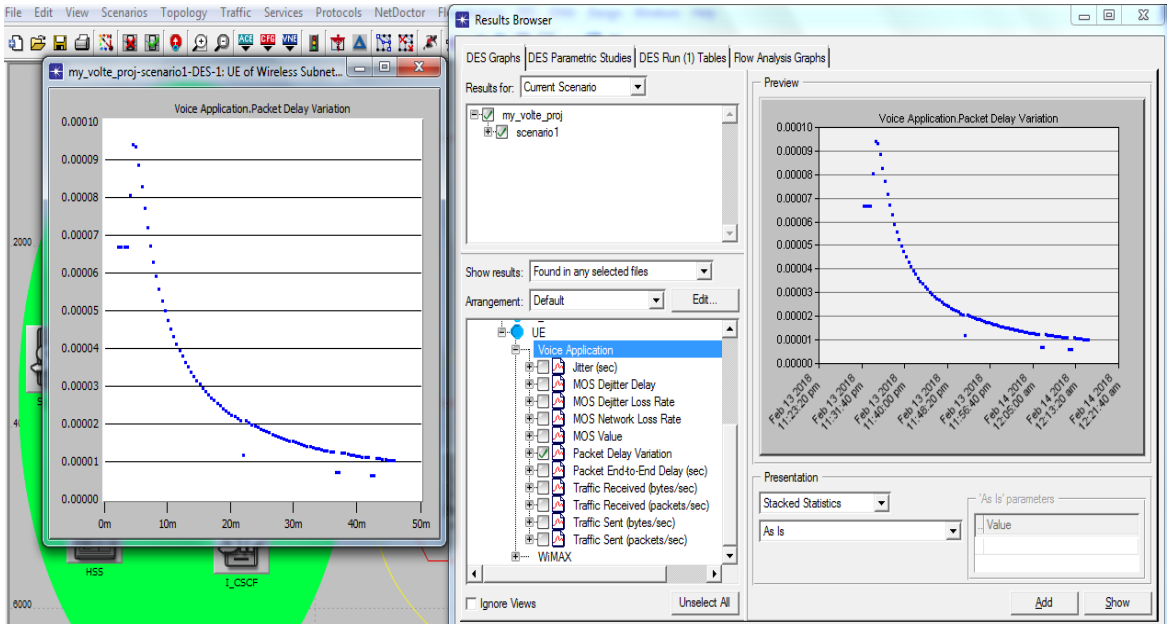


Figure 6.17: The packet delay will be low.

The simulation for wimax end user's delay will be as shown in figure 6.18. The delay will be at the first of the movement.

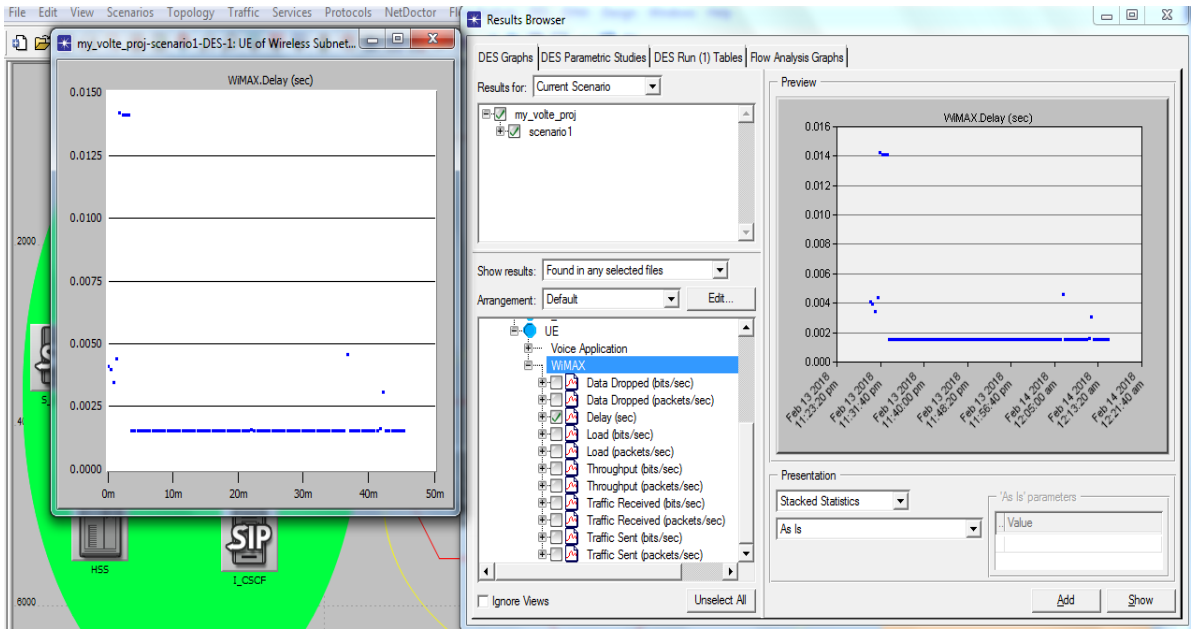


Figure 6.18: The delay at the first of the movement.

The throughput will be indicate in figure 6.19 .the throughput will be high.

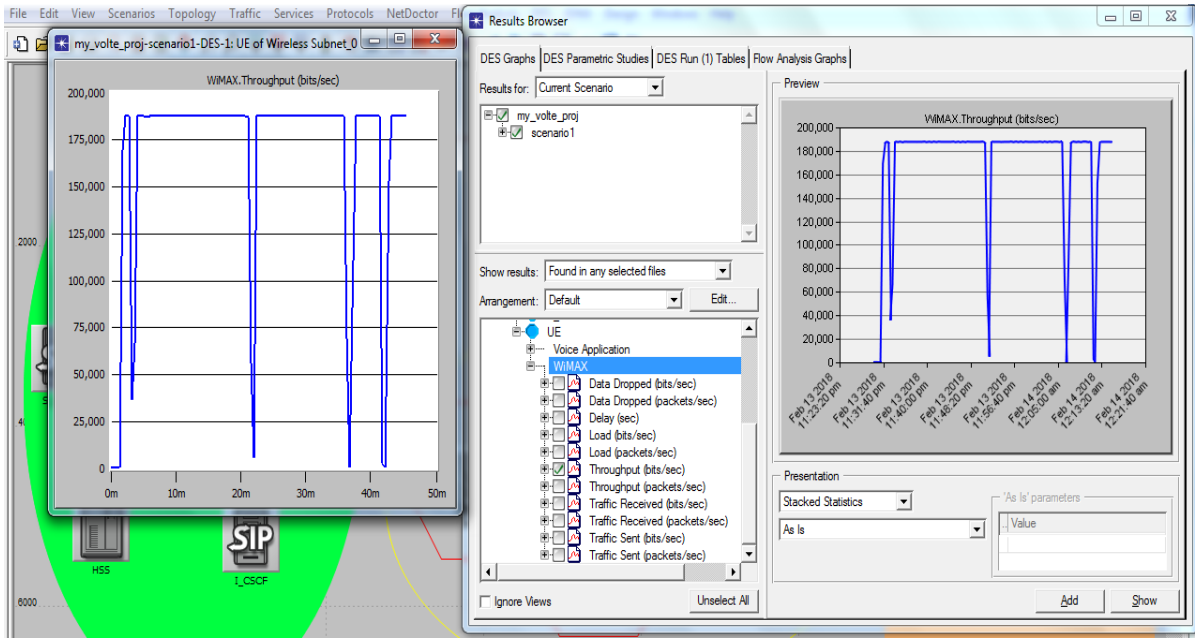


Figure 6.19: High throughput

The sending and receiving calls in phones will be shown in figure 6.20, the throughput will be high.

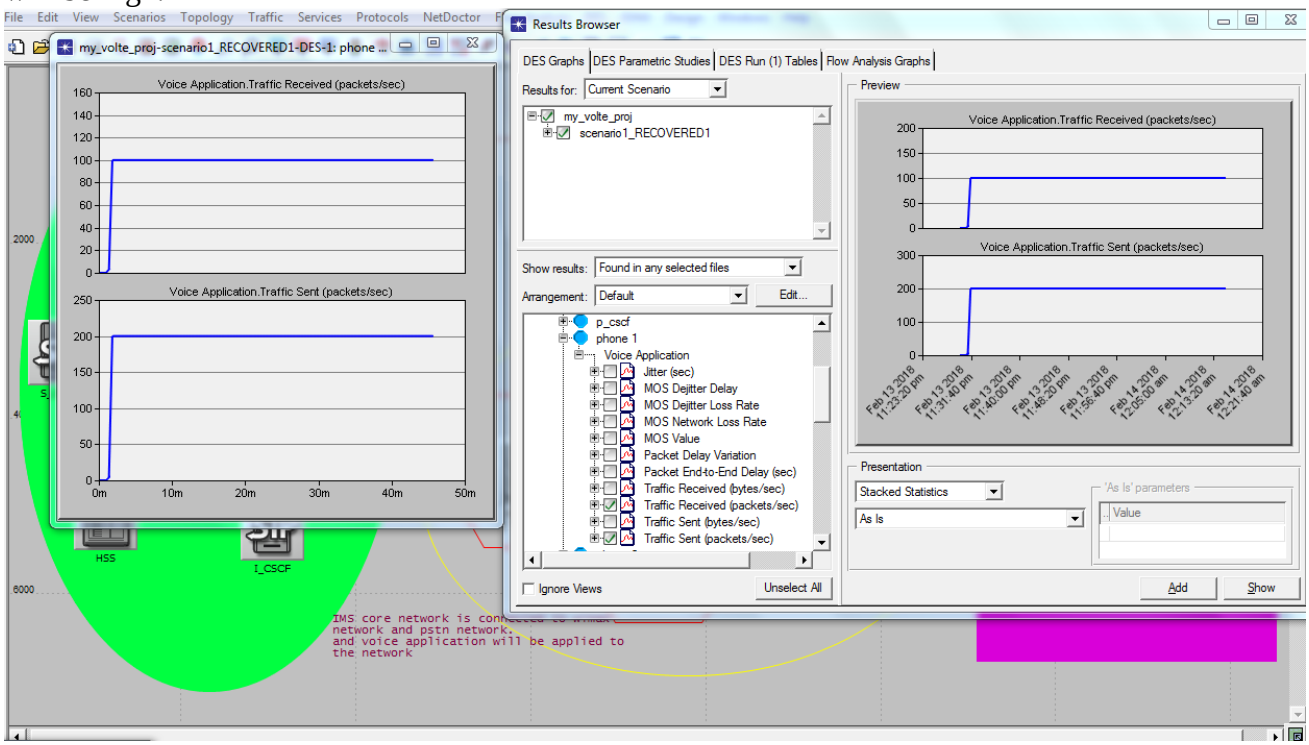


Figure 6.20: The sending and receiving calls in phones

Case Study

IP Multimedia Subsystem scenarios:

IP multimedia subsystem is an architecture for real time multimedia (voice, data, video, messages) services over IP network. These services will be developed each year.

According to the connection between Public Telecommunication Corporation (PTC) and Yemen Mobile (YM) have three scenarios:

1. Upgrade from NGN to IMS
2. Convergence
3. New IMS

In general, they need full configuration of IMS with its complexity of convergence and interconnection with other operators (MTN, SAPAPHONE…) through sip and ss7.

1. Upgrade NGN to IMS:

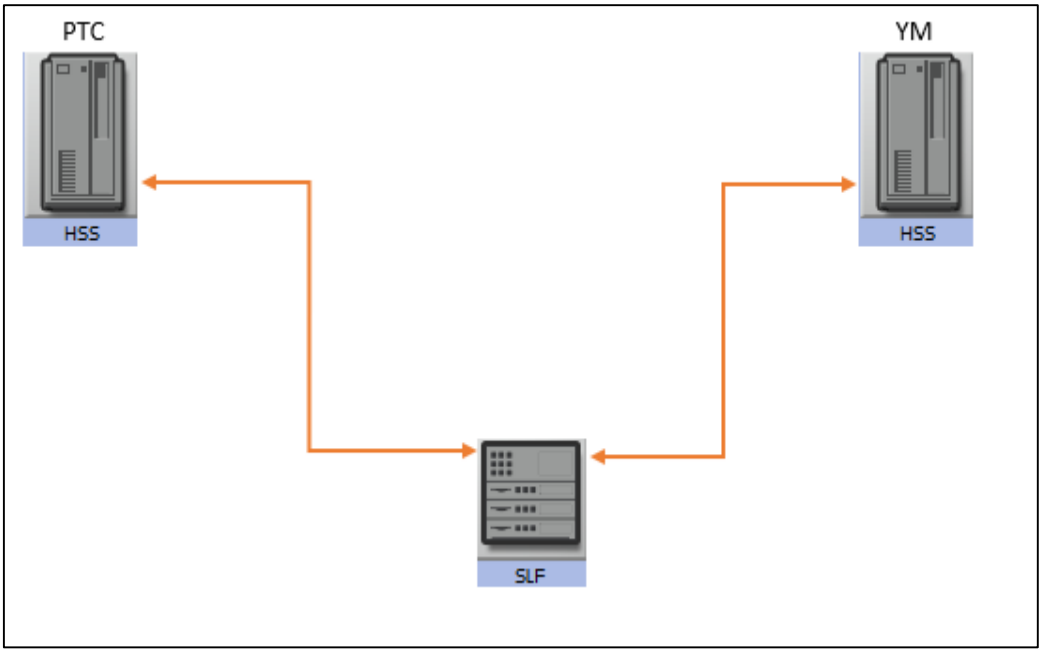
The upgrade from NGN (next generation network) to IMS will be upgrading for some components and the other components will be new. The cost for upgrading to IMS will be about 70 % from the total cost of new IMS. In addition, for that the NGN system will end after two year. So NGN will not be used.

2. The convergence

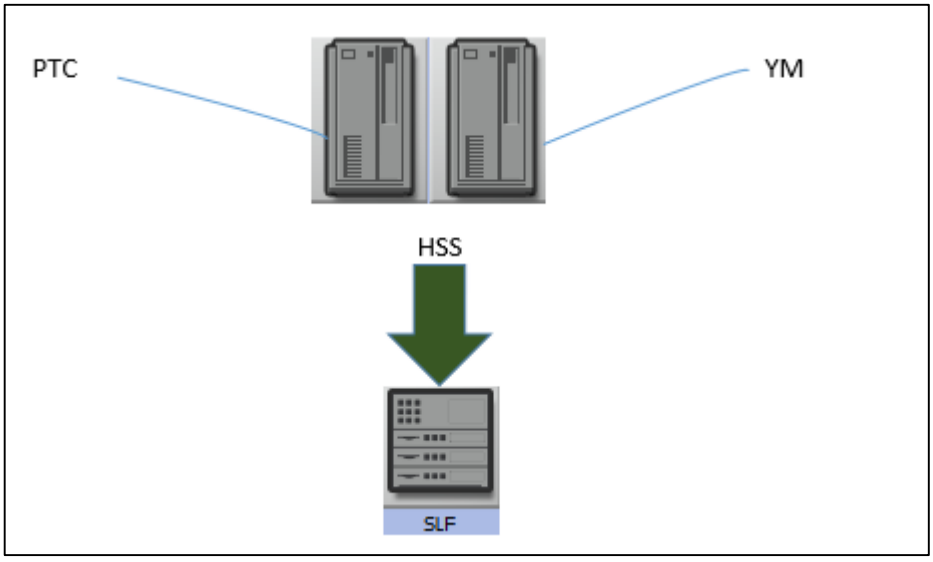
In case of convergence between YM and PTC, the configuration will be as following: One core (with two domain), these two domains are detailed as:

A. HSS

1. One HSS (AS) for each with SLF: the subscriber location function (SLF) can decide the location of SBs.
One HSS will take 1 or 2 million subscribers and the cost will be according to the companies that offer 1 or 2 dollar(s) for one number.



2. One HSS with two domains:



B. SBC:

1. One SBC (session border controller) for each YM and PTC:

It is as BGW (boarder gateway router with its firewall), SBC decide the numbers which one is mobile and which one fixed, and decide the MSAN (multi-service access network)

2. One SBC with two domains (one for YM and one for PTC) .

C. PCRF:

1. One PCRF (policy and charging rules function) for each or one PCRF with two domains.

In PTC we need the following entities (MGCF, AGCF, IM-MGW) which AGCF and MSAN can be connected though H248, and MGCF can be used to connect the other network such as circuit switch.

YM will not use those components; just they use RAN (radio access network).

In case of convergence:

1. There will be one EPC (evolved packet core)

2. YM should upgrade radio access network to eNodeB.

3. In real case: both YM and PTC:

1. Two new IMS cores with their AS.

2. PTC needs MVNO (multi virtual network operator) gateway.

3. YM needs VNO (virtual network operator).

4. YM will upgrade RAN to eNodeB.

CONCLUSION

IMS, or IP Multimedia Subsystem is having a major impact on the telecommunications industry, both wired and wire-less. It was one of the most important technology that can be connected to legacy systems and the will support the development of networks.

VoLTE is the first major IMS related application being rolled out on a large scale and the stakes are high. The combination of IMS, SIP and RAN features are essential in delivering the “carrier-grade” VoLTE experience.

Our project has as goal to analyze QoS of VoIP with IPTV and VOIP with LTE in LTE network (VoLTE), and it has goal to analyze throughput and delay over both networks.

We faced some difficulties in using voip-emulator for our study because the software has a large capacity. The practical part of IMS shows the results of simulation and emulation for VOIP and VOLTE, and these results show the delay would be low and the quality of voice is good. Moreover, the implementation of IMS infrastructure, which is presented in VOLTE simulation, was very useful for us to understand both the registration of a UE and the call flow between two users in IMS.

Abbreviations

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
ARR	IPv4 address resource record
AAAA RR	IPv6 address resource record
AAA	Authentication, authorization and accounting
AAL	ATM adaptation layer
ACA	Accounting-Answer
ACR	Accounting requests
ADSL	Asynchronous Digital Subscriber Line
AH	Authentication header
AKA	Authentication and key agreement
AMR	Adaptive multi-rate
AOR	Address of record
API	Application program interface
APN	Access point name
ARIB	Association of Radio Industries and Businesses (Japan)
AS	Application server
ATM	Asynchronous transfer mode
AUC	Authentication center
AUID	Application usage ID
AUTN	Authentication token
AUTS	Synchronization token
AV	Authentication vector
AVP	Attribute value pair; audio video profile

B2BUA	Back to back UA
BCF	Bearer Charging Function
BER	Bit error ratio
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
BNF	Backus-Naur Form grammar
BS	Bearer service; billing system
BSF	Bootstrapping Server Function
BTS	Base Transceiver Station

CAMEL	Customized Applications for Mobile network Enhanced Logic
CAP	Camel Application Part
CCF	Charging Collection Function
CCSA	China Communications Standards Association
CDMA	Code Division Multiple Access
CDR	Charging Data Record
CGF	Charging Gateway Function
CK	Ciphering key
CN	Core Network

COPS	Common Open Policy Service
COPS-PR	Common Open Policy Service Usage for Policy Provisioning
CPCP	Conference Policy Control Protocol
CPIM	Common Presence and Instant Messaging
CPS	Conference policy server
CRLF	Carriage Return Line Feed
CS	Circuit-switched
CSCF	Call Session Control Function
CSCN	Circuit Switched Core Network
CSE	CAMEL Service Environment
CSRC	Contributing source
DDDS	Dynamic Delegation Discovery System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DOI	Domain of interpretation
DOS	Denial of service
DNS	Domain name system
DSL	Digital Subscriber Line
DTMF	Dual-tone multifrequency
EAP	Extensible Authentication Protocol
ECF	Event Charging Function
EDGE	Enhanced Data Rates for Global Evolution
ENUM	E.I64 number
ESP	Encapsulation security payload
ETSI	European Telecommunications Standards Institute
FQDN	Fully qualified domain name
FSM	Finite state machine
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GBR	Guaranteed bit rate
G-CDR	GGSN-CDR
GCID	GPRS charging identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home location register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol

IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICID	IMS charging identifier
I-CSCF	Interrogating-CSCF
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IK	Integrity key
IKE	Internet Key Exchange
IMS-MGW	IP Multimedia Subsystem-Media Gateway Function
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identifier
IM-SSF	IP Multimedia Service Switching Function
IOI	Interoperator identifier
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPsec	Internet Protocol security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRC	Internet Relay Chat
ISAKMP Protocol	Internet Security Association and Key Management
ISC	IMS Service Control
ISDN	Integrated Services Digital Network
ISIM	IP Multimedia Services Identity Module
ISP	Internet Service Provider
ISUP	ISDN User Part
IV	Initialization vector
L1	Layer 1
LCS	Location services
LIA	Location-Info-Answer
LIR	Location-Info-Request
LPDP	Local policy decision point
M3UA	SS7 MTP3-user adaptation layer
MAA	Multimedia-Multimedia-Answer
MAC	Message Authentication Checksum
MAP	Mobile Application Part
MAR	Multimedia-Auth-Request
Mbone	Multicast backbone
MBR	Maximum bit rate
MCC	Mobile country code
MDS	Multimedia Delivery Service
MEGACO	Media Gateway Control Protocol
MGCF	Media Gateway Control Function
MGW	Media gateway function
MIB	Management information base
MID	Media stream identification
MITM	Man in the middle

MIME	Multipurpose Internet Mail Extension
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MNC	Mobile network code
MOBILE IP	Mobile Internet Protocol
MPV	Music photo video
MPLS	//////////
MRFC	Multimedia Resource Function Controller
MRFP	Media Resource Function Processor
MSAN	Multi system access network
MSC	Mobile switching center
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Subscriber International ISDN Number
MSRP	Message Session Relay Protocol
MTP	Message Transfer Part
MTPn	Message Transfer Part level *n*
MTU	Maximum transfer unit
NAF	Network Application Function
NAI	Network access identifier
NAPTR	Naming authority pointer
NAS	Network access server
NASREQ	Network Access Server Requirements
NDS	Network Domain Security
NTP	Network Time Protocol
OCS	Online Charging System
OMA	Open Mobile Alliance
OSA	Open Services Architecture
P2P	Peer to peer
PA	Presence agent
P-CSCF	Proxy-CSCF
PCMU	Pulse code modulation u-law
PDF	Policy Decision Function
PDP	Packet Data Protocol; policy decision point
PEF	Policy Enforcement Function
PEP	Policy Enforcement Point
PIB	Policy information base
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PNA	Push-Notification-Answer
PoC	Push to talk over the cellular service
PNR	Push-Notification-Request
PPA	Push-Profile-Answer
PPR	Push-Profile-Request
PRACK	Provisional response acknowledgement
PRC	Provisioning class
PRI	Provisioning instance
PRID	Provisioning instance identifier
PS	Packet-switched; presence server

PSI	Public service identity
PSTN	Public Switched Telephone Network
PUA	Presence user agent; Profile-Update-Answer
PUR	Profile-Update- Request
QoS	Quality of service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio access network
RAND	Random challenge
RES	Response
RFC	Requests For Comments
RLS	Resource list server
RNC	Radio network controller
ROAMOPS	Roaming operations
RSVP	Resource Reservation Setup Protocol
RTA	Registration-Termination-Answer
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RTP/AVP	RTP Audio and Video Profile
RTR	Registration-Termination-Request
S/MIME	Secure MIME
SA	Security association
SAA	Server-Assignment-Answer
SAD	Security Association Database
SAR	Server-Assignment-Request
SBLP	Service-based local policy
S-CDR	SGSN-CDR
SCF	Session Charging Function
SCS	Service Capability Server
S-CSCF	Serving-CSCF
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SDU	Service Data Unit
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SGW	Signalling Gateway
SHA	Secure Hash Algorithm
SigComp	Signalling Compression
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIPS	Secure SIP
SL	Subscriber locator
SLA	Service-level agreement
SLF	Subscription Locator Function
SMI	Structure for Management Information
S/MIME	Secure MIME
SMG	Special Mobile Group

SNA	Subscribe-Notifications-Answer
SNMP	Simple Network Management Protocol
SNR	Subscribe-Notifi cations- Request
SPD	Security Policy Database
SPI	Security Parameter Index
SPT	Service point trigger
SQN	Sequence number
SRF	Single reservation flow
SRV	Service records
SS7	Signaling System No. 7
SSF	Service Switching Function
SSRC	Synchronization source
TCP	Transmission Control Protocol
TCP/IP	TCP/IP stack
TD-CDMA	Time Division/Code Division Multiple Access
THIG	Topology Hiding Inter-network Gateway
TIA	Telecommunications Industry Association (North America)
TLS	Transport Layer Security
TTA	Telecommunications Technology Association (South Korea)
TTC	Telecommunications Technology Committee (Japan)
TTL	Time to live
TU	Transaction User
UA	User Agent
UAA	User-Authorization-Answer
UAC	User Agent Client
UAR	User-Authorization-Request
UAS	User agent server
UDA	User-Data-Answer
UDP	User Datagram Protocol
UDR	User-Data-Request
UDVM	Universal decompression virtual machine
UE	User equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
UMTS	Universal Mobile Telecommunications System
URI	Uniform resource identifier
URL	Universal resource locator
URN	Uniform resource name
USIM	Universal Subscriber Identity Module
UTRAN	UMTS terrestrial radio access network
VHE	Virtual home environment
VoIP	Voice over IP

WAP	Wireless Application Protocol
WB	Wideband
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XML	Extensible Markup Language
XRES	Expected response

References:

[1] [Telephon] Wiley - The IMS IP Multimedia Concepts and Services in the Mobile Domain.

[2] Mangini, D. (2006). IP multimedia subsystem (IMS): Driving new business models and opportunities.MetaSwitch Networks. IMS architecture. Nortel IP Multimedia Subsystem (IMS) Solution. (2006). Deliver converged multimedia services across

[3] IMS and Legal Interception (IMS) overview and applicationBertrand, G. (2007). The IP multimedia subsystem in next generation networks

[4] G Americas. (2004). IP multimedia subsystem

[5] Russell, Travis, "The IP Multimedia Subsystem (IMS), Session Control and Other Network Operations", McGraw-Hill Companies © (2008).
Copeland, Rebecca, "Converging NGN Wireline and Mobile 3G Networks with IMS", by Taylor & Francis Group, LLC © (2009)
[6] Third Generation Partnership Project (3GPP),Technical specification group services and system aspects; presence service; architecture and functional description,
Cumming, J. (2005). Session border control in IM.

[7] IP Multimedia Subsystem (IMS) Architecture
[8] Next Generation Network
[9] Moray Rumney, « LTE and Evolution to 4g wireless, Design and measurement Challenges », Aglient Technologies, by John Wiley & Sons, July 2009.
[10] « The LTE Network Architecture A comprehensive tutorial », Acatel Lucent white paper, 2009.
[11] Voice over IP over LTE (VoLTE) Impacts on LTE access EFFORT http://www.efort.com
[12] Study Paper on Voice over LTE: New Voice Dynamics by: Wasi Ahmad DDG (LTE -II),Laxmi Dir (LTE), LTE Division, TEC 2016-17

[13] Prasanna Gururaj, Raghavendrarao, « Voice over LTE », Master of Science Thesis, Department of Telecommunications at Delft University of Technology, 2012.

[14] Martin Sauter, « Voice over LTE via Generic Access (VoLGA)», A Whitepaper - August 2009.

[15] Improving the QoS of VoIP over WiMAX Networks Using OPNET Modeler.html

[16] [Opnet LTE Simulation - Opnet LTE Model Simulation]

[17] IMS, Intersystem Handover, Mobile IP, OPNET Modeler, WiMAK