

الجمهورية الجزائرية الديمقراطية الشعبية

**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

وزارة التعليم العالي والبحث العلمي

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

جامعة أبي بكر بلقايد- تلمسان

Université Aboubakr Belkaïd- Tlemcen –

Faculté de TECHNOLOGIE



## **MEMOIRE**

Présenté pour l'obtention du **diplôme** de **MASTER**

**En** : Télécommunications

**Spécialité** : Réseaux et Télécommunications (RT)

**Par** :

YAZID Marwa

SAIM Souhila

**Sujet**

**Etude et mise en place d'une solution IMS  
(IP Multimedia Subsystem) pour la VoLTE**

Soutenu publiquement, le 27 / 06 / 2022 , devant le jury composé de :

Mr BOUACHA. A

Professeur

Université de Tlemcen

Président

Mr BOUABDELLAH. R

Maitre Assistant A

Université de Tlemcen

Examineur

Mr ZERROUKI. H

Maitre de Conférences A

Université de Tlemcen

Encadreur

Année universitaire : 2021/2022

# Dédicaces

*Avec l'expression de ma reconnaissance, je dédie ce travail, A mes parents qu'ils m'ont doté d'une éducation digne, particulièrement à l'homme de ma vie, mon exemple éternel celui qui s'est toujours sacrifié pour me voir réussir, à toi mon père « ABDELKADER ».*

*A ma mère, pour son amour, ses sacrifices et sa confiance.*

*A la source de mes effort, ma sœur « ASMA ».*

*A mes frères qui m'ont toujours soutenu et encourager.*

*A ma grand-mère à qui je souhaite une longue vie.*

*A mes oncles et mes tantes.*

*A mes proches Wahiba , Bessma, Radja, Abderrahmane et TAHA.*

*A la personne qui m'a toujours aidé et accompagné pendant ce parcours, mon collègue « MORTADA ».*

*A mon binôme SAIM SOUHILA pour sa présence, son soutien durant ce long travail.*

*Et à toute la famille « YAZID ».*

**Yazid Marwa**

# Dédicaces

C'est avec un grand plaisir que je tiens à dédier ce travail :

*A mes chers parents*

Pour leur patience, leur amour, leur soutien et leurs encouragements.

*Vraiment* Aucune dédicace ne saurait exprimer mes respects, ma reconnaissance et mon profond amour.

*Que dieu vous protège et vous garde pour nous.*

*A mes frères Walide et Alae*

*A mon neveu Adem*

*A mon oncle Abdelmadjid*

*A mes beaux-frères Mohammed et Riyad*

*A mes sœurs Imene, Anissa et Asma*

*A mes grands-parents à qui je souhaite une longue vie*

*A mes amis Sabrine, Marwa, Bessma, Radjae, Nabila et Wahiba.*

*A toute la promotion Télécommunication 2021/2022 que je leurs souhaite*

*un bon avenir.*

*Enfin a tous les membres de la famille Saim.*

***Saim Souhila***

## Remerciements

*Qu'il nous soit permis d'exprimer nos gratitudees :*

*A ALLAH, le tout puissant, pour nous avoir donné la force, la santé, la volonté et la patience d'entamer et de terminer ce mémoire.*

*Nous tenons à exprimé plus particulièrement notre très profonde gratitude à notre encadreur **Mr ZERROUKI HADJ**, Maitre de conférences à l'université Abou-Bakr Belkaid - Tlemcen, nous le remercions pour son encadrement, son aide, ses conseils précieux, son patience, et sa disponibilité.*

*Nous tenons à remercier les membres du jury: le président de jurys **Mr BOUACHA ABDELHAFIDH**, Professeur à l'université Abou-Bakr Belkaid - Tlemcen, ainsi que l'examineur, **Mr BOUABDELLAH REDA**, Maitre assistant à l'université Abou-Bakr Belkaid - Tlemcen, pour nous avoir faire l'honneur d'être membre de notre jurys.*

*Nos remerciements vont aussi, aux enseignants de notre université et département de télécommunication.*

*Nous tenons fermement à mentionner le plaisir que nous avons eu d'étudier à*

***Université Abou-Bakr Belkaid- TLEMEN.***

*Nous remercions également nos professeurs pour leurs qualité de l'enseignement qu'ils nous prodigué ces cinq ans.*

**Résumé :**

La voix sur LTE ou VoLTE (Voice over LTE) est l'avenir des communications vocales du fait qu'elle soit à base d'IP et de routage IP et compatible avec les réseaux de nouvelles générations. Elle peut également assurer une très bonne qualité de service car un débit de données très élevé est attribué pour chaque paquet IP.

L'objectif de ce projet PFE consiste à simuler un réseau IMS (IP Multimedia Subsystem), qui offre un service vocal tout en se connectant au réseau mobile 4G LTE, à travers le déploiement d'une plateforme "OpenIMSCore" basée sur des solutions Opensource. Cette plateforme a pour but de simulation des fonctionnalités nécessaires à l'établissement de toute session multimédia, et aussi le lancement de tests d'échange de flux de signalisations SIP et d'établissement de sessions comme, le service de la voix et les messages SMS entre deux utilisateurs IMS.

**Mots clés :** Réseau 4G, LTE, Solution VoLTE, OpenIMSCore, Réseau IMS.

**Abstract :**

VoLTE (Voice over LTE) is the future of voice communications because it is IP-based and IP-routed and compatible with next-generation networks. It can also ensure a very good quality of service because a very high data rate is assigned for each IP packet.

The objective of this project is to simulate an IMS (IP Multimedia Subsystem) network, which offers a voice service while connecting to the 4G LTE mobile network, through the deployment of an "OpenIMSCore" platform based on Opensource solutions. This platform aims to simulate the functionalities necessary for the establishment of any multimedia session, and also the launch of tests for the exchange of SIP signaling flows and the establishment of sessions such as voice service and SMS messages. between two IMS users.

**Keywords:** 4G Network, LTE, VoLTE Solution, OpenIMSCore, IMS Network.

**ملخص:**

الصوت عبر شبكة LTE أو VoLTE هو مستقبل الاتصالات الصوتية لأنه قائم وموجه عبر بروتوكول الإنترنت ومتوافق مع شبكات الجيل الجديد. يمكن أن يضمن أيضاً جودة خدمة جيدة جداً، يتم تخصيص معدل بيانات مرتفع للغاية لكل حزمة IP.

الهدف من مشروع التخرج هو محاكاة شبكة IMS (IP Multimedia Subsystem)، والتي تقدم خدمة صوتية أثناء الاتصال بشبكة الجيل الرابع (4G) LTE المتنقلة، من خلال نشر منصة "OpenIMSCore" القائمة على حلول المصادر المفتوحة. تهدف هذه المنصة إلى محاكاة الوظائف اللازمة لإنشاء أي جلسة وسائط متعددة، وكذلك إطلاق اختبارات تبادل تدفقات بإشارات SIP وإنشاء جلسات مثل الخدمة الصوتية والرسائل النصية القصيرة بين اثنين من مستخدمي IMS.

الكلمات المفتاحية: شبكة 4G، LTE، حلول VoLTE، OpenIMSCore، شبكة IMS.



## Table des matières

Dédicaces .....	i
Remerciement .....	iii
Résumé, Abstract et ملخص .....	iv
Table des matières.....	v
Liste des figures .....	viii
Liste des tableaux .....	x
Liste des abréviations.....	xi
<b>Introduction générale.....</b>	<b>1</b>

### Chapitre I : L'évolution des réseaux mobiles

<b>I.1 Introduction .....</b>	<b>3</b>
<b>I.2 Première génération de réseau mobile (1G) .....</b>	<b>3</b>
<b>I.3 Deuxième génération du réseau mobile (2G) .....</b>	<b>3</b>
I.3.1 Architecture du réseau GSM .....	4
I.3.1.1 Le sous-système de station de base (BSS) .....	5
I.3.1.2 Le sous- système d'acheminement (NSS) .....	6
I.3.1.3 Le sous-système de maintenance (OSS) .....	6
I.3.2 Les technique d'accès au réseau .....	6
I.3.2.1 Frequency Division Multiple Access (FDMA) .....	7
I.3.2.2 Time Division Multiple Access (TDMA) .....	7
I.3.3 Réseau GPRS (2.5G) .....	7
I.3.3.1 Architecture du réseau GPRS.....	7
I.3.3.2 Les composantes du réseau GPRS.....	8
I.3.4 Réseau EDGE (2.75G) .....	8
<b>I.4 Troisième génération du réseau mobile (3G) .....</b>	<b>9</b>
I.4.1 Évolution de la 3G .....	9
I.4.2 Architecture du réseau UMTS .....	9
I.4.2.1 Equipement d'utilisateur (UE) .....	10
I.4.2.2 Réseau d'accès radio (UTRAN) .....	10
I.4.2.2.1 NodeB.....	11
I.4.2.2.2 RNC.....	11
I.4.2.3 Le réseau cœur.....	11
I.4.2.4 WCDMA dans l'UMTS .....	11
<b>I.5 La quatrième génération 4G (LTE) .....</b>	<b>12</b>
<b>I.6 La cinquième génération (5G) .....</b>	<b>12</b>
<b>I.7 Conclusion .....</b>	<b>13</b>



## Chapitre II : Le LTE et la voix sur LTE (VoLTE)

<b>II.1 Introduction</b> .....	<b>15</b>
<b>II.2 Réseaux radio mobiles 4G LTE</b> .....	<b>15</b>
II.2.1 Architecture de la 4G LTE.....	15
II.2.1.1 Le réseau d'accès LTE.....	16
II.2.1.2 Le réseau cœur EPC .....	17
<b>II.3 Solutions pour la Voix sur LTE</b> .....	<b>19</b>
II.3.1 CSFB (Circuit Switched Fall Back) .....	20
II.3.2 VoLGA (Voice over LTE via Generic Access) .....	22
II.3.2.1 VoLGA dans le réseau .....	22
II.3.2.2 VoLGA du point de vue du réseau LTE .....	23
II.3.2.3 Le VANC.....	24
II.3.2 VoLTE via IP Multimedia Subsystem (IMS) .....	24
<b>II.4 La différence entre LTE et la VoLTE</b> .....	<b>25</b>
<b>II.5 Conclusion</b> .....	<b>26</b>

## Chapitre III : La VoLTE via IP Multimédia Subsystem (IMS)

<b>III.1 Introduction</b> .....	<b>27</b>
<b>III.2 Présentation de la voix sur IP</b> .....	<b>27</b>
<b>III.3 Sous-système multimédia IP</b> .....	<b>27</b>
<b>III.4 L'architecture IMS</b> .....	<b>28</b>
III.4.1 La couche accès .....	29
III.4.2 La couche de transport .....	29
III.4.3 La couche de contrôle .....	29
III.4.4 La couche services et application .....	29
<b>III.5 Les principaux composants de l'architecture IMS</b> .....	<b>29</b>
III.5.1 Serveur d'abonné domestique (HSS) .....	30
III.5.2 Fonction de localisation d'abonné (SLF) .....	30
III.5.3 Les serveurs CSCF .....	30
III.5.3.1 Proxy CSCF (P-CSCF) .....	30
III.5.3.2 Interrogating CSCF (I-CSCF) .....	30
III.5.3.3 Serving CSCF (S-CSCF) .....	31
III.5.4 Fonction de commande de passerelle de sortie (BGCF) .....	31
III.5.5 Fonction de contrôle de passerelle média (MGCF) .....	31
III.5.6 Fonction de passerelle média (MGW) .....	31
III.5.7 Fonction de ressource Multimédias (MRF).....	32
III.5.7.1 MRFC (MultiMedia Resource Function Controller) .....	32
III.5.7.2 MRFP (MultiMedia Resource Function Processor) .....	32
III.5.8 Les serveurs d'applications AS.....	32
III.5.8.1 SIP AS (SIP Application Server) .....	32
III.5.8.2 IM-SSF (IP Multimedia-Service Switching Function) .....	32
III.5.8.3 La passerelle OSA (OSA SCS, OSA Service Capability Server).....	32



<b>III.6 Gestion des identités en IMS</b> .....	33
III.6.1 Identité Privée Multimédia IP.....	33
III.6.2 Identité Publique Multimédia IP .....	33
<b>III.7 Protocoles clés utilisés dans le réseau LTE-IMS</b> .....	33
III.7.1 Protocole DIAMETER .....	33
III.7.1.1 Les messages DIAMETER .....	34
III.7.2 Le protocole SIP .....	35
III.7.2.1 Les entités SIP .....	36
III.7.2.2 Les requêtes SIP .....	37
III.7.2.3 Les réponses SIP .....	39
III.7.2.4 Exemple de scénario .....	40
III.7.3 Le protocole SDP (Session Description Protocol) .....	41
III.7.4 Les protocoles RTP et RTCP .....	42
III.7.5 Le protocole de contrôle de passerelle H.248 et MEGACO .....	42
<b>III.8 La qualité de service (QoS) dans LTE</b> .....	43
<b>III.9 Procédure de IMS et VoLTE</b> .....	44
III.9.1 Procédure d'enregistrement IMS.....	44
III.9.2 Configuration et lancement de l'appel VoLTE .....	45
<b>III.10 Conclusion</b> .....	47

## Chapitre IV : Mise en place de la solution IMS pour la VoLTE

<b>IV.1 Introduction</b> .....	48
<b>IV.2 Open IMS Core</b> .....	48
IV.2.1 Logiciels utilisés .....	49
IV.2.1.1 Logiciel UCT IMS Client .....	49
IV.2.1.2 Logiciel Boghe IMS Client .....	49
IV.2.1.3 IMS deroid .....	49
<b>IV.3 Mise en œuvre d'OpenIMScore</b> .....	49
IV.3.1 Mise en place Machine Virtuelle .....	49
IV.3.2 Installation d'un cœur réseau IMS.....	50
<b>IV.4 Simulation et résultats</b> .....	55
IV.4.1 Cas de deux clients déjà préconfigurés .....	56
IV.4.1.1 Enregistrement des utilisateurs dans le réseau.....	56
IV.4.1.2 Test d'appel vocal.....	57
IV.4.1.3 Test de session data (message) .....	59
IV.4.2 Cas de deux clients à configurer .....	59
IV.4.2.1 Configuration des deux abonnés IMS.....	60
IV.4.2.2 Configuration et utilisation d'un client IMS .....	64
<b>IV.5 Conclusion</b> .....	70
<b>Conclusion générale</b> .....	71
<b>Bibliographie</b> .....	72





## Liste des figures

<b>Figure I.1</b> : Architecture du réseau GSM .....	4
<b>Figure I.2</b> : Architecture des réseaux GPRS .....	8
<b>Figure I.3</b> : Architecture du réseau UMTS .....	10
<hr/>	
<b>Figure II.1</b> : Architecture du réseau LTE .....	16
<b>Figure II.2</b> : Architecture plan d'utilisateur et plan de signalisation .....	17
<b>Figure II.3</b> : Architecture de la VoLTE.....	20
<b>Figure II.4</b> : Architecture de la solution CSFB.....	21
<b>Figure II.5</b> : Architecture de la solution VoLGA.....	23
<b>Figure II.6</b> : Architecture de la solution VoLTE via IMS .....	24
<b>Figure II.7</b> : Points forts et faibles des solutions CSFB, VoLGA et IMS .....	25
<hr/>	
<b>Figure III.1</b> : Architecture en couches de l'IMS .....	28
<b>Figure III.2</b> : Architecture fonctionnelle de l'IMS .....	29
<b>Figure III.3</b> : Architecture de SIP.....	36
<b>Figure III.4</b> : Format d'une requête SIP .....	37
<b>Figure III.5</b> : Format d'une réponse SIP.....	39
<b>Figure III.6</b> : Exemple d'établissement de session.....	41
<b>Figure III.7</b> : Procédure d'enregistrement IMS.....	44
<b>Figure III.8</b> : Procédure d'un lancement de l'appel VoLTE .....	46
<hr/>	
<b>Figure IV.1</b> : Architecture d'OpenIMScore .....	48
<b>Figure IV.2</b> : La zone DNS .....	51
<b>Figure IV.3</b> : Configuration DNS .....	52
<b>Figure IV.4</b> : Démarrage de P-CSCF.....	53
<b>Figure IV.5</b> : Démarrage de S-CSCF.....	53
<b>Figure IV.6</b> : Démarrage de i-CSCF.....	54
<b>Figure IV.7</b> : Démarrage de FHoSS.....	54
<b>Figure IV.8</b> : Page d'accueil de HSS.....	55



<b>Figure IV.9:</b> Enregistrement l'utilisateur Alice dans le réseau .....	56
<b>Figure IV.10:</b> Enregistrement l'utilisateur Bob dans le réseau .....	56
<b>Figure IV.11:</b> Registre de plateforme IMS .....	57
<b>Figure IV.12:</b> Alice appelle Bob .....	58
<b>Figure IV.13:</b> Fin d'appel entre Alice et Bob .....	58
<b>Figure IV.14:</b> Établissement d'une session de données entre Alice et Bob .....	59
<b>Figure IV.15:</b> Configuration de l'IMPU souhilasaim .....	60
<b>Figure IV.16:</b> Configuration de l'IMPU marwayazid .....	61
<b>Figure IV.17:</b> Configuration de l'IMPI pour souhilasaim .....	62
<b>Figure IV.18:</b> Configuration de l'IMPI pour marwayazid .....	63
<b>Figure IV.19:</b> Configuration d'IMS Suscription pour souhilasaim.....	63
<b>Figure IV.20:</b> Configuration d'IMS Suscription pour marwayazid .....	64
<b>Figure IV.21:</b> Boghe IMS Client.....	64
<b>Figure IV.22:</b> L'inscription Boghe IMS Cleint.....	65
<b>Figure IV.23:</b> Configuration networking IP P-CSCF et le port .....	65
<b>Figure IV.24:</b> Connecter àBoghe-IMS client.....	66
<b>Figure IV.25:</b> Ajouter un contactBoghe IMS client .....	66
<b>Figure IV.26:</b> Contact de souhilasaim .....	67
<b>Figure IV.27:</b> IMS Droid .....	67
<b>Figure IV.28:</b> L'inscription sur IMS Deroid .....	67
<b>Figure IV.29:</b> Configuration networking IMS Deroid .....	68
<b>Figure IV.30:</b> L'enregistrement des utilisateurs .....	68
<b>Figure IV.31:</b> Test d'appel entre deux utilisateurs .....	69
<b>Figure IV.32:</b> Appel vidéo entre deux utilisateurs .....	70



## Liste des tableaux

<b>Tableau II.1</b> : Comparaison entre LTE et VoLTE .....	26
<b>Tableau III.1</b> : Description des messages SDP .....	42
<b>Tableau III.2</b> : Définitions des supports de QoS EPS .....	43

## Liste des abréviations

<b>AAA</b> : Authentication, Authorization, Accounting	<b>ISUP</b> : Integrated Services Digital Network User Part
<b>AS</b> : Application Server	<b>IP</b> : Internet protocol
<b>AuC</b> : Authentification centre	<b>IMPU</b> : Public User Identity
<b>BSS</b> : Base station Sub-System	<b>IMPI</b> : Private User Identity
<b>BSC</b> : Base station Controller	<b>IMS</b> : IP Multimedia Subsystem
<b>BTS</b> : Base transceiver station	<b>I-CSCF</b> : Interrogating Call Session Control Function
<b>CSFB</b> : Circuit Switched Fall Back	<b>LTE</b> : Long Term Evolution
<b>CSCF</b> : Call session control Function	<b>MS</b> : Station mobile
<b>DNS</b> : Domain Name System	<b>MSC</b> : Mobile-service Switching center
<b>EIR</b> : Equipment Identity Register	<b>MAP</b> : Mobile application Part
<b>E-UTRAN</b> : Evolved Universal Terrestrial Radio Access Network	<b>MIMO</b> : Multiple input multiple output
<b>EPC</b> : Evolved Packet Core	<b>MME</b> : Mobility management entity
<b>EPS</b> : Evolved Packet system	<b>NSS</b> : Network Sub-System
<b>E-CSCF</b> : Emergency Call Session Control Function	<b>OSS</b> : Operation Sub-System
<b>FHoSS</b> : FOKUS Home Subscriber Server	<b>OSI</b> : Open Systems Interconnection
<b>GSM</b> : Global système mobile communications	<b>PCU</b> : Packet control unit
<b>GPRS</b> : General Packet Radio Services	<b>PDN</b> : Packet Data Network
<b>GUTI</b> : Globally Unique Temporary Identity	<b>PCRF</b> : Policy and Charging Rules Function
<b>GMSC</b> : Gateway mobile service Switching center	<b>PSTN</b> : Public Switched telephone Network
<b>GGSN</b> : Gateway GPRS Support Node	<b>PLMN</b> : Public land mobile Network
<b>HLR</b> : HOME location Register	<b>P-CSCF</b> : Proxy Call Session Control Function
<b>HSS</b> : Home Subscriber Server	<b>PS</b> : Packet Switched
<b>IMEI</b> : International mobile équipement Identity	<b>QoS</b> : Quality of Service
<b>IMSI</b> : international mobile Subscriber Identity	<b>RNC</b> : Radio Network Controller
	<b>RTC</b> : Réseau téléphonique commuté
	<b>RAB</b> : Radio Access Bearer
	<b>RRC</b> : Radio Resource Control



**RTP** : Real Time Protocol

**SMS** : Short Message Service

**SIM** : Subscriber Identifie module

**SS7** : Système de signalisation

Semaphort n°7

**SGSN** : Serving GPRS Support Node

**SAE** : System Architecture Evolution

**S-CSCF** : Serving Call Session Control  
Function

**SIP** : Session initial protocol

**SDP** : Session Description Protocol

**SLF** : Subscription Locator Functional

**SGW** : Serving Gateway

**SER** : SIP Express Router

**UMTS** : Universal mobile  
telecommunication system

**USIM** : UMTS Subscriber Identity  
Module

**UTRAN** : Universal Terrestrial Radio  
Access Network

**UA** : User Agent

**URI** : Uniform Resource Identifier

**VLR** : visitor location Register

**VoLTE** : Voice over LTE

## Introduction générale

L'ère des télécommunications a fait de grands progrès dans l'évolution technologique des réseaux mobiles a permis l'émergence de nouveaux appareils et de nouveaux services. Cette évolution a été toujours influencée par une forte demande des utilisateurs, il s'agit d'une part du déploiement de plusieurs générations successives de réseaux de télécommunications, chaque génération est définie comme un ensemble de normes de réseau téléphonique. Fondamentalement, le voyage d'évolution a commencé en 1979 à partir de la technologie 1G et il se poursuit toujours vers la 5G, afin de satisfaire la demande et avoir un débit de transfert des données considérables.

En 4G, la voix n'est pas prise en charge, elle passe sur le réseau 3G, voire 2G. Ce n'est qu'avec la prochaine évolution. VoLTE ou Voice over LTE qu'elle empruntera le réseau IP avec une meilleure qualité sonore et des communications vocales et données simultanément. La VoLTE ou voix sur le réseau LTE est une technologie réseau innovante qui permet d'émettre ou de recevoir les appels avec votre téléphone mobile directement via le réseau 4G de votre opérateur mobile.

Les réseaux 4G déploient la technologie d'accès radio LTE des réseaux mobiles reposent sur des réseaux cœur tout IP appelé EPC (Evolved Packet Core), alors que les services de la téléphonie mobile habituelles qui sont déjà déployés en 2G (GSM) et 3G (UMTS) ne peut pas être exploités aussitôt dans les réseaux LTE, car ce type des réseaux ne traitent pas la signalisation téléphonique. Face à ce problème, les organisations de télécommunication tel que la 3GPP (3rd Génération Partnership Project) et GSMA (GSM Association) proposent des solutions pour résoudre le problème de signalisation téléphonique sur les systèmes 4G LTE, parmi ces solutions, la VoLTE.

La VoLTE utilise le réseau IMS (Internet protocole multimédia SubSystem) comme plateforme pour gère la signalisation SIP, tarification, l'authentification, la QoS (qualité de service), ainsi que le basculement entre les différent types des réseaux (2G et 3G).

Dans ce mémoire on va simuler le réseau IMS avec ses composants cœur en déployant la plateforme "OpenIMSCore" basée sur des solutions open source.

Ce mémoire est divisé sur quatre chapitres :

Le premier chapitre est consacré à l'évolution des réseaux mobiles et les différentes générations de réseaux mobiles, en commençant par l'ancienne génération 1G, ensuite on passera à la 2G (GSM), 2.5G (GPRS), après on présentera les réseaux 3G (UMTS) et ses variantes jusqu'à la 4G (LTE).



Le deuxième chapitre représente une description détaillée sur la norme des réseaux radio mobiles LTE et l'architecture des différentes solutions de la VoLTE, ses éléments et son principe de fonctionnement.

Le troisième est concentré sur l'étude des solutions qui offrent le service téléphonique sur le sous-système multimédia IP (IMS), ses fonctionnalités et ses caractéristiques pour prendre en charge la VoLTE.

Le dernier chapitre sera consacré à la mise en place d'une solution IMS pour la VoLTE basée sur une plateforme OpenIMSCore open source, avec d'autres services comme l'IPTV.

Enfin, nous concluons ce travail en résumant les connaissances acquises durant la phase de réalisation du projet ainsi que quelques perspectives quant à l'avenir de notre implémentation.



## Chapitre I :

---

# *L'évolution des réseaux mobiles*

---

## I.1 Introduction

Les télécommunications ont connu une importante évolution depuis leur apparition. Les réseaux de la première génération (1G) proposaient aux clients de communiquer simplement par la voix via un réseau analogique. Grâce à cette évolution qui a permis de passer de l'ère analogique à l'ère numérique, la transmission des messages sur la 2G est devenue possible. La demande croissante à cette technologie a permis une autre évolution vers d'autres générations, qui peuvent permettre de surfer aussi sur internet avec un débit confortable, on parle ici de la 3G.

En raison de la demande du marché, la bande passante et la capacité de transfert des données étaient les principales parties à développer, d'où le recours à d'autres méthodes d'accès et de moyens pour une plus grande efficacité spectrale, la 3G est évoluée par la suite à la 4G LTE et maintenant vers la 5G.

Dans ce chapitre nous allons exposer l'évolution de ces réseaux mobiles d'une génération à une autre, et décrire brièvement leurs fonctionnements, leurs standards et leurs architectures ainsi que d'autres services pouvant être utilisés par chacune de ces générations cellulaires.

## I.2 Première génération de réseau mobile (1G)

La première génération de réseau cellulaire a été introduite à la fin des années 70 et des normes entièrement mises en œuvre. La 1G utilisait des signaux analogiques pour transférer les informations. Ces informations n'étaient limitées qu'aux appels vocaux, avec une vitesse maximale de 2.4 kbps et l'FDMA était le système d'accès utilisé. La qualité de la voix était grande sans beaucoup de sécurité, et subissait parfois des appels interrompus avec un coût élevé et sans Roaming (le pouvoir d'appeler ou d'être appelé en tout point du territoire).

La technologie de la 1G utilisait essentiellement des standards comme AMPS (basé sur FDMA), NMT et TACS (qui reposent sur la technologie AMPS). Ce sont les normes de télécommunications analogiques qui ont été introduites dans les années 1980, et se sont poursuivies jusqu'à leur remplacement par les télécommunications numériques de la 2G.

## I.3 Deuxième génération du réseau mobile (2G)

Après cette technologie analogique qui limite l'utilisation des abonnées, au début des années 90, le système mondial de communication mobile a déclenché une nouvelle génération, qui a marqué une rupture avec la 1G, c'est la 2G qui a permis d'améliorer l'analogique avec des solutions numériques à commutation de circuits. La 2G vient de faciliter les difficultés de la génération précédente et qui répond à la demande des utilisateurs, en offrant la possibilité d'appeler et d'être appelé (Roaming), et la continuation de la communication même en déplaçant (Handover) qui n'était pas offert en 1G.



Le réseau GSM est dit de « seconde génération » (2G), il utilise les bandes de fréquences 900 MHz et 1800 MHz en Europe. Par contre aux Etats-Unis, la bande de fréquence utilisée est la bande 1900 MHz.

Ce réseau doté un débit maximal de 9,6 kbps. Il devient possible de transmettre, ce qui permet de passer des appels vocaux ainsi que des données numériques de faible volume, tels que les messages textes SMS (Short Message Service) ou des messages multimédias MMS (Multimédia Message Service).

La 2G se divise principalement en deux technologies. Les normes d'accès multiple par répartition dans le temps (TDMA), utilisant une technique de découpage temporel des canaux de communication afin d'augmenter la capacité du réseau. L'autre tranche 2G est l'accès multiple par répartition en fréquence (FDMA) permettant de diffuser un signal radio sur une grande gamme de fréquence.

### I.3.1 Architecture du réseau GSM

La mise en place d'un réseau GSM permet à un opérateur de proposer des services de type « Voix » à ses clients, en donnant accès à la mobilité, tout en conservant un interfaçage avec le réseau fixe RTC existant. Les équipements introduit par GSM et les fonctions relatives à la gestion des utilisateurs mobiles sont été regroupé dans un type de réseau appelé PLMN.

Le réseau GSM est composé de trois sous-ensembles [1], comme montre la figure I.1 :

- Le sous-système radio BSS (Base Station Mobile) : pour assurer et gérer les transmissions radios.
- Le sous-système d'acheminement NSS (Network Sub Système) : qui comprend l'ensemble des fonctions nécessaires pour les appels et la gestion de la mobilité.
- Le sous-système d'exploitation et de maintenance OSS (Operation Sub-Système) : qui permet à l'opérateur d'exploiter et contrôler son réseau.

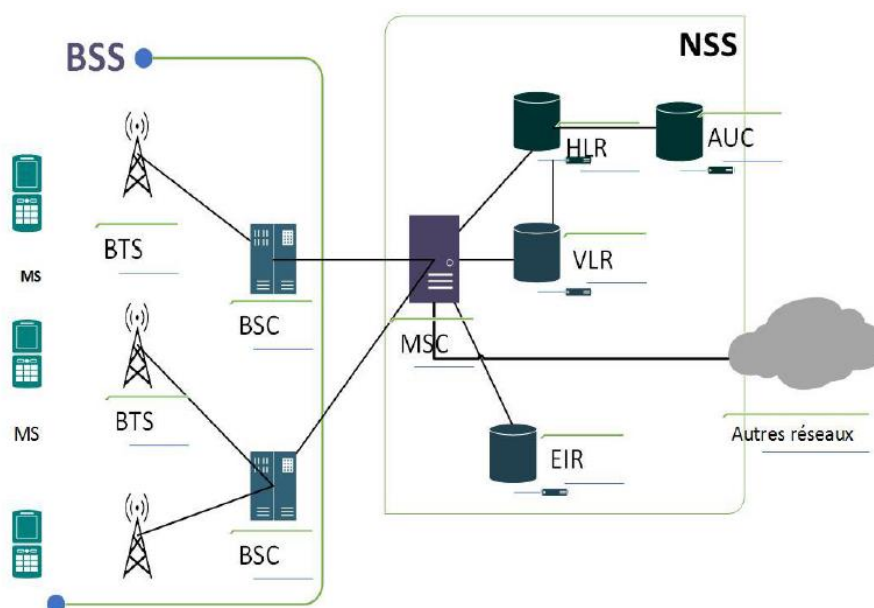


Figure I.1 : Architecture du réseau GSM [2].

Les interfaces sont aussi des composants importants d'un réseau GSM, elles supportent le dialogue entre les équipements et permettent leur inter fonctionnement. En GSM, on distingue les principales interfaces :

- **L'interface Um** : elle est localisée entre la station mobile (MS) et la station de base (BTS). On la nomme couramment « interface radio » ou « interface air ». C'est l'interface la plus importante du réseau.
- **L'interface Abis** : cette interface relie la station de base à son contrôleur
- **L'interface A** : relie le sous-système radio au sous-système réseau.

### I.3.1.1 Le sous-système de station de base (BSS)

Le sous-système radio (BSS) est composé de trois éléments :

**La station mobile MS (Mobile Station)** : terminal mobile authentifié et autorise à accéder au réseau mobile. Il associe de :

- **Terminal physique**, appelé Mobile Equipement (ME) : Chaque terminal mobile est identifié par un code unique (IMEI). Ce code est vérifié à chaque utilisation et permet la détection et l'interdiction de terminaux volés.
- **La carte SIM** (Subscriber Identity Module) : est une carte à puces qui contient dans sa mémoire le code (IMSI), qui identifie l'abonné de même que les renseignements relatifs à l'abonnement. Cette carte peut être utilisée sur plusieurs appareils. Il est à noter que l'utilisateur ne connaît pas son IMSI mais il peut protéger sa carte à puce à l'aide d'un numéro d'identification personnel à quatre chiffres.

**Les BTS (Base Transceiver Station)** : sont des émetteurs récepteurs ayant un minimum d'intelligence, assurant la réception les appels entrant et sortant des équipements mobiles.

- Chargée de la transmission radio : modulation, démodulation, égalisation, codage correcteur d'erreur.
- Gère toute la couche physique : multiplexage TDMA, chiffrement, saut de fréquence...
- Réalise l'ensemble des mesures radio nécessaires pour vérifier qu'une communication se déroule normalement.
- gère la couche liaison de données pour l'échange de signalisation entre les mobiles et l'infrastructure.

**Les BSC (Base Station Controller)** : contrôlent un ensemble de BTS et permettent une première concentration des circuits. C'est véritablement l'organe intelligent du sous-système radio, Gèrent :

- l'allocation des fréquences, le contrôle de puissance.
- le contrôle d'admission.

- le Handover : décision et exécution
- les mesures reçues par les BTSs

### I.3.1.2 Le sous- système d'acheminement (NSS)

Le NSS est le cœur du réseau, il comprend des commutateurs et des bases de données. Ce réseau est composé de :

**MSC (Mobile-service Switching Centre)** : est un élément central du système de réseau GSM/CDMA. Il agit comme un centre de contrôle d'un sous-système de commutation de réseau (NSS). Cet élément connecte les appels entre les abonnés en commutant les paquets vocaux numériques entre les chemins du réseau. Il gère les communications des mobiles sous sa couverture et la mobilité des usagers en dialoguant avec le VLR. Ce dernier gère l'établissement des communications entre un mobile et un autre MSC et exécute le Handover si hors BSC, lors d'appels d'abonné fixe vers un mobile, c'est le MSC qui sert de passerelle active

**VLR (visitor location Register)** : est une base de données qui gère les abonnés présents dans une zone géographique et leur mobilité, il permet de vérifier leurs caractéristiques et le transfert d'information de localisation, les informations détectées les bases de données sont une copie de l'original qui est conservé dans le HLR.

**HLR (HOME location Register)** : c'est une base de données qui gère un PLMN et mémorise le profil de l'abonné et le VLR dans lequel il est enregistré.

**AUC (authentication centre)** : centre d'authentification qui mémorise pour chaque abonné sa clé utilisée, pour pouvoir authentifier les demandes de service et pour le chiffrement des communications, un AUC est en général associé à chaque HLR.

**EIR (Equipment Identity Register)** : base de données comportant les informations de la sécurité relative à un téléphone mobile. Ce dernier doit potentiellement pouvoir accueillir n'importe quelle carte SIM de n'importe quel réseau.

### I.3.1.3 Le sous-système de maintenance (OSS)

Le OSS permet à l'opérateur de contrôler son réseau. La mise en place d'un réseau GSM (en mode circuit) va permettre à un opérateur de proposer des services de type « Voix » à ses clients en donnant accès à la mobilité tout en conservant un interfaçage avec le réseau fixe RTC existant.

## I.3.2 Les techniques d'accès au réseau

L'objectif des techniques d'accès est d'optimiser le nombre d'utilisateurs par unité de fréquence de la bande passante allouée à l'opérateur pour permettre offrir le service de communication entre les

abonnés du réseau fixe RTCP (PSTN) et ceux du réseau mobile, et les abonnés du réseau mobile entre eux. Les techniques d'accès en 2G sont FDMA et TDMA.

### I.3.2.1 Frequency Division Multiple Access (FDMA)

- La technique FDMA permet de diviser la bande passante en segments de fréquence, chaque segment étant utilisable par un abonné.
- La moitié des segments contigus sont affectés pour le trafic sortant et l'autre moitié au trafic entrant.
- Une bande de garde est généralement fournie entre le trafic entrant et sortant.
- Avec FDMA tous utilisateurs partagent le canal de fréquence simultanément. Cependant chaque utilisateur transmet à une fréquence unique.
- Cette technique est compatible avec les signaux numériques et analogiques.

### I.3.2.2 Time Division Multiple Access (TDMA)

- La bande fréquentielle est divisée en trames TDMA, chaque trame est divisée en  $n$  times slots. Chacun de ces  $n$  times slots de la trame est assigné à un abonné différent. De cette façon une bande de fréquence peut contenir jusqu'à  $n$  abonnés.
- La transmission d'un seul abonné comporte différents time slots assignés cycliquement à l'abonné (un TS par trame).
- Avec la TDMA, chaque bande de fréquence est uniquement employée par un seul abonné à un moment donné.

### I.3.3 Réseau GPRS (2.5G)

Le standard GPRS (General Packet Radio Services) est une évolution de la norme GSM, repose sur la transmission en mode paquet. Le déploiement du GPRS nécessite la mise en place d'une infrastructure réseau basée sur la commutation de paquets, et l'introduction de passerelles pour s'adosser aux réseaux GSM existants.

Le réseau GPRS, aussi appelé 2,5G ou 2G+, améliore notablement le débit maximal de transfert de données (171,2 Kbit/s, avec un débit moyen de 48 Kbit/s) par rapport à la 2G. Permettant le transfert de données de volume modéré, le GPRS est le précurseur sur l'internet mobile. Notons que tous les téléphones portables sont aujourd'hui au moins compatibles au réseau 2,5G [3].

Ainsi, la norme GPRS utilise l'architecture de réseau GSM pour la transmission de la voix et permet d'accéder aux réseaux de données (notamment Internet) en utilisant soit le protocole IP, soit le protocole X.25.

#### I.3.3.1 Architecture du réseau GPRS

La mise en place d'un réseau GPRS va permettre à un opérateur de proposer de nouveaux services de type «Data» ses clients. Comme le GPRS utilise le GSM, il a gardé la grande partie de son infrastructure tout en ajoutant deux nouveaux composants : SGSN et GGS.

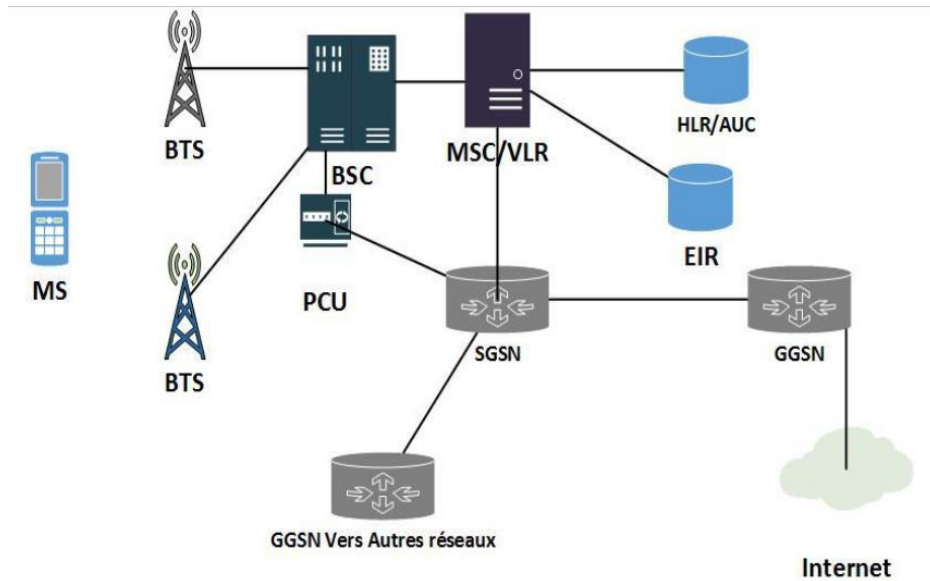


Figure I.2 : Architecture des réseaux GPRS [2].

### I.3.3.2 Les composantes du réseau GPRS

Les réseaux GPRS incluent dans leur architecture de nouveaux éléments, permettant de supporter le trafic des données et la commutation des paquets, ces éléments sont :

- **Le nœud de service SGSN** (Serving GPRS Support Node) : c'est l'équivalent de la VLR dans le réseau GSM, joue un rôle de routeur, il gère les terminaux de la zone donnée. Le SGSN est le contrôleur des terminaux GPRS présents dans sa zone de surveillance.
- **Le nœud de passerelle GGSN** (Gateway GPRS Support Node) : même fonction que le GMSC pour le GSM, utilisé comme interface entre le réseau IP de l'opérateur et le réseau internet public, ou d'autres fournisseurs de services mobiles.
- **Le module PCU** (Packet control unit) : unité de contrôle chargée de la gestion de l'allocation des ressources radio pour des services GPRS, de la congestion et de la diffusion d'informations système liées au GPRS. Localisée dans la BTS, ou BSC ou SGSN.
- **Le module BG** pour la sécurité : Les recommandations introduisent le concept de BG (Border Gateway) qui permettent de connecter les réseaux GPRS via un réseau fédérateur, et qui assurent les fonctions de sécurité pour la connexion entre ces réseaux.
- **Le routeur IP** : L'opérateur peut prendre le parti de gérer et d'administrer ses propres routeurs IP afin d'ouvrir le réseau GPRS vers les réseaux de données externes.

### I.3.4 Réseau EDGE (2.75G)

Le réseau EDGE (Enhanced Data Rate for GSM Evolution) appelé aussi 2,75G, a fait suite à la technologie GPRS et a permis de tripler le débit du GPRS, ouvrant ainsi la porte aux applications multimédias. Certains opérateurs comme Orange et Bouygues Telecom ont déployé EDGE afin de faciliter la transition entre 2G et 3G [3].

## I.4 Troisième génération du réseau mobile (3G)

La 3G, fait son apparition dans les années 2000, sous l'action de l'Union Internationale des Télécommunications (UIT) avec le sigle IMT-2000, qui va désigner l'ensemble des technologies d'accès radio et de réseaux cellulaires de la troisième génération. Elle est représentée principalement par les normes Universal Mobile Télécommunications System (UMTS) et CDMA2000, marque le passage des systèmes de téléphonie à des systèmes tournés vers des services multimédia. L'objectif est de débrider les débits pour enfin avoir une expérience d'Internet en mobilité similaire à celle de l'Internet fixe. L'idée de la 3G est d'ajouter des amplificateurs avant chaque antenne pour permettre d'amplifier le signal pour qu'il puisse être reçu à une autre antenne en améliorant les terminaux.

La 3G (troisième génération de réseaux mobiles), utilise la norme UMTS, offre un accès à l'Internet haut débit, entre 144 kbit/s et 2 Mbit/s, avec un débit moyen de quelques centaines de Kbit/s. Ce qui vous permet notamment de :

- Télécharger plus rapidement des données, des applications ou bien des jeux.
- Envoyer des vidéos.
- Regarder des vidéos en streaming sur YouTube, Dailymotion, etc.
- Faire de la visio-conférence.
- Accéder à la TV mobile.
- Bénéficier du GPS.

### I.4.1 Évolution de la 3G

Notons que la 3G a connu trois évolutions successives [3] :

- La 3G+ aussi appelée « H » pour HSPA (High Speed Packet Access), avec un débit compris entre 300 kbit/s et 14,4 Mbit/s, pour une moyenne de 3,6 Mbit/s. Bref, la 3G+ est 7 fois plus rapide que la 3G.
- Le H+ (ou HSPA+), avec un débit moyen de 5 Mbit/s, pour un débit théorique maximal de 21 Mbit/s.
- Le H+ Dual Carrier (ou DC-HSPA+), doté d'un débit moyen de 10 Mbit/s, et un débit plafond de 42 Mbit/s.

Bref, la 3G et ses évolutions ont permis de démocratiser complètement l'utilisation de l'Internet mobile.

### I.4.2 Architecture du réseau UMTS

L'architecture d'un réseau UMTS est divisée en deux groupes (voir la Figure I.3). Le premier groupe correspond au réseau d'accès radio (RAN, Radio Access Network ou UTRAN, UMTS Terrestrial RAN), qui supporte toutes les fonctions radio. Le deuxième groupe correspond au réseau cœur (CN, Core Network), qui est responsable de la commutation et du routage des communications (voix et données) vers des réseaux externes. Afin de compléter le système, un terminal utilisateur (UE, User Equipment) est également défini, qui est situé entre l'utilisateur réel et le réseau d'accès radio.

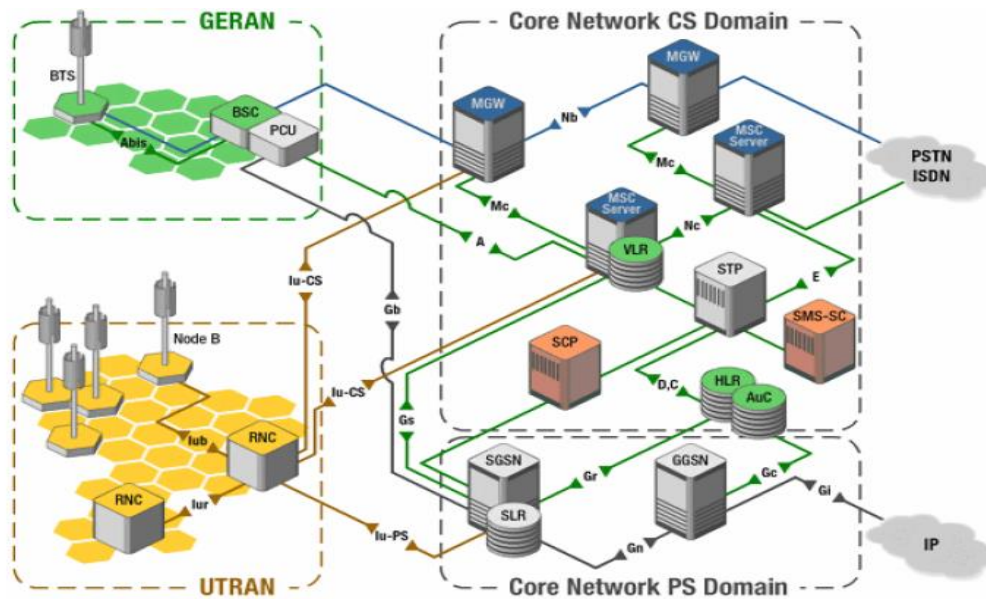


Figure I.3 : Architecture du réseau UMTS [2].

#### I.4.2.1 Equipement d'utilisateur (UE)

L'UE (User Equipment) consiste en un ME (Mobile Equipment) et un USIM (UMTS Subscriber Identity Module).

- **ME (Mobile Equipment)** : est le terminal radio employé pour la communication radio sur l'interface radio Uu.
- **L'USIM (UMTS Subscriber Identity Module)** : est une carte à puce dans laquelle sont stockées les données concernant l'utilisateur et son abonnement, telles que son identité, les clés de chiffrement et d'authentification.

#### I.4.2.2 Réseau d'accès radio (UTRAN)

Le réseau d'accès UTRAN est doté de plusieurs fonctionnalités (Sécurité, Mobilité, Gestion des ressources radio, Synchronisation). Sa fonction principale est de transférer les données générées par l'utilisateur. Il est une passerelle entre l'équipement utilisateur et le réseau cœur via les interfaces Uu et Iu. Il est composé de deux entités : stations de base appelées NodeB, et des contrôleurs radio RNC liées à travers des interfaces de communication. Plusieurs types d'interfaces de communication coexistent au sein de réseau UMTS [4] :

- **Uu** : Interface entre un équipement utilisateur et le réseau d'accès UTRAN. Elle permet la communication avec l'UTRAN via la technologie CDMA.
- **Iu** : Interface entre le réseau d'accès UTRAN et le réseau cœur de l'UMTS. Elle permet au contrôleur radio RNC de communiquer avec le SGSN.
- **Iur** : Interface qui permet à deux contrôleurs radio RNC de communiquer.
- **Iub** : Interface qui permet la communication entre un NodeB et un contrôleur radio RNC.

#### **1.4.2.2.1 NodeB**

Un NodeB est un équipement liant le terminal UE au RNC à travers l'interface Iub. De ce fait, le NodeB garantit les fonctions de transmission radio : modulation, démodulation, étalement de spectre...

Il est responsable aussi, de la gestion des fréquences de cellules radio, des codes d'étalement, de la synchronisation, de la gestion de signalisations de l'interface Iub, ainsi que la gestion des canaux dédiés et partagés.

#### **1.4.2.2.2 RNC**

Le rôle principal du RNC (Radio Network Controller) est de gérer les communications entre le NodeB et le réseau cœur de l'UMTS. Il peut avoir deux modes de fonctionnement [4] :

- **Le Serving RNC (SRNC)** : Permet de gérer la signalisation associée, prendre les décisions de Handover, gérer le contrôle de puissance...
- **Le Drift RNC (DRNC)** : Permet de gérer d'autres cellules extérieures au SRNC également utilisées par le mobile, transférer les données de manière transparente entre le mobile et le SRNC.

#### **1.4.2.3 Le réseau cœur**

Le réseau cœur de l'UMTS est composé de trois parties dont deux domaines :

- Le domaine CS (Circuit Switched) utilisé pour la téléphonie et la commutation de circuits.
- Le domaine PS (Packet Switched) qui permet la commutation de paquets.
- Les éléments communs aux domaines CS et PS.

#### **1.4.2.4 WCDMA dans l'UMTS**

CDMA (Code Division Multiple Access) est une technique de répartition par codes, où tous les mobiles coexistent dans une même bande de fréquence et transmettent sur les mêmes intervalles temporels, mais utilisent des techniques d'étalement de spectre, pour lesquels chaque utilisateur possède un code unique dans la cellule qui détermine les fréquences utilisées. CDMA consiste à redistribuer et étaler le signal sur une très grande largeur de bande jusqu'à le rendre invisible idéalement pour les autres utilisateurs de la même largeur de bande.

W-CDMA (Wideband CDMA) représente la même technique que CDMA, en utilisant une bande plus large de 5 MHz. L'orientation du WCDMA vers la transmission de données en mode paquet a permis à l'utilisateur d'établir des communications de bande passante variable, même en cours d'appel, ce qui économise la bande passante. En plus de ces avantages, on cite :

- Transmission efficace en mode paquet.
- Compatibilité avec les systèmes 2G et possibilité d'intégrer de nouvelles technologies.
- Gain de traitement plus élevé.



- Possibilité de transmettre des services à haut débit.
- Meilleure performance pour détecter les trajets multiples.
- Support des deux modes FDD et TDD.

### I.5 La quatrième génération 4G (LTE)

Avec l'attribution des bandes de fréquences pour l'exploitation d'un service de communication sans fil, le coup d'envoi du déploiement des réseaux mobiles de 4ème génération est donné.

La 4G, au-delà du terme « Marketing », annonce de profonds changements et investissements techniques pour les opérateurs de réseaux mobiles avec le déploiement d'un nouveau réseau d'accès et d'un nouveau réseau cœur. Pour les utilisateurs, la 4G annonce une meilleure qualité du réseau (débits, latence) et le développement de nouveaux services innovants.

Le vocabulaire technique pour désigner ce futur ensemble, composé du réseau d'accès appelé LTE (pour Long Term Evolution), et d'un réseau cœur appelé ePC (evolved Packet Core), est EPS (pour Evolved Packet System). Ce nouveau réseau remplacera progressivement les anciens réseaux 2G (GSM, GPRS, EDGE) et 3G (UMTS, HSxPA).

Comme pour ses prédécesseurs, le réseau EPS est standardisé par l'organisme 3GPP qui l'introduit dans les versions 8 et supérieures de ses normes. Selon l'ITU-R (International Télécommunication Union - Radio), le LTE ne remplit pas les critères d'un véritable réseau de 4ème génération, et le terme 4G est donc erroné. Il serait plus exacte de parler de 3,9 G. Le véritable réseau d'accès 4G, selon l'ITU-R, sera le successeur du LTE : le LTE Advanced. Mais pour des raisons évidentes de « Marketing » et pour faciliter la discussion, le terme 4G est de fait utilisé pour désigner le nouveau réseau : LTE + ePC = EPS [5].

La promesse de ce nouveau réseau est d'apporter plus de qualité pour les utilisateurs finaux (débit, latence, QoS, IMS, ...) et plus de confort pour la maintenance, l'exploitation et l'évolutivité pour les opérateurs (full IP, IPv6, rapprochement avec le monde Internet, ...). Le LTE fait l'objet de notre travail, et sera traité en détail du chapitre suivant.

### I.5 La cinquième génération (5G)

La 5G est le réseau mobile de 5ème génération. Il s'agit d'une nouvelle norme mondiale sans fil après les réseaux 1G, 2G, 3G et 4G. La 5G permet un nouveau type de réseau conçu pour connecter pratiquement tout le monde, y compris les machines, les objets et les appareils.

La technologie sans fil 5G est destinée à offrir des débits de données de point multi-Gbit/s, une latence ultra faible, plus de fiabilité, une capacité réseau massive, une disponibilité accrue et une expérience utilisateur plus uniforme pour un plus grand nombre d'utilisateurs. Des performances plus élevées et une efficacité améliorée permettent de connecter de nouvelles industries.

Tout d'abord, la 5G doit permettre de répondre à l'explosion de notre consommation de data. Selon les opérateurs, les données augmentent de 40% par an. À ce rythme, le réseau 4G sera saturé d'ici un à deux ans. En 2025, en effet, un utilisateur consommera 200 Go tous les mois. Voilà donc le premier intérêt de la 5G : éviter la saturation du réseau dans les zones très denses, comme les gares, les aéroports ou encore les stades, en lui apportant de l'oxygène grâce à de nouvelles fréquences. 310 MHz dans la bande des 3,5 GHz ont ainsi été vendus aux enchères aux opérateurs. En outre, les opérateurs peuvent basculer en 5G les fréquences dont ils disposent pour la 4G, à savoir les bandes 700, 800 et 900 MHz, ainsi que dans les bandes 1,8, 2,1 et 2,6 GHz. Enfin, dans les années plus tard, ( pas avant 2022 ou 2023), la bande de fréquences des 26 GHz sera également attribuée à la 5G [6].

L'architecture de la 5G est très avancée, ses éléments de réseau et divers terminaux sont typiquement mis à niveau. De même, les fournisseurs de services peuvent mettre en œuvre la technologie avancée pour adopter facilement les services à valeur ajoutée.

Cependant, l'évolutivité est basée sur la technologie radio cognitive qui comprend diverses caractéristiques importantes, telles que la capacité des appareils à identifier leur emplacement géographique ainsi que la météo, la température, etc. La technologie radio cognitive agit comme un émetteur-récepteur (faisceau) qui peut capter et répondre de manière perceptive avec signaux dans son environnement d'exploitation. De plus, il distingue rapidement les changements de son environnement et réagit donc en conséquence pour fournir un service de qualité ininterrompu.

## I.6 Conclusion

Dans ce chapitre introductif, nous avons vu les technologies autour des réseaux mobile, qui sont évolués et leur développement qui s'est déroulé en plusieurs étapes, afin d'améliorer votre expérience utilisateur.

Ce développement a commencé par le réseau 1G, qui s'agit d'une toute première génération accessible par le biais de téléphone analogique, Ensuite la 2G, c'était le premier réseau qui marque le passage de l'analogique vers le numérique et qui ne permettaient que du transport de voix et des SMSs en mode circuit, il est toujours actif. Puis le déclenchement de la GPRS et l'EDGE pour accélérer le transfert des données avec un débit limité.

L'amélioration ne s'arrête pas, la 3G est venue pour accompagner la génération des Smartphone dans le monde et le premier mobile avec haut débit, conçu pour la transmission de la voix avec les données. La 3G prend en charge la voix sur circuit et les données en mode paquet contrairement à la 4G qui est basé uniquement sur IP (mode paquet). Maintenant vient la 5G, qui ne représente pas une évolution des réseaux précédents, mais elle correspond à une nouvelle fondation technologique développée, pour but de soutenir les demandes croissantes des clients.

Dans le chapitre suivant, nous verrons ce que la technologie 4G LTE nous apporte comme innovations par rapport les générations qui le précède.

## Chapitre II :

---

### *Le LTE et la voix sur LTE (VoLTE)*

---

## II.1 Introduction

Le monde des télécommunications est toujours en mouvement .La 4G est la quatrième génération des standards pour la téléphonie mobile. L'une des caractéristiques de la 4G est d'être un réseau mobile tout IP, ne permettant pas les appels voix par commutation de circuit comme c'est le cas pour la 2G ou 3G. Bien sûr, des appels téléphoniques sont possibles sur un mobile supportant la 4G, mais l'appel est effectué sur le réseau 2G ou 3G, alors que le réseau 4G LTE s'appuie sur la commutation de paquet IP pour le transport des communications vocales et des SMS. En 2014, les opérateurs mobiles ont commencé à déployer la norme VoLTE pour prendre en charge les appels vocaux grâce à une procédure appelée « CSFB » (Circuit Switch Fall-Back).

Dans ce chapitre on va essayer de présenter la technologie LTE, son architecture et plus essentiellement la voix sur LTE (VoLTE). Par la suite, on parlera en détail de l'architecture sur les différentes solutions de la VoLTE, ses éléments et son principe de fonctionnement.

## II.2 Réseaux radio mobiles 4G LTE

La 4G LTE est le nom d'un projet au sein du 3GPP (Organisme de standardisation), visant à rédiger les normes techniques de la future quatrième génération en téléphonie mobile. Elle permet le « très haut débit mobile », c'est-à-dire des transmissions de données à des débits théoriques supérieurs à 100 Mbit/s.

La LTE s'inscrit dans la continuité des réseaux 3G, et basée sur deux techniques radios telles que l'OFDMA et le MIMO pour un transfert de données à très haut débit, avec une large portée, un plus grand nombre d'appels par unité et moins de latence.

Une des particularités de la 4G est d'avoir un cœur de réseau basé sur IP et de ne plus offrir de mode commuté (établissement d'un circuit pour transmettre un appel "voix"), ce qui signifie que les communications téléphoniques utiliseront la voix sur IP (en mode paquet).

LTE implique de modifier le cœur du réseau, les émetteurs radio et de développer des terminaux mobiles adaptés. De même, ils permettraient de généraliser des usages tels que la télévision mobile personnelle, le téléchargement, le streaming, la vidéoconférence...

### II.2.1 Architecture de la 4G LTE

L'architecture du réseau LTE (voir la figure II.1) est assez différente de l'existant en téléphonie mobile 2G et 3G, il n'y a plus de contrôleurs radio entre les antennes-relais et le cœur de réseau. Le réseau LTE est constitué de deux domaines :

- Le réseau d'accès, appelé LTE ou E-UTRAN (Evolved-UTRAN)
- Le réseau cœur, appelé EPC ou SAE.

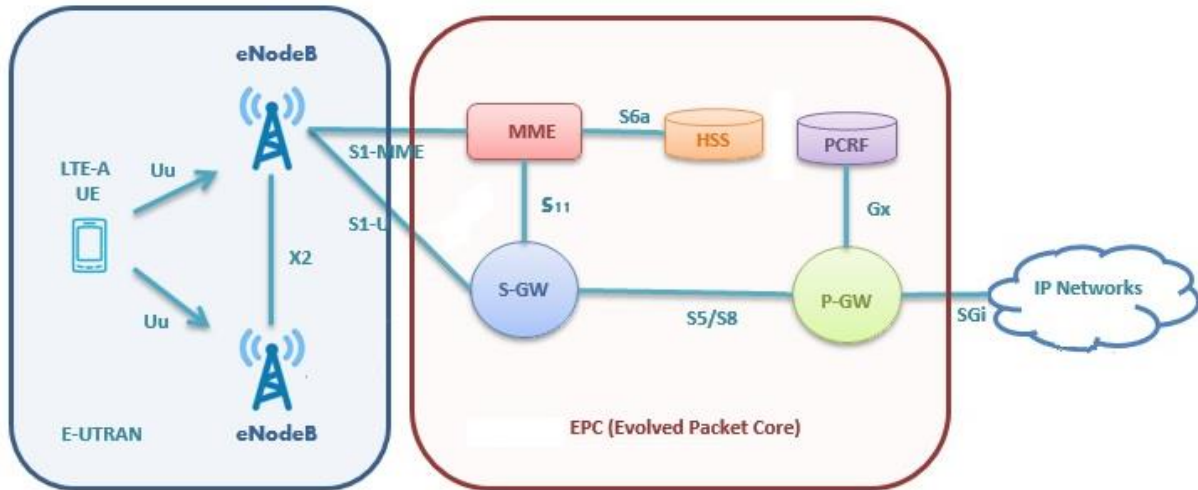


Figure II.1 : Architecture du réseau LTE [7].

### II.2.1.1 Le réseau d'accès LTE

Le réseau d'accès E-UTRAN assure la connexion des mobiles et la réservation des ressources radio entre le mobile UE (User Equipment) et l'entité eNB (evolved Node Base station), sur une bande de fréquences (LTE) ou sur plusieurs bandes de fréquences (LTE-Advanced) [8].

**eNodeB :** L'eNodeB est l'équivalent de la BTS dans le réseau GSM et NodeB dans l'UMTS, Ce sont des antennes qui relient l'équipement utilisateur (UE) avec le réseau cœur du LTE via les RF air interface. Ainsi, il est responsable de la transmission et de la réception radio avec l'UE, qui est basé sur la technologie MIMO. Cette entité est offre deux qualités au réseau :

- La sécurité : en cas de problème d'un relais.
- Un partage des ressources équitable : en cas de saturation du lien principale.

On distingue deux interfaces dont dispose l'eNodeB soit SI et X2 :

**L'interface SI :** c'est l'interface intermédiaire qui relie l'E-UTRAN aux composants de l'EPC. Elle est divisée en deux interfaces élémentaires :

- SI-C (SI-Contrôle) entre l'eNodeB et le MME, qui est utilisée pour l'établissement du support (bearer) radioélectrique et pour le paging et pour la gestion de la mobilité.
- SI-U (SI-Usager), qui est situé entre l'eNodeB et le Serving GW et qui est supporté uniquement le trafic du mobile.

**L'interface X2 :** est relie les eNodeB adjacents. Son rôle est de réaliser des échanges de données et de signaux de connexion entre différents UTRAN, ainsi sa fonction principale est de minimiser la perte de paquets lors de la mobilité intercellulaire de l'utilisateur en mode ACTIF (handover).

### II.2.1.2 Le réseau cœur EPC

Le cœur de réseau appelé « EPC » (Evolved Packet Core) utilise des technologies « full IP », c'est-à-dire, basées sur les protocoles Internet pour la signalisation, le transport de la voix et des données. Ce cœur de réseau permet l'interconnexion via des routeurs avec les eNodeB distants, les réseaux des autres opérateurs mobiles, les réseaux de téléphonie fixe et le réseau Internet [9].

L'EPC d'un opérateur LTE est principalement constitué de deux parties (Figure II.2) :

**Plan d'utilisateur (User Plane) :** Constituent les passerelles de services, Serving Gateway (SGW), qui transportent le trafic de données et concentrent le trafic de plusieurs eNodeB. Un ou plusieurs PGW servent de passerelles vers le réseau Internet, le PGW a aussi pour rôle d'attribuer les adresses IP aux terminaux LTE.

**Plan de signalisation (Control Plane) :** Gère la mobilité et le rattachement des abonnés sur le réseau, il s'agit du MME. Une base de données permettant entre autre d'authentifier l'abonné, de consulter leurs abonnements et de chiffrer les communications, il s'agit du HSS. Une politique de tarification, qui permet de gérer l'accès au réseau de données (PDN) en fonction du forfait de l'abonné, il s'agit du PCRF.

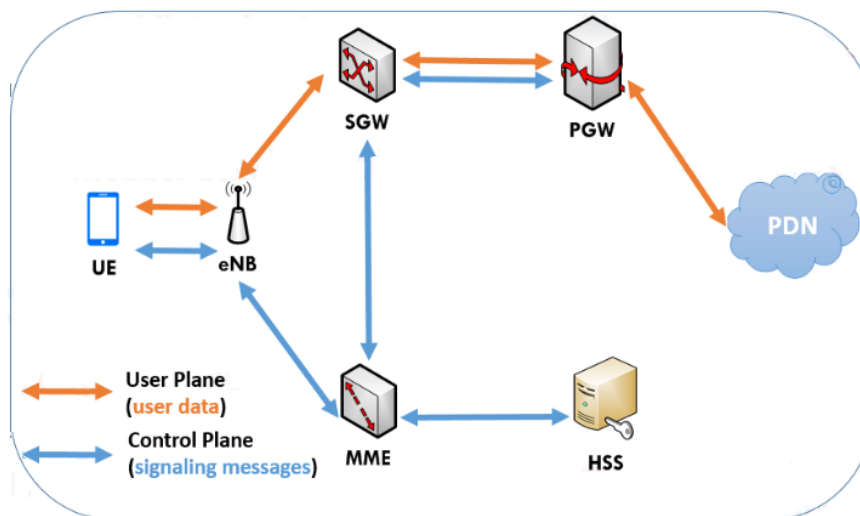


Figure II.2 : Architecture plan d'utilisateur et plan de signalisation [10].

Le chemin du plan de contrôle va de l'UE à l'eNodeB, puis au MME puis au HSS et au SGW puis du SGW au PGW. Tandis que le chemin du plan utilisateur va de l'UE à l'eNodeB, puis de l'eNodeB directement à la SGW puis de la SGW à la PGW et de la PGW à la PDN.

**MME :** fait référence à l'entité de gestion de la mobilité. MME est responsable de l'authentification de l'UE. En outre, il est responsable à la poursuite de l'emplacement de l'UE et la sélection d'une bonne SGW. Comme il réalise le dernier point de la protection par codage, donc par conséquent, c'est le point qui valide l'interception de signalisation. Ainsi, qu'elle contrôle le signal entre le UE (Utilisateur

Equipment) et le réseau cœur, et assure l'établissement, la maintenance, et l'élargissement de la porteuse radio services.

**S-GW (Serving GetWay)** : c'est la jonction principale entre le réseau radio accès et le réseau cœur, qui achemine les paquets de données et maintient la connexion de l'inter-eNodeB Handover, puis inter-système Handover entre LTE et GSM/UMTS et réserve le contexte du terminal mobile (UE), comme les paramètres de la porteuse service et le routage des informations [9].

**P-GW (Packet-Switch GetWay)** : Fournit la connectivité au terminal mobile (UE) vers le paquet externe du réseau de l'information et alloue les adresses IP d'un UE, ainsi que les applications de la QoS, et maintient la connexion mobile entre LTE/UMTS/GSM systèmes et le non 3GPP système.

**HSS (Home Subscriber Server)** : Une base de données centrale pour les abonnés 4G, similaire au HLR en GSM, authentifie un utilisateur sur la base de vecteurs d'authentification, stocke le profil d'abonnement des utilisateurs de réseau et porte l'appel de control et la session management. Elle est désignée aussi à l'autorisation, la sécurité, le débit et fournit une localisation détaillée à l'utilisateur.

**PCRF (Policy and Charging Rules Function)** : Responsable sur la décision principale du control. Il fournit une QoS d'autorisation pour décider le traitement des données en respectant l'abonnement des utilisateurs [9].

La fonction de contrôle des politiques et des règles de facturation est responsable de la prise de décision en matière de contrôle des politiques, ainsi que du contrôle des fonctionnalités de facturation basées sur les flux dans la fonction d'application du contrôle des politiques (PCEF), qui réside dans la P-GW. Le PCRF fournit l'autorisation QoS (identificateur de classe QoS [QCI] et débits binaires) qui décide comment un certain flux de données sera traité dans le PCEF et s'assure que cela est conforme au profil d'abonnement de l'utilisateur.

PCRF assure la gestion du service et le contrôle du service 4G. Il gère et contrôle dynamiquement les sessions de données, permet de nouveaux modèles commerciaux. En dehors de cela, PCRF LTE a également la fonctionnalité de faciliter l'accès d'autres appareils hors du réseau 3GPP - comme le Wifi ou les appareils haut débit fixes - au réseau 4G LTE.

En d'autres termes, PCRF LTE est le gestionnaire de politique de la nouvelle technologie 4G LTE. Toutes les règles et réglementations de qualité de service (QoS) sont distribuées à la passerelle du réseau de données par paquets par le PCRF LTE, ce qui en fait un aspect très précieux de la politique et du système de gestion de la sécurité de toute organisation.

Le serveur de politique ou PCRF est un élément clé du NDN. Il fournit le lien critique entre les couches de service et de transport et est le point de décision central - le cerveau - des réseaux LTE. Le



PCRF fournit le contrôle granulaire de la qualité de service, ce qui est essentiel pour gérer les ressources, permettre une itinérance transparente, établir de nouveaux modèles commerciaux et monétiser les services.

Un concept LTE fondamental est la capacité de reconnaître et de différencier les flux de trafic. Le degré et la granularité avec lesquels ce flux peut être influencé dynamiquement déterminent en grande partie la mesure dans laquelle un opérateur peut façonner la bande passante, mettre en œuvre la QoS, gérer l'allocation des ressources et créer de nouvelles applications. C'est là que la politique entre en jeu. Le PCRF est l'élément clé du réseau qui permet ce contrôle précis, essentiel pour gérer et monétiser avec succès les réseaux LTE. En tant que tel, il s'agit d'un élément stratégique et d'une considération dans la conception du réseau LTE.

Afin de bien comprendre l'architecture du réseau LTE, nous devons savoir quelle est la différence entre le plan de contrôle et le plan utilisateur.

Les nœuds utilisent le plan de contrôle pour échanger des messages de signalisation entre eux. Les messages de signalisation contrôlent la session de données de l'UE. À l'aide des messages de signalisation, les nœuds peuvent initier une modification ou mettre fin à la session de données de l'UE. Pendant que les nœuds utilisent le plan utilisateur, afin d'échanger les données utilisateur envoyées et reçues entre l'UE et le PDN.

### II.3 Solutions pour la Voix sur LTE

Le LTE est un système IP complet conçu exclusivement pour l'acheminement des données, il ne permet pas la transmission de la voix.

Tout comme les lignes fixes ou la voix sur IP ont été déployées depuis longtemps, afin d'établir des appels et de transmettre la voix au cœur d'un réseau LTE, une solution différente était nécessaire qui permet la prise en charge de la voix sur IP (VoIP) et la mise en œuvre d'une infrastructure IMS qui offre un service vocal tout en se connectant au réseau LTE, que nous appelons cela "VoLTE".

Le réseau IMS est essentiellement utilisé pour fournir les services basiques de la voix qui sont fournis par les réseaux CS existants, il s'appuie sur le protocole SIP et offre une meilleure qualité de service pour les flux vocaux. En plus de ceci il fournit des services multimédia avancés comme les vidéoconférences et les jeux en ligne (Real time gaming).

La technologie VoLTE été normalisée en 2014 par l'organisme 3GPP et le GSMA et concerne désormais une très large majorité des opérateurs. Cette option est aujourd'hui disponible chez Bouygues Telecom, Orange, SFR et autres. L'architecture d'une solution de la VoLTE est donnée par la figure II.3.

Il faut comprendre qu'à l'origine, la 4G était uniquement dédiée à la navigation sur Internet. Quand vous vouliez passer un coup de fil, votre téléphone basculait sur la 2G ou 3G. C'est notamment ce qui expliquait parfois un petit temps de latence avant que le téléphone de votre destinataire ne commence à sonner. Avant cela pouvait durer de 8 à 9 secondes. Aujourd'hui, ce n'est (presque) plus le cas, on parle en moyenne de 2 secondes. Par ailleurs, grâce à la VoLTE, il est donc possible de téléphoner et de conserver une bonne qualité pour naviguer sur Internet [11].

A cet effet, afin d'assurer un service de voix sur les nouveaux réseaux 4G. L'organisme 3GPPa proposé plusieurs solutions :

- CSFB (Circuit Switched FallBack),
- VoLGA (Voice over LTE via Generic Access),
- IMS (IP Multimedia Subsystem).

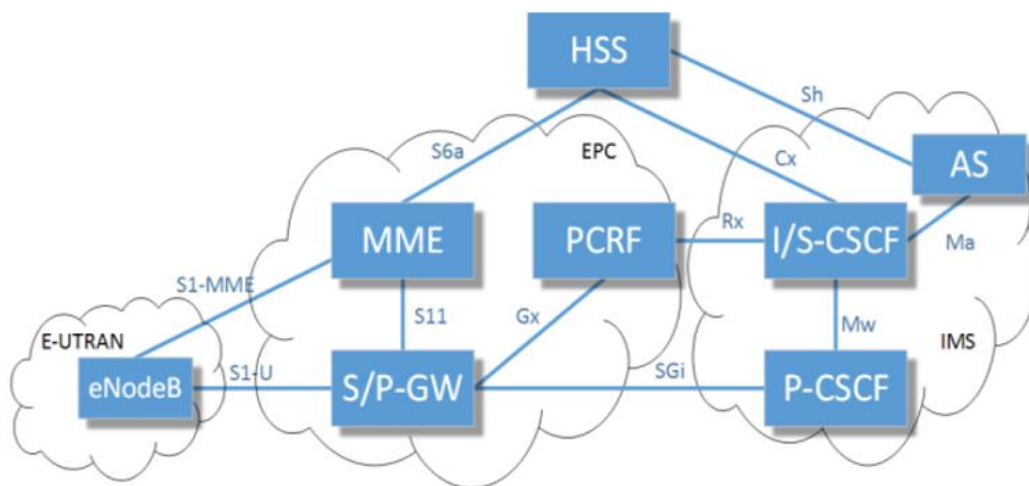


Figure II.3 : Architecture de la VoLTE [12].

### II.3.1 CSFB (Circuit Switched Fall Back)

CS Fallback est le mécanisme pour déplacer un abonné à partir de LTE vers une autre technologie comme le GSM, L'UMTS ou le CDMA2000 qui fonctionnent tous à commutation de circuit. Il est consisté tout simplement à continuer d'utiliser le réseau 2G/3G pour les services de téléphonie et à réserver le réseau 4G aux services de transmission de données.

Le principe du CS Fallback est assez simple : Lorsqu'un terminal mobile reçoit un appel téléphonique (Voix), il est informé via le message de Paging que le réseau auquel il doit accéder est le réseau de Commutation de Circuit (CS). Par conséquent, si le mobile était attaché sur le réseau 4G, il bascule vers le réseau 3G, et le mobile envoie une réponse d'acquiescement vers le cœur de réseau en commutation de circuit (CS-Core). A partir de ce moment, toute la signalisation pour la session d'appel téléphonique est prise en charge par le réseau 3G [13].

Pour que le Cœur de réseau 4G (EPC : Evolved Packet Core) soit compatible avec la technologie CSFB, il est nécessaire que ce dernier puisse communiquer avec le cœur de réseau en commutation de circuit CS-Core du réseau 2G/3G. En effet, le MME (mobilité Management Entity) doit pouvoir contacter le MSC (Mobile Switch Center) et la VLR afin de donner procuration au réseau 2G/3G de la gestion de la mobilité. L'interface utilisée se nomme SG, et fait référence, en reprenant son rôle, à l'interface Gs existante entre le SGSN et le MSC dans le réseau 3G.

Lorsque l'appel est accepté, la technologie CSFB utilise à nouveau l'interface SG pour informer le réseau LTE de l'acceptation de l'appel. L'acquiescement est donc transmis par le réseau en Commutation de Circuit (CS) vers le réseau LTE en empruntant l'interface SG [13]. L'architecture réseau de CS fallback est illustrée dans la figure II.4 :

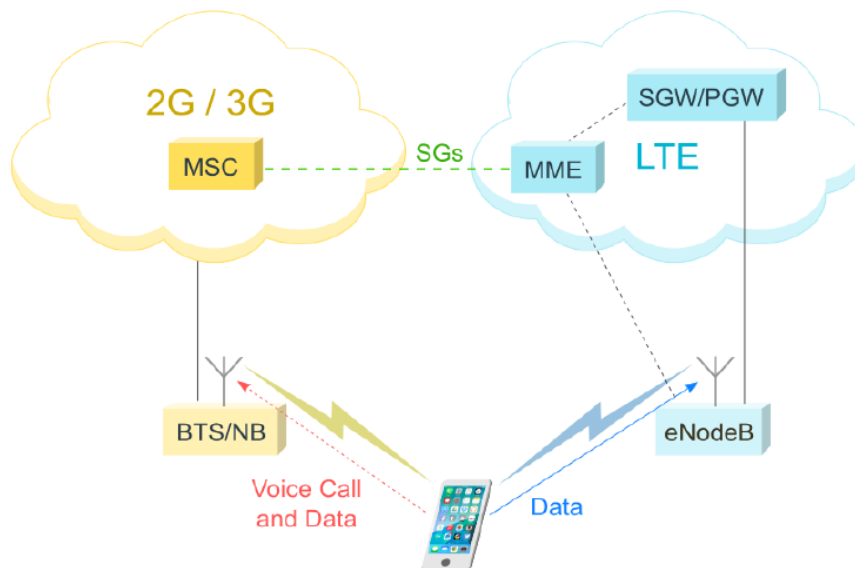


Figure II.4 : Architecture de la solution CSFB [15] .

Le point critique du CSFB est la durée du processus, principalement le temps qu'il faut à l'UE pour quitter la connexion 4G et se retrouver sur la connexion 3G. En raison de retards liés au repli et à la récupération, l'établissement d'appel de latence est pire que pour les réseaux 2G / 3G originaux. Il serait ainsi impossible par exemple, de proposer des services combinant voix et données en tirant profit du débit 4G (conférence, collaboration, jeux ...).

Il s'agit là des principaux écueils du CSFB qui souffre en outre d'autres insuffisances (mauvaise intégration avec de potentielles LTE, mauvaise occupation de la bande radio ...).

En résumé, le CSFB offre l'avantage de permettre une réutilisation complète de l'infrastructure existante (réseau, services, systèmes de facturation..), en ne nécessitant que quelques mises à jour mineures. Cependant il s'agit là d'une solution permettant plus de prolonger la vie du réseau 2G/3G

existant que de tirer profit de l'introduction de la 4G, ce qui risque de réduire fortement l'intérêt de déployer cette nouvelle technologie [14].

### II.3.2 VoLGA (Voice over LTE via Generic Access)

VoLGA est une solution de migration alternative, qui consiste à ajouter des passerelles dans le cœur de réseau pour transférer les appels et SMS du réseau 4G vers le réseau 2G/3G. La passerelle est donc située pour permettre la communication entre l'EPC et les MSC. Cette Gateway se nomme VoLGA Access Network Controller (VANC) et agirait comme une BSC qui transite des paquets IP.

Cette seconde solution permet également de réutiliser l'infrastructure voix existante mais de manière un peu plus évoluée. Elle consiste à connecter le réseau EPS au cœur de réseau NSS qui fournit le service téléphonique 2G/3G par l'intermédiaire d'une passerelle VANC (VoLGA Access Network Controller). La signalisation 2G/3G de la téléphonie est ainsi réutilisée mais est transportée sur le réseau de données 4G en étant encapsulée au sein de paquets IP. Le réseau EPS joue alors le rôle de réseau d'accès au même titre que le BSS (Base Station Sub-system) du réseau 2G ou l'UTRAN (UMTS TRANsport Network) du réseau 3G [14].

VoLGA prend en charge deux modes de fonctionnement soit mode A VoLGA et mode lu VoLGA :

- **Le mode A VoLGA** : prend en charge une extension des services GSM CS qui est obtenue en tunnel lisant les protocoles NAS (Non Access Stratum) entre l'UE et le réseau central sur les supports EPS et l'interface A vers le MSC.
- **Le mode VoLGA lu** : prend en charge une extension des services UMTS CS qui est obtenue en tunnel lisant les protocoles NAS (Non Access Stratum) entre l'UE et le réseau central sur les supports EPS et l'interface lu-CS vers le MSC.

#### II.3.2.1 VoLGA dans le réseau

La figure II.5 donne un aperçu de la configuration de base du réseau pour VoLGA dans le réseau domestique comme décrit dans la spécification VoLTE (Voice over LTE).

Pour un démarrage facile, les interfaces optionnelles qui permettent une qualité de service explicite dans le réseau LTE et celles nécessaires pour transférer les appels vocaux en cours vers un réseau à commutation de circuits ne sont pas représentées.

Cette solution présente l'avantage de n'apporter aucune modification tant au niveau du réseau EPS que du cœur de réseau NSS. Par contre, le mobile doit intégrer des adaptations pour le transport, sur le réseau 4G, de la signalisation NAS (Non Access Stratum) échangée entre le mobile et le réseau NSS [14].

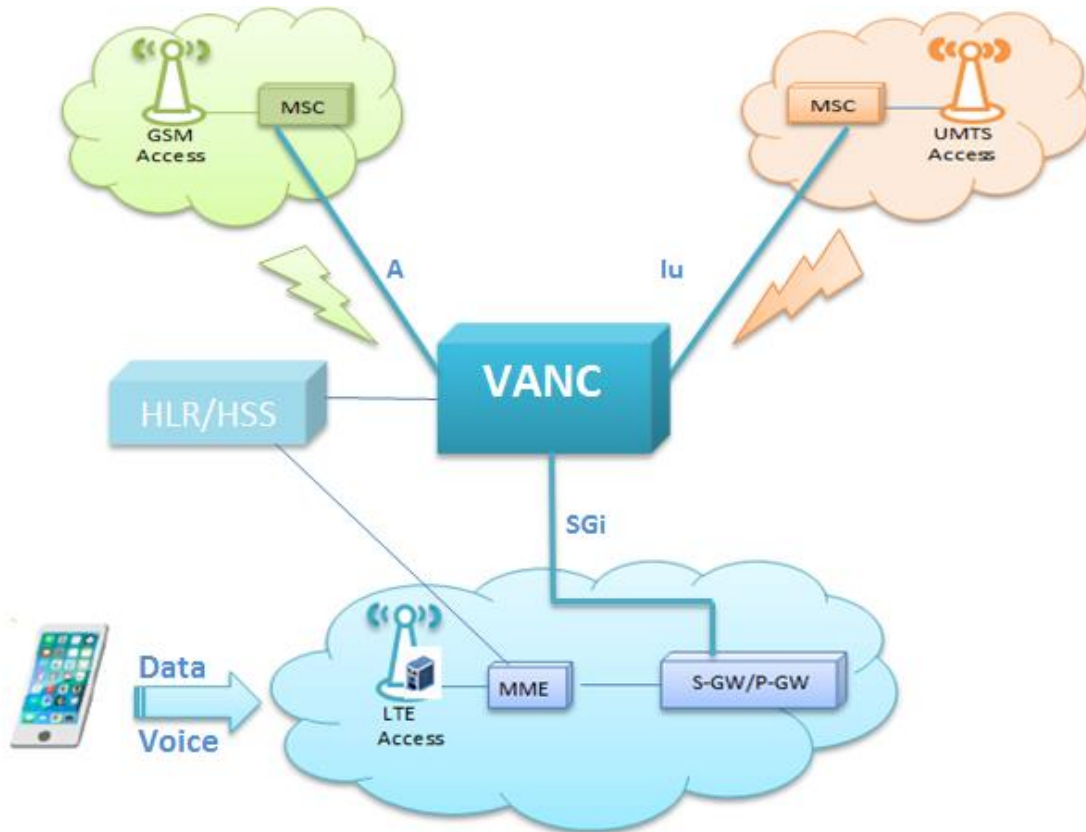


Figure II.5 : Architecture de la solution VoLGA.

VoLGA permet de réutiliser l'infrastructure existante, ce qui assure un déploiement rapide ainsi qu'une transparence complète du réseau vis-à-vis des services téléphoniques. De plus, VoLGA ne souffre pas des défauts majeurs de CSFB en assurant un accès simultané aux services voix 2G/3G et données LTE. Au niveau du réseau, VoLGA ne nécessite que le déploiement de quelques nouveaux éléments (VANC principalement). Le terminal, en revanche, devra également intégrer cette nouvelle technologie afin d'être en mesure d'encapsuler la téléphonie 2G/3G dans des paquets IP.

Le support de VoLGA dans le terminal constitue le principal obstacle à son adoption, car cela nécessite un support fort des fournisseurs de mobiles pour une technologie de transition, qui n'a pas vocation à être utilisée sur le long-terme. Ce point est de plus exacerbé par le fait qu'il s'agit d'une technologie non adoptée par le 3GPP, l'organisme qui est en charge des spécifications GSM et LTE. Par ailleurs, VoLGA, comme CSFB, ne permet pas de véritables services de convergence car les réseaux gérant la voix et les données restent séparés [14].

### II.3.2.2 VoLGA du point de vue du réseau LTE

Du côté LTE, le VANC se connecte à la passerelle de réseau de données par paquets (P-GW) via l'interface S-Gi standard. La signalisation et le trafic de données utilisateur (c'est-à-dire les paquets vocaux) sont transportés sur cette interface. Du point de vue du réseau central LTE, le VANC ressemble à tout autre

nœud externe basé sur IP et les paquets IP échangés entre un appareil sans fil et le réseau Evolved Packet Core (EPC). Ils sont transmis de manière transparente via le réseau Evolved Packet Core (EPC).

### II.3.2.3 Le VANC

Le VANC se comporte comme un BSC (VoLGA A-mode) ou RNC (VoLGA lu-mode) vis-à-vis du domaine CS. Le VANC se comporte également comme une fonction d'application (AF) vis-à-vis du PCRF. Le VANC comprend une fonction de passerelle de sécurité (SeGW) qui termine un tunnel d'accès à distance sécurisé à partir de chaque UE, fournissant une authentification mutuelle, un cryptage et une protection de l'intégrité pour le trafic de signalisation.

### II.3.2 VoLTE via IP Multimedia Subsystem (IMS)

La dernière solution est un système autonome, qui est représentée comme la solution cible à long terme est celle de la mise en œuvre de l'IMS. Il réside en dehors du réseau LTE et est connecté à la passerelle PDN via l'interface SGI. L'IMS a été conçu à l'origine par l'organisme de normalisation sans fil 3GPP, dans le cadre de la vision de l'évolution des réseaux mobiles au-delà du GSM.

L'IMS repose sur une évolution du protocole UMTS (3G version 5), conçue pour supporter une surcouche réseau indépendante du type d'accès (UMTS, WLAN, GPRS, DSL, etc.). L'architecture est également compatible avec des réseaux plus anciens par le biais de passerelles, notamment GSM. Basé sur le protocole IP (Internet Protocol), elle assure la connexion entre les différentes infrastructures réseau en présence, et contrôle les sessions et appels, voix et multimédia. Dans cette optique, l'IMS gère à la fois les flux voix et données [16]. La figure II.6 représente l'architecture de la solution VoLTE via IP Multimedia Subsystem (IMS).

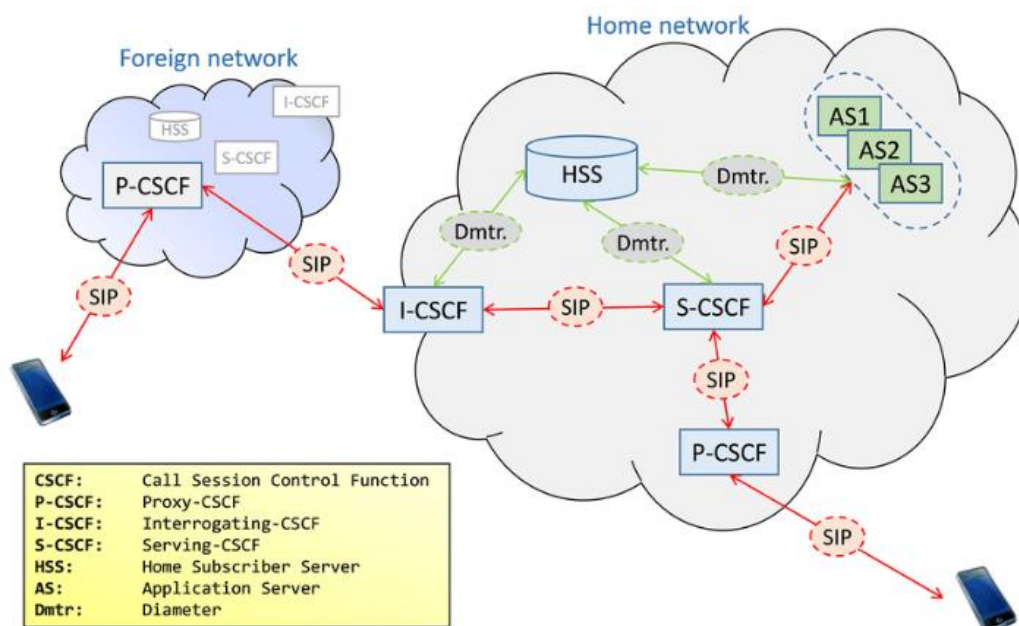


Figure II.6 : Architecture de la solution VoLTE via IMS [16].

Le réseau IMS est basé sur l'emploi du protocole de signalisation SIP (sessions Initiation Protocol), qui permet l'enregistrement du mobile au service téléphonique et l'établissement d'une session et du protocole SDP (Session Description Protocol), associé au protocole SIP, qui supporte la négociation du média (voix, vidéo, données). La seconde fonction assurée par l'architecture IMS, concerne le traitement du flux média pour les fonctions indisponibles dans le réseau 4G comme la conférence, la génération des annonces et les passerelles vers les réseaux téléphonique fixes PSTN (Public Switched Téléphone Network) et les réseaux de mobiles PLMN (Public Mobile Network) [14].

Cette solution sera d'autant plus facile et moins risquée à déployer dès le début que l'opérateur dispos déjà d'une infrastructure IMS opérationnelle sur d'autres réseaux d'accès, ADSL par exemple. Afin de réduire ce risque lié à l'introduction immédiate d'un nouveau système complexe, les principaux acteurs de la téléphonie ont lancé l'initiative One Voice. Cette initiative a conduit à la définition d'un sous-ensemble de fonctionnalités IMS définies par le 3GPP. Ce sous-ensemble permet ainsi de simplifier le déploiement de l'IMS dans un cadre LTE tout en garantissant une interopérabilité maximale.

La figure II.7 présente un résumé des avantages et des inconvénients de trois solutions de la VoLTE citées précédemment.

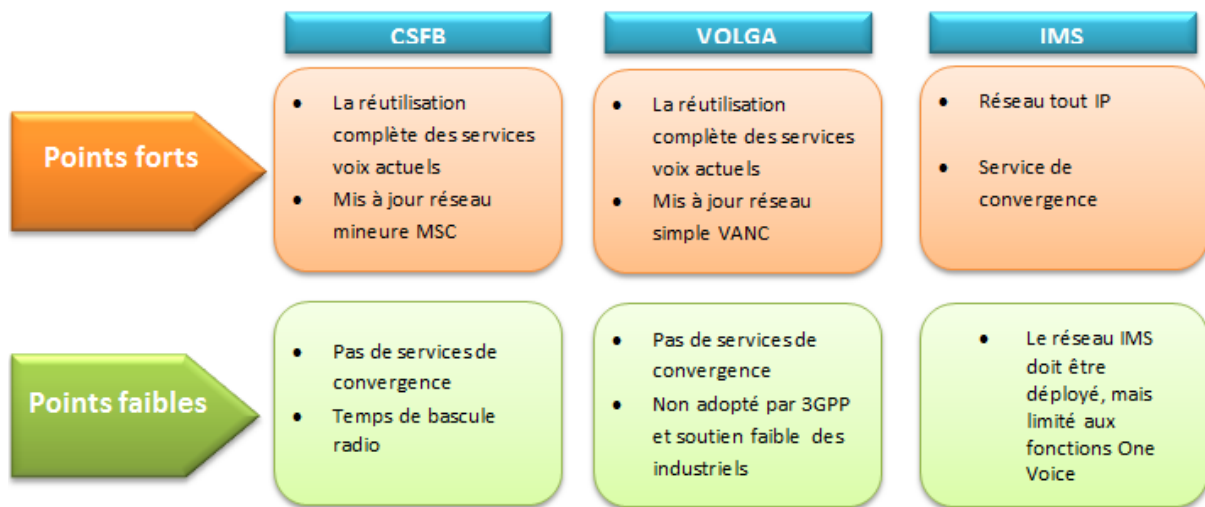


Figure II.7 : Points forts et faibles des solutions CSFB, VoLGA et IMS.

#### II.4 La différence entre LTE et la VoLTE

En termes simples, VoLTE est une amélioration par rapport à LTE. En résumé la différence entre ces deux technologies dans le tableau ci-dessous :

	LTE	VoLTE
<b>La définition</b>	Une norme de communication sans fil haut débit.	Une norme de communication sans fil haut débit, y compris les appareils connectés à l'internet des objets (IoT) et les dispositifs portables.

<b>La signification</b>	Long Term Evolution.	Voice Over Long Term Evolution.
<b>Support simultané</b>	Peut ou non prendre en charge simultanément les services d'appel vocal et de données.	Prend en charge simultanément les services d'appel vocal et de transmission de données.
<b>La qualité de la voix</b>	Peut réduire la qualité de la voix lors de l'utilisation simultanée de données et de la voix.	N'affectera pas la qualité de la voix si vous utilisez à la fois la voix et les données.
<b>Vitesse de connexion de l'appel</b>	Lent.	Elevée, supérieure à celle du réseau LTE

**Tableau II.1** : Comparaison entre LTE et VoLTE.

## II.5 Conclusion

Ce chapitre intitulé la 4G (LTE) et la solution de VoLTE, a pour but de décrire la technologie 4G LTE, qui permet le transfert de données avec un très grand débit et une portée très importante. LTE est un réseau mobile tout IP, ne permet pas les appels voix. Bien entendu, la voix reste le service le plus important, que le LTE peut offrir une multitude de solutions pour sa prise en charge.

La technique VoLTE considérée comme la solution principale de la voix pour les utilisateurs LTE. Elle fait une migration du service vocal à commutation circuit vers la commutation de paquets. Pour ce faire, cette technologie a donc besoin d'une architecture IP Multimedia Subsystem (IMS) qui aidera à la gestion et pour conserver les appels directement sur le réseau LTE. Alors que la VoLTE devait définir un profil pour la voix sur LTE utilisant l'IMS.

Le prochain chapitre étudiera la solution IP Multimedia Subsystem pour la prise en charge de la voix sur LTE.



## Chapitre III :

---

*La VoLTE via IP Multimedia  
Subsystem (IMS)*

---

### III.1 Introduction

LTE est un réseau IP complet conçu pour le transfert de données. S'orientant vers cette nouvelle technologie, les appels vocaux continuent à représenter une part essentielle dans la gestion des revenus des opérateurs mobiles, et plus de 80 % de leurs revenus de la voix et du SMS. C'est pourquoi ils ont besoin d'une solution stable et normalisée pour fournir ces services sur un réseau LTE dédié principalement au transfert de données à haut débit.

VoLTE, ou Voix sur LTE, qui est présentée comme la solution cible à long terme est celle de la mise en œuvre de l'IMS (IP Multimedia Subsystem) et de la prise en charge de la voix sur IP (VoIP). A l'adoption de l'IMS qui s'est alors imposée comme une architecture multimédia normalisée basé sur l'emploi du protocole de signalisation SIP, en offrant des fonctionnalités clés telles que la qualité de service (QoS), la sécurité, la gestion de groupe, et de messagerie vocale instantanée.

Ce chapitre est consacré au sous-système multimédia IP, ses fonctionnalités et ses caractéristiques pour prendre en charge la VoIP, du point de vue LTE.

### III.2 Présentation de la voix sur IP

VoIP signifie Voice Over Internet Protocol, c'est-à-dire transmission de la voix par Internet. Elle convertit les données, comme la voix ou multimédia, la vidéo ou flux audio, en signal numérique et le transfert via le réseau Internet (IP) en paquets de données numériques.

La VoIP peut faciliter certaines tâches et fournir des fonctionnalités plus difficiles ou plus coûteuses à mettre en œuvre sur les réseaux RTC traditionnels :

- En peut transmettre plus d'un appel sur la même ligne téléphonique haut-débit.
- Les communications unifiées sont sécurisées avec la technologie de la voix sur IP.
- Réductions de coût significatives par rapport à un standard téléphonique traditionnel.
- Les utilisateurs peuvent profiter d'appels gratuits et d'appels internationaux ou longue distance à prix réduits.

### III.3 Sous-système multimédia IP

Le IP Multimedia Subsystem (IMS) est une architecture de réseau conçue pour fournir des services IP multimédias fixes et mobiles (téléphonie, la messagerie, les photos, les vidéos..).

La technologie IMS est définie comme la clé de la convergence vers le tout IP des réseaux et services télécoms. Elle doit permettre aux opérateurs de proposer, sur téléphones mobiles, des services fonctionnant sur IP. IMS est une architecture de service standardisée définie par le 3GPP, l'ETSI et l'IETF basée sur le protocole SIP (Session Initiation Protocol) pour l'initialisation de sessions multimédias, utilisé

pour la visioconférence ou la voix sur IP. L'IMS est adapté aussi bien aux réseaux filaires qu'aux réseaux mobiles. Cela favorisera donc la convergence fixe / mobile. Il permettra également l'interfonctionnement avec les réseaux RTC. L'IMS est la seule architecture de référence pour la convergence fixe / mobile actuellement normalisée [18].

Né de l'IP standard, le sous-système multimedia IP (IMS) utilise des applications VoIP basées sur le SIP. De même, l'IMS utilise d'autres protocoles tels que RTP/RTCP pour la transmission des services à temps réel comme la voix sur IP est assurée.

Il ya des exigences qui ont conduit à la conception de l'IMS 3GPP [19] :

- L'appui à la création de propriété intellectuelle des sessions multimédias.
- Support d'un mécanisme pour négocier la Qualité de Service (QoS).
- Soutien à l'interfonctionnement avec l'Internet et les autres réseaux.
- Support pour contrôle rigoureux imposé par l'exploitant à l'égard des services livrés à l'utilisateur final.
- Soutien à la création d'un service rapide, sans nécessiter l'uniformisation.

### III.4 L'architecture IMS

La plateforme IMS qui en résulte définit les éléments et les fonctions sur quatre couches peuvent être identifiées, chacune d'elles étant liée à un domaine spécifique (Figure III.1).

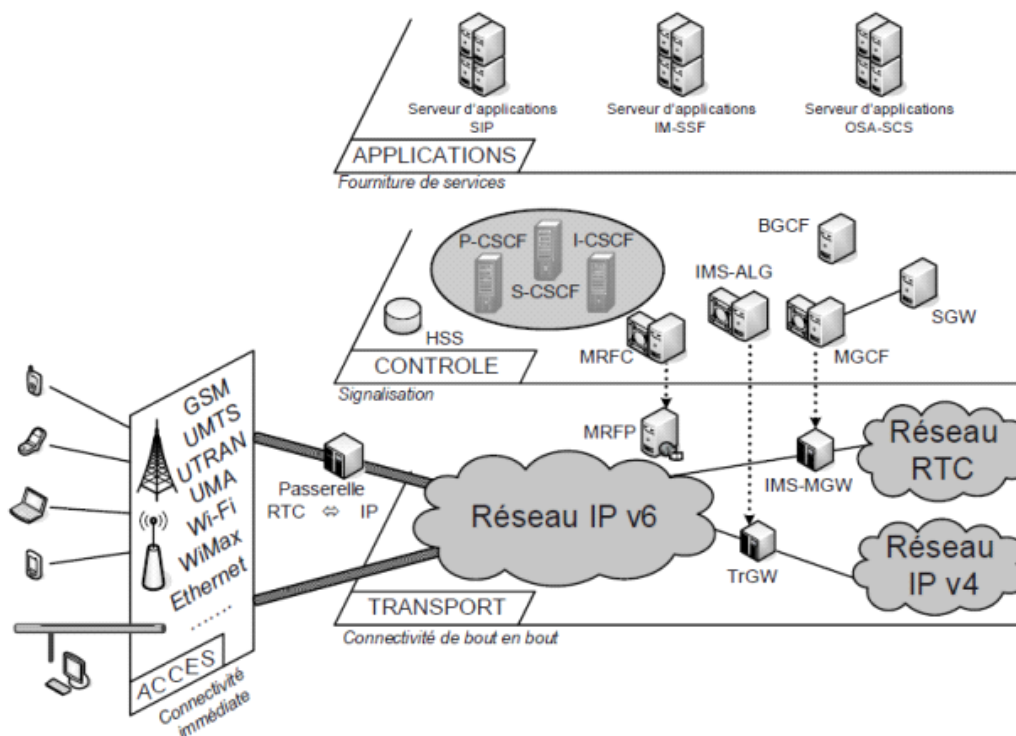


Figure III.1 : Architecture en couches de l'IMS [20].

### III.4.1 La couche accès

Elle définit la manière dont l'utilisateur se connecte au réseau, peut représenter tout accès haut débit tel que : E-UTRAN, GSM, UMTS, CDMA2000, xDSL, Wi-Fi, WiMax, Ethernet, ATM, la fibre optique...etc.

### III.4.2 La couche de transport

Elle représente un réseau IP qu'est formé d'un maillage de commutateurs et de routeurs, le transport de l'information par les routeurs et le choix de la route empruntée.

### III.4.3 La couche de contrôle

La couche de contrôle est la partie intelligente du modèle, qui offre les capacités de contrôle de la fourniture de services au-dessus du domaine IP et gère toutes les sessions SIP établies à travers l'architecture IMS. Elle contrôle en particulier, l'ouverture des sessions SIP et l'établissement des appels. Cette couche comportant le noyau IMS (IMS Core) et d'autres services.

### III.4.4 La couche services et application

Cette couche permet l'exécution et l'offre de services à valeur ajoutés. Elle fournit l'ensemble des applications disponibles dans une architecture IMS qu'ils soient audio, vidéo ou texte. De plus, une couche application comportant les serveurs d'application comme l'AS, intégrant les services IMS et la souscription au serveur maison HSS.

## III.5 Les principaux composants de l'architecture IMS

Comme on peut le voir sur le schéma de la figure III.2, l'architecture IMS repose sur différentes entités, nécessaires à son bon fonctionnement.

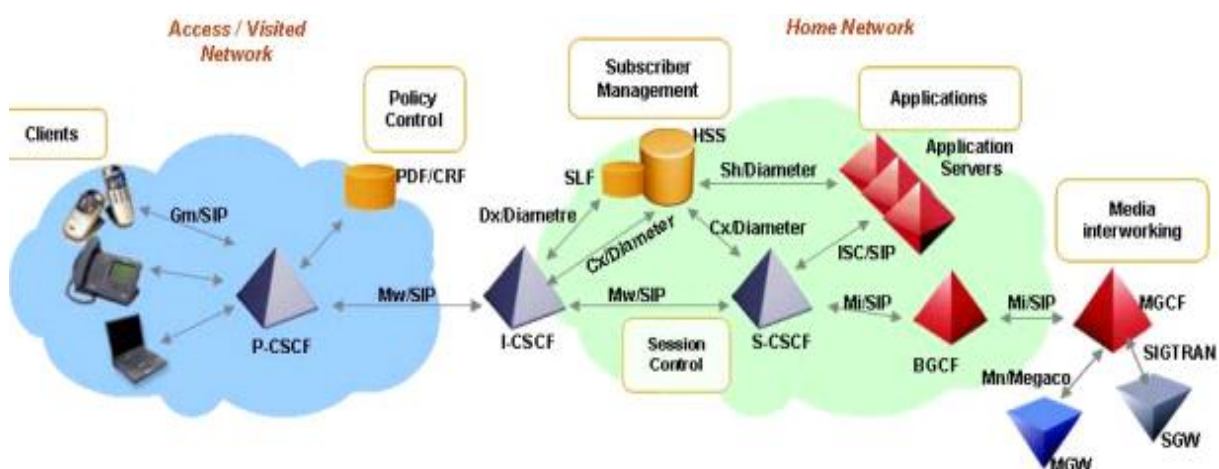


Figure III.2 : Architecture fonctionnelle de l'IMS [22].

### III.5.1 Serveur d'abonné domestique (HSS)

L'entité HSS est une base de données qui stocke différents types d'informations sur les abonnés au réseau IMS. Il contient toutes les informations dont un utilisateur a besoin pour ouvrir une session multimédia :

- Fonction de localisation d'un abonné
- Serveur d'authentification des mobiles
- Le profil de chaque abonné c'est à dire l'ensemble des services auxquels il est souscrit, les informations d'enregistrement, et les profils des serveurs d'application.
- L'adresse du S-CSCF alloué à l'utilisateur.

### III.5.2 Fonction de localisation d'abonné (SLF)

L'entité SLF (Subscription Locator Functional) permet aux entités CSCF de trouver l'adresse de l'entité HSS affectée à un UE, lorsque plusieurs entités HSS sont déployées [21].

### III.5.3 Les serveurs CSCF

Le C-CSCF (Fonction de commande de session d'appel) est un serveur de contrôle de session, qui traite la signalisation SIP en IMS pour communiquer entre les entités. IL est responsable de l'établissement, du suivi, du soutien et de la diffusion des sessions multimédias. Cela a induit la définition de trois entités CSCF suivantes :

#### III.5.3.1 Proxy CSCF (P-CSCF)

Le P-CSCF est le premier point de contact avec le cœur du réseau IMS, il reçoit toute la signalisation SIP envoyée ou dirigée vers l'utilisateur (UE), et peut assurer la compression et la décompression des messages SIP.

Un seul P-CSCF est attribué à chaque abonné pendant la phase d'enregistrement et ne change pas tout au long de la période d'enregistrement. Il maintient également l'association de sécurité entre lui-même et l'utilisateur.

Le P-CSCF peut être localisé dans le home network, comme dans le visited network.

#### III.5.3.2 Interrogating CSCF (I-CSCF)

Le I-CSCF est le point d'accès à un réseau IMS de l'extérieur ou d'un abonné en Roaming qui est toujours localisé dans le réseau nominale (home network) de l'abonné.

L'entité I-CSCF est aussi assure le routage des messages émis ou reçus des autres réseaux vers le S-CSCF. Pour une requête SIP, il contacte le HSS pour identifier le S-CSCF correspondant et renvoie les messages de cette session à ce S-CSCF.

### III.5.3.3 Serving CSCF (S-CSCF)

Le S-CSCF est un serveur SIP prend en charge le contrôle de la session, il est toujours localisé dans le home network.

Les fonctions réalisées par le S-CSCF pendant une session comprennent [22] :

- Le S-CSCF est toujours localisé dans le home network.
- *SIP Registrar* : Il maintient l'association entre l'adresse IP du terminal et le SIP adresse de l'utilisateur (Public User Identity).
- *Télécharger le profil de l'utilisateur de HSS* :
  - A travers les « filtercriteria », le S-CSCF envoie les requêtes SIP satisfaisant ces critères vers des serveurs d'applications correspondant au service demandé. De cette façon il fournit des services de type réseau intelligent (Signalisation d'intelligence),
  - Authentification, enregistrement.
- *Service de translation* : Consultation du DNS pour traduire le TEL-URI en SIP-URI,
- Il obtient l'adresse de l'I-CSCF dans le réseau destinataire lors de l'établissement de session.

### III.5.4 Fonction de commande de passerelle de sortie (BGCF)

Le Breakout Gateway Control Function est essentiellement un serveur SIP qui offre le routage des requêtes en fonction des numéros de téléphone, utilisé pour passer d'un réseau IMS à un réseau de commutation de circuit ou bien pour choisir la bonne passerelle RTC/CS lorsque l'interconnexion a lieu dans le réseau où est situé le BGCF.

### III.5.5 Fonction de contrôle de passerelle média (MGCF)

L'entité MGCF assure l'établissement, le maintien et la libération des connexions dans l'entité MGW. Une connexion représente une association entre une terminaison en entrée (l'interface avec les réseaux tiers PSTN et PLMN) et une terminaison en sortie (l'interface avec le réseau IP) et inversement [23].

### III.5.6 Fonction de passerelle média (MGW)

Interface pour le plan de données entre le réseau IMS/IP et les réseaux PSTN à commutation de circuit. D'un côté, elle capable d'envoyer et de recevoir le flux IMS sur le protocole RTP, d'un autre côté il utilise le PCM pour coder la voix et la transmettre sur des times slots au réseau CS. Une autre fonction de transcodage lorsque le terminal ne supporte pas les codes utilisés par le CS [22].

### III.5.7 Fonction de ressource Multimédias (MRF)

Permet de gérer et traiter des flux multimédias au cours d'une session IMS. Son rôle est de gérer la signalisation vers tous les utilisateurs d'une conférence. Elle se décompose de deux entités logiques :

#### III.5.7.1 MRFC (MultiMedia Resource Function Controller)

La MRFC interprète la signalisation SIP reçu via S-CSCF et pouvant également établir des ponts de conférence entre plusieurs correspondants et assurer le transcodage de médias.

#### III.5.7.2 MRFP (MultiMedia Resource Function Processor)

Est l'équipement qui fournit la ressource média sous le contrôle du MRFC. Pour la partie traitement des flux de données, elle mélange les flux média pour fournir le service de conférence. C'est-à-dire l'application des demandes formulées par l'utilisateur dans les flux.

### III.5.8 Les serveurs d'applications AS [21]

Les serveurs d'applications ou AS (Application Server) sont des entités SIP fournissant différents types de services aux utilisateurs. Ils sont connectés au serveur S-CSCF, qui fait fonction d'intermédiaire entre l'utilisateur et les services. On distingue trois grandes familles de serveurs d'applications, qui sont :

#### III.5.8.1 SIP AS (SIP Application Server)

Ces serveurs permettent l'exécution des services nativement implémentés pour fonctionner avec SIP. Les services les plus classiques (service de présence, push-to-talk, messagerie instantanée, etc.) sont généralement implémentés au sein de ces serveurs.

#### III.5.8.2 IM-SSF (IP Multimedia-Service SwitchingFunction):

Pour permettre la mobilité de l'abonné tout en lui garantissant la fourniture de ses services même s'il se trouve dans une infrastructure qui n'appartient pas à son opérateur de services (on parle de roaming pour désigner la connexion d'un utilisateur à un réseau qui n'est pas celui de son opérateur), il est nécessaire d'avoir une passerelle, appelée IM-SSF, afin de connecter l'abonné au serveur d'applications de son opérateur.

#### III.5.8.3 La passerelle OSA (OSA SCS, OSA Service Capability Server) :

Qui est un type particulier de serveur d'application qui termine la signalisation SIP, et qui interagit avec des serveurs d'application OSA en utilisant l'API OSA.

## III.6 Gestion des identités en IMS

### III.6.1 Identité Privée Multimédia IP

L'identité privée multimédia IP (IMPI) est une identité globale unique attribuée par l'opérateur du réseau domestique, elle a la forme d'un identifiant d'accès au réseau (NAI), c'est-à-dire utilisateur.nom@domaine, et est utilisée pour l'enregistrement, l'identification et l'authentification d'un abonné au réseau IMS. Chaque utilisateur IMS doit avoir un IMPI.

### III.6.2 Identité Publique Multimédia IP

L'identité publique multimédia IP (IMPU) est une identité attribuée par l'opérateur et est utilisée pour le routage de la signalisation SIP.

Utilisée aussi par tout utilisateur pour demander des communications à d'autres utilisateurs. Il peut y avoir plusieurs IMPU par IMPI. L'IMPU peut également être partagé avec un autre téléphone, afin que les deux soient joignables avec la même identité (par exemple, un seul numéro de téléphone pour toute une famille). A un utilisateur IMS est alloué un ou plusieurs User ID Publiques par l'opérateur.

IMPU peut être en trois formats:

- une URI SIP => sip:gaetan.boivin@opérateur.com
- Un numéro de tél => +336xxxxxxx
- Un mix des deux => Sip : +336xxxxxxx@opérateur.com user=phone

## III.7 Protocoles clés utilisés dans le réseau LTE-IMS

### III.7.1 Protocole DIAMETER

Le protocole DIAMETER est un protocole utilisé par les applications informatiques en réseau pour activer l'authentification utilisateur sécurisée, d'autorisation et de comptabilité (AAA). Il fournit les mécanismes de base pour établir un transport fiable, délivrer le message et gérer les erreurs.

DIAMETER peut être le successeur du protocole RADIUS, à qui il a repris les principales fonctions (DIAMETER est compatible avec Radius), et en a rajouté de nouvelles pour s'adapter aux nouvelles technologies (IPv4 Mobile, NASREQ...), et plus particulièrement offrir des services aux applications mobiles.

La fonction AAA dans IMS est partagée entre deux entités. Le HSS fournit la prise en charge de l'autorisation et de l'authentification, et les serveurs de facturation assurent la fonction de comptabilité. Cela permet de fournir un meilleur cadre pour prendre en charge différentes méthodes comptables.



Le profil de service stocké dans le HSS contient les informations pertinentes sur l'identité de l'utilisateur et les services autorisés pour le multimédia. La tâche d'autorisation peut être activée en accédant à ces informations relatives au service. La fonction d'authentification permet de contrôler l'accès du mobile au réseau à partir de l'identité stockée dans la carte SIM et dans la base de données HSS.

Le protocole DIAMETER permet aux entités de contrôle de session et aux serveurs d'application d'assurer la fonction d'autorisation et d'authentification. L'I-CSCF et le S-CSCF communiquent avec le HSS via l'interface Cx/Dx, et de même les serveurs d'application communiquent via l'interface Sh/Dh pour obtenir le profil de service et les informations d'autorisation.

### III.7.1.1 Les messages DIAMETER

Les messages suivants sont échangés entre I-CSCF et le HSS sur l'interface Cx, qui est caractérisée par l'application DIAMETER et qui définit un ensemble de commandes (requêtes/ réponses).

#### a) La requête UAR /UAA

Un message UAR (User Autorisation Request) est envoyé par I-CSCF dès qu'il reçoit une requête REGISTER, au HSS pour les raisons suivantes :

- le HSS vérifie deux conditions :
  - L'identité publique doit être attribuée à un utilisateur légitime du système
  - L'utilisateur ne doit pas être bloqué
- HSS vérifie l'accord de Roaming avec le réseau visité ou se trouve le P-CSCF.
- I-CSCF a besoin de savoir s'il y a un S-CSCF alloué à l'utilisateur pour lui renvoyer le message SIP REGISTER. Sinon l'I-CSCF recevra un ensemble de capacités qui va lui permettre de choisir un.
- Pour vérifier si les deux identités (publique et privée) sont utilisables pour authentifier l'utilisateur, le HSS va les corrélérer.

HSS répond par un UAA (User Autorisation Answer) à l'I-CSCF qui contient le résultat AVP (Result Attribute Value Paires), ce résultat pour informer I-CSCF s'il continue la procédure de l'enregistrement. Si oui la requête UAA va contenir aussi des AVPs pour aider l'I-CSCF à déterminer ou choisir un S-CSCF.

#### b) La requête MAR /MAA

Lorsque le S-CSCF reçoit le message d'enregistrement il doit authentifier l'utilisateur. Donc il doit télécharger le vecteur d'authentification du HSS car pour une première fois le S-CSCF ne les a pas. Il envoie un MAR (Multimedia Auth Request) au HSS pour lui demander ces vecteurs et enregistrer au même temps son URI dans le profil de l'utilisateur pour que d'autres CSCFs soient capables de savoir qu'elle

est les-CSCF alloué à cet utilisateur. Le HSS répond par les vecteurs dans le message MAA (Multimedia Auth Answer).

### c) La requête SAR / SAA

Une fois l'utilisateur authentifié, le S-CSCF envoie le message SAR (Server Assignment Request) au HSS pour lui indiquer que l'utilisateur est enregistré chez lui et pour lui demander son profile complet (ou le reste de son profile). Le HSS répond par un message SAA (Server Assignment Answer) contenant le profile demandé. Le S-CSCF peut aussi envoyer le message SAR au HSS si l'utilisateur n'est plus enregistré pour garder le HSS au courant de l'état d'enregistrement de l'utilisateur. Le HSS peut autoriser le S-CSCF de garder le profile de l'utilisateur et de lui rester affecter. Le HSS contrôle cette possibilité.

## III.7.2 Le protocole SIP

SIP (Session Initiation Protocol) est un protocole de signalisation permettant l'établissement, la libération et la modification de sessions multimédias. Il appartient à la couche applicative du modèle OSI (Open System Interconnect). Il hérite de certaines fonctionnalités du protocole HTTP (HyperText Transfer Protocol), utilisé pour naviguer sur le web, et du protocole SMTP (Simple Mail Transfer Protocol), utilisé pour transmettre des messages électroniques (e-mail). En effet, SIP s'appuie sur un modèle transactionnel client/serveur, et l'adressage utilise le concept d'URL (Uniform Resource Locator) SIP qui ressemble à une adresse e-mail. Chaque participant dans un réseau SIP est donc adressable par une URL SIP. Par ailleurs, les requêtes SIP sont acquittées par des réponses identifiées par un code numérique.

De plus, la plupart des codes de réponses SIP ont été empruntés au protocole HTTP (par exemple, « 404 Not Found » quand le destinataire n'est pas localisé). Une requête SIP est constituée d'en-têtes ou headers comme une commande SMTP. Tout comme le protocole SMTP, SIP est un protocole textuel. SIP a été étendu afin de supporter la signalisation pour de nombreux services tels que la présence, la messagerie instantanée, le transfert d'appel, la conférence et les services complémentaires de téléphonie.

SIP a été retenu par le 3GPP pour l'architecture IMS comme protocole pour le contrôle de session et le contrôle de service. Il remplace peu à peu les protocoles ISUP (ISDN User Part) pour le contrôle d'appel dans le RTC (Réseau Téléphonique Commuté), et INAP (Intelligent Network Application Protocol) pour le contrôle de service dans l'architecture Réseau Intelligent. Toutefois, SIP n'est qu'un protocole de signalisation. Une fois la session établie, les participants de la session s'échangent directement leur trafic audio/vidéo à travers d'autres protocoles comme RTP (Real-time Transport Protocol) par exemple.

SIP se charge de l'authentification et de la localisation des multiples participants. Il n'est cependant pas un protocole de réservation de ressource. Il s'agit d'un protocole de contrôle d'appel et non de contrôle du média. Mais il peut effectuer la négociation sur les types de média utilisables par les

différents participants en encapsulant des messages SDP (Session Description Protocol). SIP peut fonctionner au-dessus de plusieurs protocoles de transport, notamment UDP (User Datagram Protocol) et TCP (Transmission Control Protocol).

### III.7.2.1 Les entités SIP

L'architecture de SIP comporte plusieurs catégories d'entités qui s'échangent des messages (voir figure III.3). On distingue les entités utilisatrices (ou agents utilisateurs) constituées du terminal utilisateur, et les entités réseau qui sont des serveurs (serveur proxy, de redirection, de localisation et d'enregistrement). La figure III.3 illustre l'architecture de SIP, montrant de façon générale les communications entre les entités. On a seulement considéré un terminal utilisateur car on veut insister sur les échanges entre le terminal et les services que ce dernier est susceptible d'utiliser lors de ses communications.

On constate qu'il existe deux catégories de services: l'un fourni au niveau du terminal utilisateur, et l'autre fourni au niveau des serveurs du réseau. Les serveurs du réseau sont répartis en deux classes :

- Les serveurs de redirection et proxy, qui facilitent le routage des messages de signalisation et jouent le rôle d'intermédiaires.
- Les serveurs de localisation et d'enregistrement, qui ont pour fonction d'enregistrer ou de déterminer la localisation des abonnés du réseau.

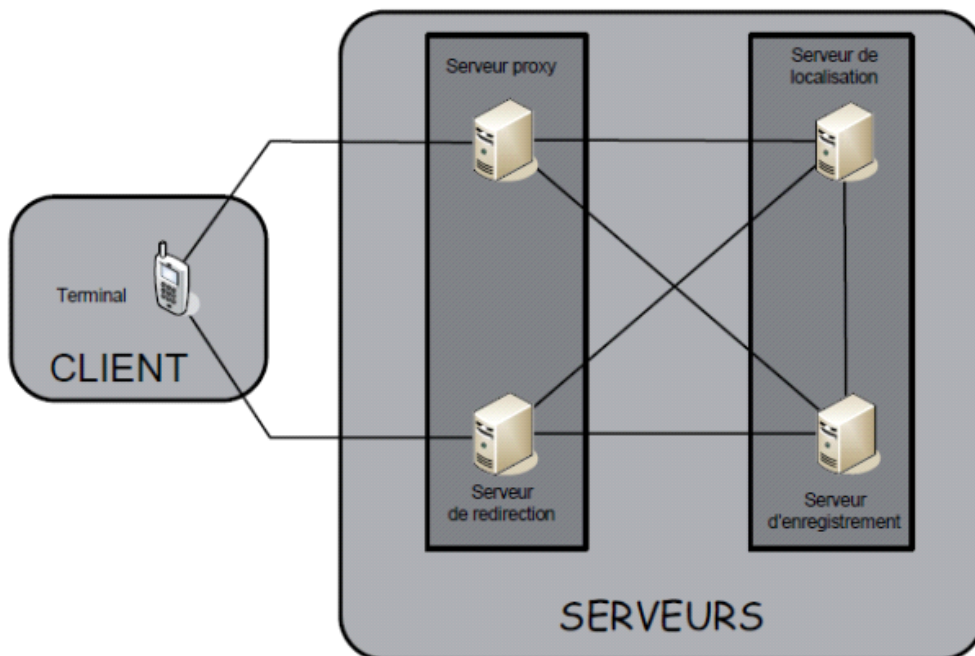


Figure III.3 : Architecture de SIP [20].

### III.7.2.2 Les requêtes SIP

Comme on l'a vu dans la structure générale d'un message SIP, une requête SIP est composée de trois parties : une ligne de requête, les champs d'en-tête du message et le corps. On s'intéressera principalement à la ligne de requête qui est composée de trois champs, comme le montre la figure suivante.

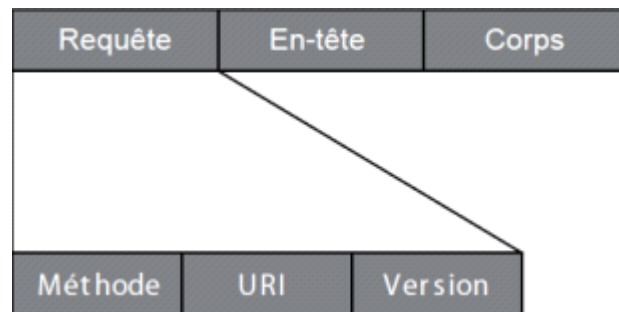


Figure III.4 : Format d'une requête SIP [20].

La figure III.4 montre que la partie ligne de requête se compose des trois champs suivants :

- *Méthode* : qui indique l'action sollicitée.
- *URI* : qui précise le destinataire de la requête.
- *Version* : qui spécifie le numéro de la version du protocole SIP utilisée.

SIP dispose de six méthodes fondamentales pour formuler ses requêtes. Ces méthodes doivent être supportées par tous les terminaux et serveurs sollicités. Néanmoins, des méthodes complémentaires ont été ajoutées pour d'éventuelles améliorations [24] [25] [26].

#### a) Méthode INVITE

La méthode INVITE permet d'initier une communication en invitant un correspondant à y participer. Elle peut aussi être utilisée pour une conférence afin d'inviter plusieurs interlocuteurs à communiquer au sein d'une même session. Le corps du message de cette méthode fournit à l'appelé les paramètres de session souhaités et supportés par l'appelant. Par exemple, l'appelant spécifiera le codec souhaité et le type de flux requis (voix, vidéo, etc.).

Généralement, l'appelant ne se contente pas d'une seule proposition, mais offre de multiples possibilités de paramètres. Ses préférences sont définies par l'ordre dans lequel apparaissent ses propositions. Notons qu'une autre utilisation classique de cette méthode consiste à renégocier dynamiquement de nouveaux paramètres de session. Par exemple, si, durant une session déjà établie, l'un des interlocuteurs souhaite enrichir la voix par la vidéo, il fait sa demande par une requête d'invitation.

**b) Méthode ACK**

La méthode ACK (ACKnowledgement) est utilisée pour confirmer les paramètres de session. Cette méthode correspond à un acquittement de l'appelant. Elle peut être utilisée dans les deux cas suivants :

1er cas : Elle fait suite à l'acceptation d'un appel par l'appelé. Avec la méthode INVITE, l'émetteur a fait connaître au récepteur les paramètres qu'il supporte et ses préférences. En réponse, le récepteur en a fait autant. Au final, l'émetteur compare les paramètres supportés par les deux terminaux et indique par la méthode ACK ceux qui seront utilisés. Si le corps de la méthode ACK est vide, les paramètres proposés par l'appelant pourront être adoptés pour la session.

2ème cas : Elle fait suite à une réponse de localisation fournie par un serveur de redirection. Une fois la détermination de la position de l'appelé effectuée, le serveur de redirection retourne le résultat à l'UAC. Celui-ci valide la réception de ce résultat par la méthode ACK.

**c) La méthode OPTIONS**

Permet d'interroger un serveur SIP, y compris l'entité UAS, sur différentes informations. Elle comporte globalement deux volets : l'état du serveur et ses capacités. Par exemple, cette méthode offre la possibilité de savoir si un utilisateur que l'on souhaite appeler est présent, c'est-à-dire disponible pour initier une communication. Cette réponse est pratique en ce qu'elle donne des informations sur un serveur, sans avoir à initier une communication pour autant. Autrement dit, la requête ne fait pas sonner le poste du récepteur, puisqu'elle n'établit pas d'appel, mais agit comme un indicateur de présence.

Avec cette méthode, il est possible d'obtenir des informations sur un serveur relativement aux types de médias supportés (audio, vidéo, données), aux codecs supportés, aux méthodes supportées et aux options d'appels, si le serveur en a diffusé. Le serveur qui reçoit cette requête répond par son état et ses capacités.

**d) Méthode CANCEL**

La méthode CANCEL permet d'abandonner une demande. Elle annule une requête dont la réponse n'est pas encore parvenue au demandeur. Elle ne permet pas d'interrompre une session, mais indique que la réponse n'est plus attendue et qu'il n'est donc pas nécessaire de traiter la requête. Par exemple, si un utilisateur envoie un message d'invitation INVITE et qu'il attende la réponse de l'appelé, il peut à tout moment émettre un message CANCEL afin d'annuler l'invitation sans avoir à attendre la réponse de l'appelant.

La méthode CANCEL est nécessairement acquittée par un message ACK pour signifier que l'annulation est prise en compte. Cette méthode CANCEL est aussi utilisée par les serveurs. Par exemple, une demande de recherche d'un utilisateur peut solliciter plusieurs serveurs de localisation en parallèle,

qui vont tous rechercher la présence de l'abonné dans leur base de données et retourner le résultat de la recherche. Dès qu'un serveur a trouvé l'abonné, les autres serveurs n'ont plus besoin de poursuivre leur recherche. Un message d'annulation leur est donc envoyé.

#### e) Méthode REGISTER

La méthode REGISTER permet d'enregistrer la localisation, plus particulièrement l'adresse IP auprès d'un serveur d'enregistrement. Elle assure ainsi le service de localisation. L'information enregistrée correspond à une entrée dans la base spécifiant la correspondance d'une adresse SIP avec une adresse IP. Cette entrée a une durée de vie limitée. Passé ce délai, le serveur de localisation la supprime de sa base de données. Par défaut, la durée est d'une heure. Périodiquement, chaque terminal doit rafraîchir cette entrée pour la conserver en base ou, s'il est mobile, la modifier le cas échéant.

Une autre manière de gérer la durée de vie de l'enregistrement est d'utiliser le champ expire de la méthode afin d'imposer une durée de validité fixe, qu'il n'est pas nécessaire de mettre à jour. Le risque dans ce cas est que si l'abonné se déconnecte du réseau sans l'indiquer au serveur d'enregistrement, il reste considéré comme actif dans le réseau (une tentative infructueuse de communication est initiée)

#### f) Méthode BYE

La méthode BYE permet de libérer une communication et de terminer ainsi la session. Cette requête peut être émise indifféremment par l'appelant ou par l'appelé. Cette méthode n'attend pas d'acquiescement, puisqu'une terminaison d'appel peut être décidée de façon unilatérale.

### III.7.2.3 Les réponses SIP

Pour toute requête, le récepteur final doit y répondre, ne serait-ce qu'une réponse temporaire pour informer l'émetteur que sa requête est prise en compte et en train d'être traitée puis sera suivie d'une réponse finale dès que possible. La figure III.5 illustre le format d'une réponse SIP.

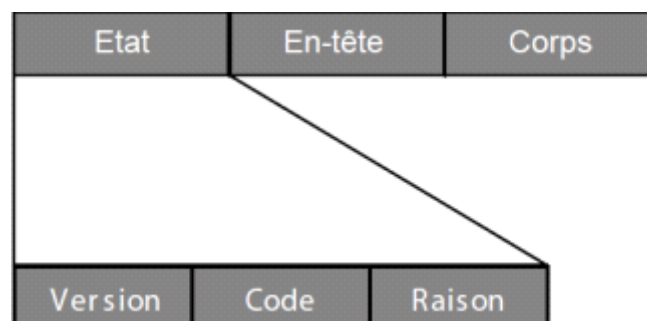


Figure III.5 : Format d'une réponse SIP [20].

D'après la figure, on voit que les réponses aux requêtes SIP débutent par une ligne d'état ou Status Line, laquelle comporte les trois champs suivants :

- *Version* : c'est la version du protocole SIP utilisée.
- *Code d'état (Status Code)* : code numérique à trois chiffres spécifiant la réponse donnée à la requête. Cet entier est codé sur trois bits.
- *Raison (Reason Phrase)* : message textuel expliquant brièvement le code d'état de la réponse.

Il s'agit en effet d'un élément redondant par rapport au code d'état. Cependant, le protocole offre ainsi un niveau de clarté plus accessible, qui favorise la compréhension des messages protocolaires par les utilisateurs comme par les programmeurs. Il existe six classes de réponse dans lesquelles sont répertoriés tous les messages de retour possibles. Le premier chiffre de chaque code spécifie la catégorie à laquelle appartient le code [20] :

**Classe 1xx (Message d'information)** : La requête est en cours de traitement. C'est une réponse temporaire, qui est purement informative. Une réponse définitive (ou finale, correspondant à toute autre catégorie que 1xx) devra être émise au plus tard dans 200 ms.

**Classe 2xx (Message de succès)** : La requête a été reçue, comprise et acceptée par le serveur.

**Classe 3xx (Message de redirection)** : Ce message de réponse décrit une autre action à effectuer avant de finaliser la requête. Cela peut être une nouvelle position de l'utilisateur qui est retournée ou bien une information sur un autre service imposé ou proposé pour satisfaire l'appel.

**Classe 4xx (Message d'erreur requête client)** : La syntaxe est erronée ou la requête ne peut être prise en charge. Dans ce cas, l'appelant ne doit renvoyer la même requête que s'il a fait une modification ou passé un certain délai ou encore sollicité un autre serveur.

**Classe 5xx (Message d'erreur serveur)** : La requête est correcte, mais le serveur n'a pas réussi à la traiter, car le service n'est plus disponible sur le serveur sollicité.

**Classe 6xx (Message d'échec général)** : Aucun serveur ne peut traiter cette requête, car ils sont occupés, inaccessibles ou refusent l'appel. La syntaxe de la requête n'est pas en cause.

#### III.7.2.4 Exemple de scénario

La figure III.6 décrit un scénario d'établissement de session au niveau du trapèze SIP. Ce scénario met en évidence une caractéristique majeure de SIP : lors de sa réponse, l'UAS peut déclencher un échange direct des messages SIP à venir (cas (a)); ou bien les serveurs proxy peuvent obliger les messages SIP qui vont suivre à passer par eux (cas (b)) [20].

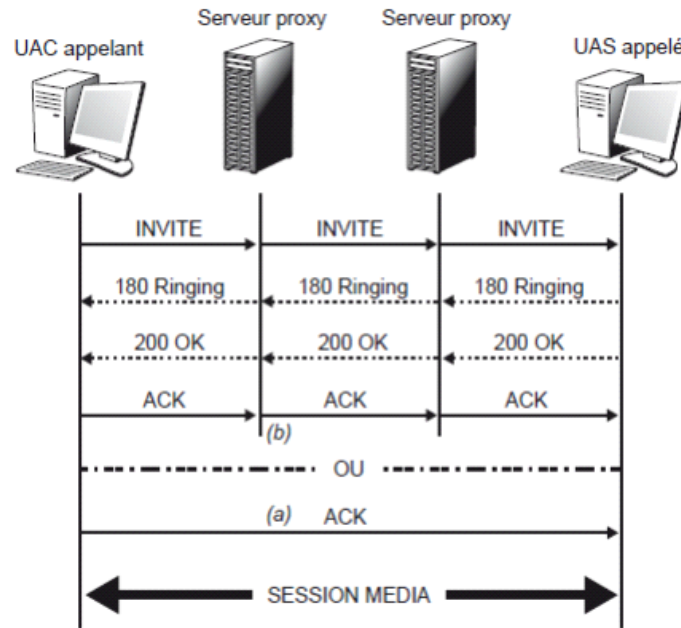


Figure III.6 : Exemple d'établissement de session [20].

### III.7.3 Le protocole SDP (Session Description Protocol)

SDP signifie Session Description Protocol et il est utilisé pour une session multimédia afin que chaque partie de communication se comprenne en termes de diverses capacités multimédia. SDP est généralement porté par un message SIP (par exemple, dans le corps de SIP : message INVITE comme indiqué dans cet exemple). Les paramètres sont comme suite :

*Média* : le type de média (par exemple, audio, vidéo, jeu).

*Port* : contient le numéro de port où ces médias peuvent être reçus.

*Transport* : le protocole de transport à utiliser, soit le protocole de datagramme utilisateur (UDP), soit le profil audio et vidéo du protocole de transport en temps réel (RTP/AVP).

*Format-List* : contient plus d'informations sur les supports, généralement les types de charge utile définis dans RTP/AVP.

Le tableau III.1 donne une description des messages SDP.

Attribue	Paramètres de profile
v	Version du protocole <i>SDP</i> The value must always be equal to zero: v=0
o	Origine de la session La ligne 'origine' se compose de six champs : (<username>, <sess-id>, <sess-version>, <nettype>, <addrtype> et <adresse-unicast>).
s	Le nom de session "s=" contient un seul champ s= <nom de session>. Exemple: "s=-"
t	La ligne time "t=" se compose de deux champs t= <heure de début> et <heure d'arrêt>.



c	Exemple: "t=0 0"
m	La ligne de connexion "c=" se compose de trois champs, c=<type de réseau> <type d'adresse> <adresse de connexion>
a	La ligne media "m=" se compose de quatre champs <media>, <port>, <proto> et <fmt> La ligne d'attribut "a=" est constituée d'un ou deux champs <attribute> ou <attribute><value> contenant plusieurs informations : Codec, Ptime, fmp, Silence suppression.....

**Tableau III.1 :** Description des messages SDP.

SDP signifie Session Description Protocol et il est utilisé pour une session multimédia afin que chaque partie de communication se comprenne en termes de diverses capacités multimédia. SDP est généralement porté par un message SIP (par exemple, dans le corps de SIP : message INVITE comme indiqué dans cet exemple). Les paramètres sont comme suite :

#### III.7.4 Les protocoles RTP et RTCP

Le protocole RTP (Real Time Protocol) est utilisé pour fournir les fonctions de transport pour la transmission en temps réel de données. Il est utilisé conjointement avec le protocole RTCP (Real Time Control Protocol) pour permettre le management des données livrées et permettre un contrôle minimal. En utilisant aussi bien les modes Unicast (point à point) que Multicast (multipoint).

RTP et RTCP se trouvent dans la couche application mais ils utilisent le protocole de transport UDP (car il est plus rapide que TCP).

#### III.7.5 Le protocole de contrôle de passerelle H.248 et MEGACO

Megaco/H.248 sont les protocoles de contrôle de passerelle multimédia définis par l'IETF et l'UIT-T pour une utilisation dans des environnements de commutation distribués. Ils sont des noms équivalents pour le même protocole, développé conjointement entre l'IETF et l'ITU-T.

Dans de tels environnements, la logique de signalisation est située sur les contrôleurs de passerelle multimédia (MGC - également appelés agents d'appel ou Soft Switches) et la logique multimédia est située sur les passerelles multimédia (MG). À l'aide de MGCP ou de Megaco/H.248, les MGC peuvent contrôler les MG pour configurer des chemins de média (par exemple, le trafic vocal) à travers le réseau distribué.

Le protocole Megaco/H.248 a été développé à partir du MGCP Media Gateway Control Protocol. Il fournit des fonctionnalités globalement équivalentes et a une structure très similaire.

DC-MGCP et DC-Megaco/H.248 fournissent des implémentations de code source complètes, évolutives et tolérantes aux pannes des protocoles MGCP et Megaco/H.248.

### III.8 La qualité de service (QoS) dans LTE

Les paquets Internet arrivent en désordre, en retard et parfois avec perte. Ce n'est plus le cas avec l'IMS, vu la QoS assurée de bout en bout. Il est possible que l'équipement de l'utilisateur discute sa capacité et son besoin en qualité de service durant l'établissement d'une session SIP (Session Initiation Protocol).

Selon la recommandation ITU E.800 27, la qualité de service (QoS) est définie comme la totalité des caractéristiques d'un service de télécommunications? Qui portent sur sa capacité à satisfaire les besoins déclarés et implicites de l'utilisateur du service. L'architecture IMS vise à garantir que les politiques de QoS appliquées entre les requêtes spécifiques pour les applications (Session Initiation Protocol - SIP / Session Description Protocol - SDP) et les flux multimédias (Real-time Transport Protocol - RTP), sont définies par les opérateurs de réseau en fonction du type des exigences commerciales et de service au niveau de l'application, qui sont utilisées pour gérer les ressources du réseau et améliorer la qualité de service.

Dans une session VoLTE, trois supports sont utilisés (Tableau III.2) :

- *Porteur avec QCI 9* : Porteur par défaut créé lors de la connexion au réseau.
- *Bearer avec QC15* : Bearer créé pour la signalisation IMS (messages SIP) dès la connexion à l'IMS APN est établi.
- *Support avec QC11* : Ce support est créé une fois que la session vocale a été lancée avec succès, pour assurer transport (messages RTP).

QCI	Resource type	Priority	Packet Delay Budget	Packet Loss Rate	Exemple Services
1	GBR	2	100ms	10 <sup>-2</sup>	Conversational Voice
2		4	150ms	10 <sup>-3</sup>	Conversational Video
3		3	50ms	10 <sup>-3</sup>	(Live Streaming) Real Time Gaming
4		5	300ms	10 <sup>-6</sup>	Non Conversational Video (buffered video).
5		1	100ms	10 <sup>-6</sup>	IMS Signalling
6	NON GBR	6	300ms	10 <sup>-6</sup>	Vidéo (Buffered Streaming)
7		7	100ms	10 <sup>-3</sup>	Interactive Gaming
8		8	300ms	10 <sup>-6</sup>	Vidéo (Buffered Streaming)
9		9	300ms	10 <sup>-6</sup>	Vidéo (Buffered Streaming)

Tableau III.2 : Définitions des supports de QoS EPS [27].

### III.9 Procédure d'IMS et VoLTE

#### III.9.1 Procédure d'enregistrement IMS

Le mobile peut maintenant commencer la procédure d'enregistrement IMS, qui est illustrée dans la figure III.7. Il y a deux étapes. Dans un premier temps, le mobile envoie sa demande d'enregistrement à l'IMS, qui répond par un défi d'authentification.

Dans un deuxième temps, le mobile envoie une deuxième demande d'enregistrement qui contient sa réponse au défi du réseau, et l'IMS accepte l'enregistrement du mobile. La méthode associée à cette fonctionnalité d'enregistrement est REGISTER, à partir du protocole de signalisation SIP.

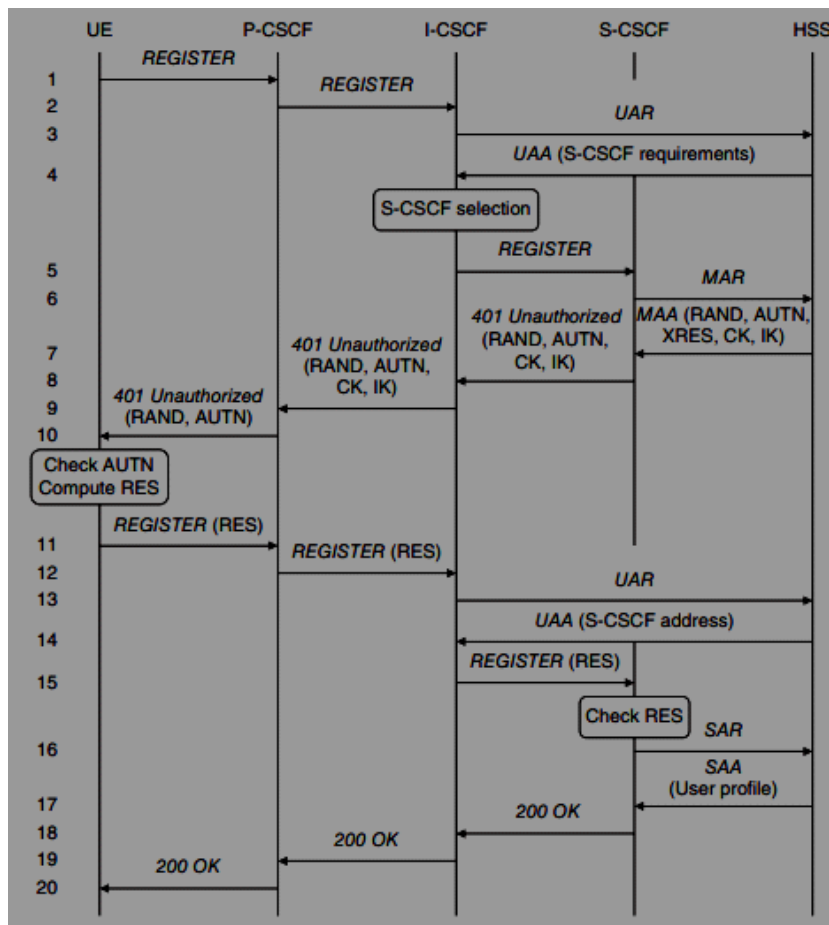


Figure III.7 : Procédure d'enregistrement IMS [28].

La procédure d'enregistrement IMS est exposée comme suite [28] :

- Pour commencer la procédure, le mobile envoie sa requête d'enregistrement (REGISTER) au proxy CSCF .
- en utilisant l'adresse IP qu'il a découverte précédemment. À son tour, le proxy CSCF transmet la demande à un CSCF interrogateur.

- L'I-CSCF doit maintenant trouver un CSCF de service qui enregistrera le mobile. Pour ce faire, il envoie une autorisation d'utilisateur diamètre (UAR) au serveur de l'abonné d'origine et indique les identités publiques et privées de l'utilisateur.
- Dans une réponse d'apparence inhabituelle, le HSS renvoie les capacités que le CSCF en service devrait ont afin de s'occuper de cet utilisateur.
- En inspectant une liste interne d'appareils et leur capacité, le CSCF interrogatrice peut sélectionner un CSCF de service approprié et peut y transmettre la demande d'enregistrement.
- Le CSCF de service doit maintenant authentifier l'utilisateur. Pour ce faire, il envoie une demande d'authentification multimédia de diamètre (MAR) au serveur de l'abonné d'origine.
- Le serveur HSS répond avec un vecteur d'authentification qui contient les quantités RAND, AUTN, XRES, CK et IK.
- La CSCF en service conserve XRES, mais envoie les autres quantités au serveur mandataire et interroge les CSCF dans une réponse d'erreur non autorisée 401.
- Le proxy CSCF conserve CK et IK pour une utilisation dans le cryptage et la protection de l'intégrité, et envoie RAND et AUTN au mobile
- Le mobile vérifie le jeton d'authentification du réseau, calcule sa réponse, RES, et envoie RES au proxy CSCF dans une seconde requête d'enregistrement.
- Le proxy CSCF transmet cette demande à une CSCF interrogatrice comme auparavant.
- Le CSCF interrogée envoie une autre demande d'autorisation d'utilisateur au serveur de l'abonné d'origine.
- Mais le serveur HSS est maintenant au courant de la CSCF en service et peut renvoyer son adresse IP.
- A son tour, le CSCF interrogateur envoie la demande d'INSCRIPTION avec la requête REGISTER à l'adresse suivante.
- Le CSCF en service peut maintenant vérifier la réponse du mobile au défi de l'authentification. Si la réponse est correcte, le CSCF en service informe le serveur de l'abonné d'origine que le mobile est maintenant enregistré à l'aide d'une demande d'assignation de serveur de diamètre (SAR).
- Le serveur HSS répond avec le profil du mobile user.
- Pour terminer la procédure, la CSCF en service envoie une réponse de succès de 200 OK au mobile.

### III.9.2 Configuration et lancement de l'appel VoLTE

La procédure d'un lancement de l'appel VoLTE, donné par la figure III.8, est décrite comme suite [28] :

- (1) (2) Le mobile d'origine envoie sa demande INVITE et son offre SDP à son CSCF proxy, qui envoie la demande au CSCF en service.

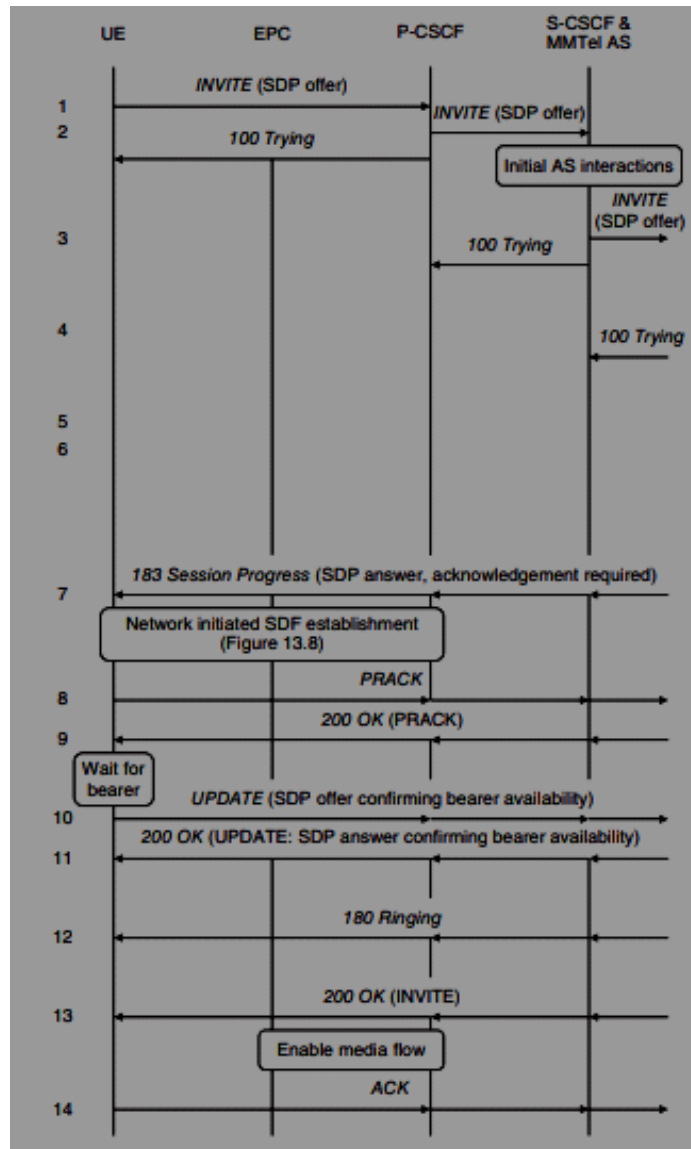


Figure III.8 : Procédure d'un lancement de l'appel VoLTE [28].

- (3) Le CSCF de service cherche la destination mobile et envoie la requête à un CSCF interrogateur dans le réseau de destination par le biais des fonctions de contrôle des frontières d'interconnexion.
- (4) A son tour, le CSCF interrogateur recherche les détails d'enregistrement du mobile de destination dans le serveur de l'abonné d'origine et transmet la demande au CSCF de service du mobile.
- (5, 6) Qui envoie la demande au mandataire CSCF et au mobile. Dans le cas d'une demande INVITE, chaque CSCF envoie également 100 réponses provisoires à son prédécesseur pour confirmer que la demande est arrivée à bon port et qu'elle n'a pas à être retransmise.
- (7) P-CSCF transmet le message "183 progression de la session" au terminal d'origine. En utilisant cette réponse, le terminal d'origine compare les codecs du terminal de terminaison avec les siens et décide du type de codec à utiliser davantage

- (8) Le mobile source envoie l'accusé de réception au moyen d'une requête PRACK .
- (9) La destination mobile répond avec un 200 OK. Les mobiles peuvent faire correspondre cette réponse au PRACK plutôt qu'au INVITE initial en examinant les en-têtes SIP.
- (10) À l'issue de la procédure d'activation au porteur dédiée, le mobile source sait que le réseau d'accès LTE peut lui apporter la qualité de service qu'il requiert. Il informe l'appareil de destination à l'aide d'une deuxième offre SDP. Il intègre l'offre dans une requête SIP UPDATE
- (11) Le mobile de destination répond 200 OK (UPDATE : réponse SDP confirmant la disponibilité du support).
- (12) Une fois toutes ces étapes terminées, le téléphone sonne et le mobile de destination renvoie une réponse provisoire de 180 sonneries à la source.
- (13) Il n'est pas nécessaire de demander un accusé de réception ici, car il n'y a plus d'informations SDP intégrées. Une fois que l'utilisateur répond, le mobile de destination renvoie une réponse de succès de 200 OK à l'INVITE initial.
- (14) Lorsqu'elles reçoivent cette réponse, les CSCF proxy savent que la signalisation SIP et SDP est terminée, elles demandent donc à leurs PCRF respectifs d'activer les flux médias, et les PCRF disent aux passerelles PDN d'ouvrir les portes au trafic des utilisateurs. Pour terminer la procédure, l'appareil source envoie une requête SIP finale appelée ACK.

### III.10 Conclusion

Ce chapitre montre que l'IP Multimedia Subsystem est une nouvelle infrastructure de réseau mobile, une nouvelle façon de fournir des services de communication en temps réel riche (voix, vidéo, données...) aux réseaux LTE.

Dans le même ordre d'idée, l'IMS a pour but d'offrir aux opérateurs une architecture de service multi-média standard. Il est basé sur le protocole IP pour le transport de données et le protocole SIP pour la signalisation et le contrôle de session. De plus, on a vu aussi la procédure pour établir un appel. Alor que, L'établissement, la modification et la libération de session dans l'IMS implique un échange de messages SIP/SDP de bout en bout.

Le quatrième chapitre consiste à simuler un réseau IMS avec ses composantes de base à travers le déploiement d'une plateforme « OpenIMSCore ».

## Chapitre IV :

---

*Mise en place de la solution IMS  
pour la VoLTE*

---

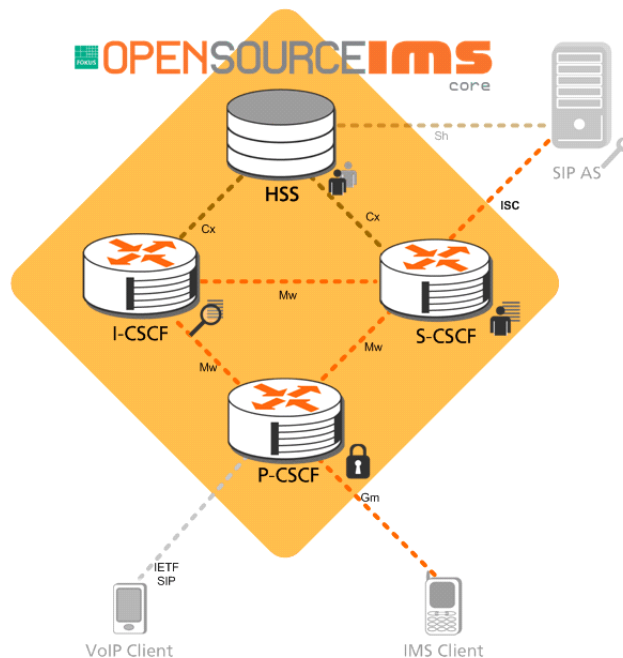
## IV.1 Introduction

Dans ce chapitre, on va appliquer les notions théoriques vues et étudiées dans les chapitres précédents, donc il représente le cadre applicatif dans ce projet. C'est dans cette thématique qu'on va simuler l'architecture de voix sur LTE. Nous avons utilisé l'architecture IMS comme cœur du réseau car elle est compatible avec la norme LTE.

Notre contribution consiste à simuler un réseau IMS avec ses composants de base à travers le déploiement d'une plateforme "OpenIMSCore" basée sur des solutions Opensource. Cette plateforme a servi comme banc d'essai pour la simulation de certaines fonctionnalités nécessaires à l'établissement de toute session multimédia, à savoir la configuration et l'enregistrement des utilisateurs IMS. Elle a aussi servi au lancement de tests d'échange de flux de signalisations SIP et d'établissement de sessions multimédia (service voix et message SMS) entre deux utilisateurs IMS.

## IV.2 Open IMS Core

OpenIMSCore est un projet lancé en 2006, et développé par l'institut de recherche en télécommunications FOKUS (Fraunhofer Institute for Open Communication System), basé à Berlin, en Allemagne.



**Figure IV.1:** Architecture d'OpenIMSCore.

L'Open IMS Core est une implémentation opensource de l'IMS qui garantit les fonctions de contrôle d'un cœur de réseau IMS assurées par les trois serveurs CSCF. Elle fournit également la base de données HSS



ou FHoSS (FOKUS Home Subscriber Server) basée sur MySQL. Les quatre composants sont tous basés sur des logiciels libres Opensource (Figure IV.1).

Le projet Open IMS Core de l'institut Fraunhofer FOKUS a pour but de combler le vide qui existe de nos jours sur l'IMS dans le monde open source. L'idée est de permettre aux utilisateurs de développer des services IMS et de mettre en œuvre les concepts qui entourent l'IMS.

## **IV.2.1 Logiciels utilisés**

### **IV.2.1.1 Logiciel UCT IMS Client**

Le client IMS UCT est une implémentation libre et gratuite d'un client IMS 3GPP, lancé en 2006 où seule la version Linux existe, développé par un groupe de recherche de l'Université du Cap, en Afrique du Sud.

Logiciel UCT IMS Client a pour but d'utilisation des services de communication offerts grâce à l'architecture IMS.

### **IV.2.1.2 Logiciel Boghe IMS Client**

Boghe IMS Client est un logiciel applicatif hébergé sur un serveur et accessible via un navigateur web. Utilisé pour toute communication et plus précisément la messagerie instantanée, en deux versions d'IP (IPv4 et IPv6). Boghe IMS Client est utilisé pour le test d'appel après avoir enregistré l'utilisateur dans IMS Core (utilisateur authentifié), fonctionnant avec adresse IP du réseau, est disponible sur la plateforme Windows et linux. Nous l'avons utilisé sous Windows pour enregistrer nos utilisateurs.

### **IV.2.1.3 IMS droid**

IMSDroid est une application mobile, téléchargeable sur les Smartphone androïde, permettant d'effectuer les appels et les messages entre utilisateurs enregistrés pour l'objectif de tester le fonctionnement des services sur OpenIMS, et fonctionnant avec les identités publiques et privées (IMPU et IMPI).

## **IV.3 Mise en œuvre d'OpenIMSCore**

L'installation de l'OpenIMSCore exige quelques logiciels et ressources matérielles nécessaires au fonctionnement de la plateforme.

### **IV.3.1 Mise en place Machine Virtuelle**

L'installation d'un cœur réseau IMS OpenIMSCore, nécessite au préalable, la préparation d'une machine virtuelle nommée Ubuntu, dans notre cas nous avons adopté la version Ubuntu 14.04.

Sa configuration nécessite les ressources suivantes :

- Processeur Dual Core.
- 2 Go de RAM.
- 15 Go d'espace libre sur le disque dur ou sur le disque SSD.
- Utiliser VMware Player et installer Ubuntu 14.04.

### IV.3.2 Installation d'un cœur réseau IMS

#### ▪ Pré-requis :

```
sudo apt-get install libcurl4-gnutls-dev
sudo apt-get install bison
sudo apt-get install curl
sudo apt-get install debhelpercdbslintian build-essential
fakerootdevscriptsbuilder dh-make debootstrapdpkg flex libxml2-dev
libmysqlclient15-dev ant docbook-to-man

sudo apt-get install ipsec-tools

sudo apt-get install subversion
sudo apt-get install mysql-server-5.5
```

#### ▪ Installation du JDK 7:

```
sudo add-apt-repository ppa:webupd8team/java
sudo apt-get update
sudo apt-get install openjdk-7-jdk
sudo apt-get install openjdk-7-jdk -set-default
```

#### ▪ Récupération du code source d'OpenIMSCore (via SVN)

- Créer le dossier `/opt/OpenIMSCore` :

```
sudo mkdir /opt/OpenIMSCore
cd /opt/OpenIMSCore
```

- Créer un nouveau répertoire `ser_ims` et y placer les serveurs CSCF :

```
sudo mkdir ser_ims
sudo svn checkout https://svn.code.sf.net/p/openimscore/code/ser_ims/trunk/ ser_ims
```

- **Installation d'OPENIMS CORE:**

```
cdser_ims
sudo make install-libs all
cd ..
```

On obtient la sortie ci-dessus si l'exécution est un succès.

- **Compilation du composant FHoSS:**

- Créer le dossier FHoSS et y placer le serveur HSS :

```
sudomkdirFHoSS
sudosvn checkout https://svn.code.sf.net/p/openimscore/code/FHoSS/trunk/ FHoSS
cd FHoSS
sudo ant compile deploy
sudosed -i 's/JAVA_HOME/bin/java/JAVA_HOME/usr/bin/java/g' deploy/startup.sh
cd ..
```

- **Configuration MySQL:**

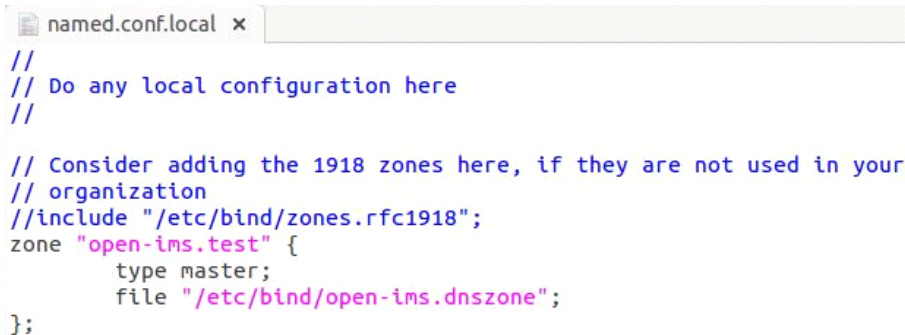
- Placez-vous dans le dossier d'openIMS et effectuer les 3 dumps suivants :

```
mysql -u root -p -h localhost<ser_ims/cfg/icscf.sql
mysql -u root -p -h localhost<FHoSS/scripts/hss_db.sql
mysql -u root -p -h localhost<FHoSS/scripts/userdata.sql
```

Le mot de passe demandé est le mot de passe super utilisateur de MySQL : on a utilisée « root »

- **Configuration DNS:**

- Modifier le fichier **/etc/bind/named.conf** en ajoutant la zone suivante :



```
named.conf.local x
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "open-ims.test" {
    type master;
    file "/etc/bind/open-ims.dnszone";
};
```

Figure IV.2 : La zone DNS

- Editer le fichier **/etc/resolv.conf**, supprimer (ou commenter) le contenu existant et ajouter les lignes suivantes :

```
*resolv.conf x
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
search      open-ims.test
domain      open-ims.test
nameserver  192.168.83.140
```

Figure IV.3 : Configuration DNS.

- On va redémarrer Bind Server par :

```
sudo /etc/init.d/bind9 restart
```

#### ▪ Fichiers de configuration de OpenIMSCore

- Copier les fichiers de configuration .cfg et .xml, ainsi que les scripts de lancement .sh des serveurs x-cscf dans le répertoire de votre choix (nous avons choisi de les placer dans le répertoire d'openIMS pour plus de simplicité et d'organisation) :

```
sudo cp ser_ims/cfg/*.cfg ./
sudo cp ser_ims/cfg/*.xml ./
sudo cp ser_ims/cfg/*.sh ./
```

#### ▪ Lancement d'Open OpenIMS :

- On va lancer les fichiers *pcscf.sh*, *icscf.sh* et *scscf.sh*.

```
sudo ./pcscf.sh
sudo ./scscf.sh
sudo ./icscf.sh
cd FHoSS/deploy
sudo sh startup.sh
```

Tout cela doit fonctionner en parallèle.

#### ➤ P-CSCF

La figure IV.4 montre l'exemple de démarrage de P-CSCF.

```

souhila@souhila-vm: /opt/OpenIMSCore
Aliases:
    tcp: localhost:4060
    udp: localhost:4060
    *: pcscf.open-ims.test:4060

0(1756) init_tcp: using epoll_lt as the io watch method (auto detected)
0(1756) Maxfwd module- initializing
0(1756) INFO:P-CSCF:mod_init: Initialization of module
0(1756) INFO:P-CSCF:mod_init: E-CSCF uri is sip:ecscf.open-ims.test:7060
0(1756) DBG:P-CSCF:mod_init: Can not import load_client_rf. This module might r
require client_rf module.
0(1756) DBG:P-CSCF:mod_init: Usage of the charging info in the pcscf module wil
l be disabled, no charging correlation possible.
0(1756) INFO:P-CSCF:mod_init:E-CSCF uri is sip:ecscf.open-ims.test:7060
0(1756) INFO: udp_init: SO_RCVBUF is initially 163840
0(1756) INFO: udp_init: SO_RCVBUF is finally 327680
0(1756) 1(1757) 2(1758) 3(1759) INFO:P-CSCF:mod_init: Initialization of modu
le in child [2]
5(1761) INFO:P-CSCF:mod_init: Initialization of module in child [3]
INFO:P-CSCF:mod_init: Initialization of module in child [1]
6(1762) INFO:P-CSCF:mod_init: Initialization of module in child [-1]
4(1760) INFO:P-CSCF:mod_init: Initialization of module in child [0]
INFO:P-CSCF:mod_init: Initialization of module in child [-1]
INFO:P-CSCF:mod_init: Initialization of module in child [4]

```

Figure IV.4 : Démarrage de P-CSCF.

## ➤ S-CSCF

La figure IV.5 montre la capture d'écran de démarrage de S-CSCF.

```

souhila@souhila-vm: /opt/OpenIMSCore
14(1795) [16777217,10415]
14(1795) [16777221,10415]
14(1795) -----
14(1795) --- Peer List: ---
14(1795) S[R_Open] hss.open-ims.test:3868 D[ ]
14(1795) [16777216,10415]
14(1795) [16777216,4491]
14(1795) [16777216,13019]
14(1795) [16777216,0]
14(1795) [16777217,10415]
14(1795) [16777221,10415]
14(1795) -----
5(1786) INF:S-CSCF:----- Registrar Contents begin -----
5(1786) INF:S-CSCF:----- Registrar Contents end -----
14(1795) --- Peer List: ---
14(1795) S[R_Open] hss.open-ims.test:3868 D[ ]
14(1795) [16777216,10415]
14(1795) [16777216,4491]
14(1795) [16777216,13019]
14(1795) [16777216,0]
14(1795) [16777217,10415]
14(1795) [16777221,10415]
14(1795) -----

```

Figure IV.5: Démarrage de S-CSCF



### ➤ I-CSCF

La capture d'écran de démarrage d'I-CSCF est montrée par la figure IV.6.

```
souhila@souhila-vm: /opt/OpenIMSCore
14(2001) INFO:peer_connect(): Trying to connect to 127.0.0.1 port 3868
14(2001) INFO:peer_connect(): Peer hss.open-ims.test:3868 connected
14(2001) --- Peer List: ---
14(2001) S[Wait_Conn_Ack] hss.open-ims.test:3868 D[ ]
14(2001) -----
12(1997) --- Peer List: ---
12(1997) S[I_Open] hss.open-ims.test:3868 D[ ]
12(1997) [16777216,10415]
12(1997) [16777216,4491]
12(1997) [16777216,13019]
12(1997) [16777216,0]
12(1997) [16777217,10415]
12(1997) [16777221,10415]
12(1997) -----
14(2001) --- Peer List: ---
14(2001) S[I_Open] hss.open-ims.test:3868 D[ ]
14(2001) [16777216,10415]
14(2001) [16777216,4491]
14(2001) [16777216,13019]
14(2001) [16777216,0]
14(2001) [16777217,10415]
14(2001) [16777221,10415]
14(2001) -----
14(2001) --- Peer List: ---
```

Figure IV.6 : Démarrage d'I-CSCF.

### ➤ Serveur FHoSS:

Finalement, Le lancement de FHoSS est présenté par la figure IV.7.

```
souhila@souhila-vm: /opt/OpenIMSCore/FHoSS/deploy
Building Classpath
Classpath is lib/xml-apis.jar:lib/xercesImpl.jar:lib/xerces-2.4.0.jar:lib/xalan-2.4.0.jar:lib/tomcat-util.jar:lib/tomcat-http.jar:lib/tomcat-coyote.jar:lib/struts.jar:lib/servlets-default.jar:lib/servlet-api.jar:lib/naming-resources.jar:lib/naming-factory.jar:lib/mysql-connector-java-3.1.12-bin.jar:lib/mx4j-3.0.1.jar:lib/log4j.jar:lib/junit.jar:lib/junit.jar:lib/jta.jar:lib/jsp-api.jar:lib/jmx.jar:lib/jdp.jar:lib/jasper-runtime.jar:lib/jasper-compiler.jar:lib/jasper-compiler-jdt.jar:lib/hibernate3.jar:lib/ehcache-1.1.jar:lib/dom4j-1.6.1.jar:lib/commons-validator.jar:lib/commons-modeler.jar:lib/commons-logging.jar:lib/commons-logging-1.0.4.jar:lib/commons-lang.jar:lib/commons-fileupload.jar:lib/commons-el.jar:lib/commons-digester.jar:lib/commons-collections-3.1.jar:lib/commons-beanutils.jar:lib/cglib-2.1.3.jar:lib/catalina.jar:lib/catalina-optional.jar:lib/c3p0-0.9.1.jar:lib/base64.jar:lib/asm.jar:lib/asm-attrs.jar:lib/antlr-2.7.6.jar:lib/FHoSS.jar::log4j.properties:..
[main] INFO de.fhg.fokus.hss.main.TomcatServer - Tomcat-Server is started.
[main] INFO org.apache.catalina.startup.Embedded - Starting tomcat server
[main] INFO org.apache.catalina.core.StandardEngine - Starting Servlet Engine: Apache Tomcat/5.5.9
[main] INFO org.apache.coyote.http11.Http11Protocol - Initializing Coyote HTTP/1.1 on http-127.0.0.1-8080
[main] INFO org.apache.coyote.http11.Http11Protocol - Starting Coyote HTTP/1.1 on http-127.0.0.1-8080
[main] WARN org.apache.catalina.connector.MapperListener - Unknown default host: 127.0.0.1
```

Figure IV.7 : Démarrage de FHoSS.

### ▪ Configuration des abonnés IMS :

L'implémentation d'open source « open IMS Core » permet la configuration par défaut d'un couple d'utilisateurs « Alice et Bob », Ces derniers sont suffisants pour la réalisation des tests.

- Rendez sur l'interface d'administration du FHoSS : <http://hss.open-ims.test:8080>

Les informations de connexion par défaut sont :

-Login : **hssAdmin**

Mot de passe : **hss**

The screenshot shows the web console for FHoSS (The FOKUS Home Subscriber Server, Rel. 7). The browser address bar shows 'localhost:8080/hss.web.console/'. The page has a navigation menu with 'HOME', 'USER IDENTITIES', 'SERVICES', 'NETWORK CONFIGURATION', and 'STATISTICS'. The 'User Identities' section is active, showing a sidebar with options for 'IMS Subscription Search Create', 'Private Identity Search Create', and 'Public User Identity Search Create'. The main content area displays 'Private User Identity - Search Results' with a table of results:

ID	Identity	Auth. Scheme	SQLN
4	alice@open-ims.test	127	000000000000
2	bob@open-ims.test	255	000000000000

Below the table, there is a 'Rows per page' dropdown menu set to 20.

Figure IV.8 : Page d'accueil de FHoSS.

Le couple enregistré sur la base de données Fhosspar défaut :

- [alice@open-ims.test](mailto:alice@open-ims.test)
- [bob@open-ims.test](mailto:bob@open-ims.test)

#### IV.4 Simulation et résultats

Après l'installation de l'implémentation open source « Open IMS Core » (de Fraunhofer FOKUS), nous avons commencé à tester la simulation selon deux cas:

- Deux clients pré-configurés par défaut
- Deux clients à configurer

##### IV.4.1 Cas de deux clients déjà préconfigurés

Nous avons utilisé un client UCT pour faire les tests d'un appel vocal suivi d'un message texte entre Alice et bob. Par défaut, les profils des clients Alice et Bob sont déjà configurés dans UCT IMS Client.

**Etape 1 :** Téléchargement de l'application. Nous avons téléchargé cette application sur notre pc.

**Etape 2 :** Paramétrage

#### IV.4.1.1 Enregistrement des utilisateurs dans le réseau

Nous avons lancé le client UCT IMS, enregistrer et connecter les utilisateurs par défaut d'Alice et de Bob, comme montrent les figures IV.9 et IV.10 respectivement pour les deux utilisateurs Alice et Bob.

**Pour l'utilisateur Alice:**

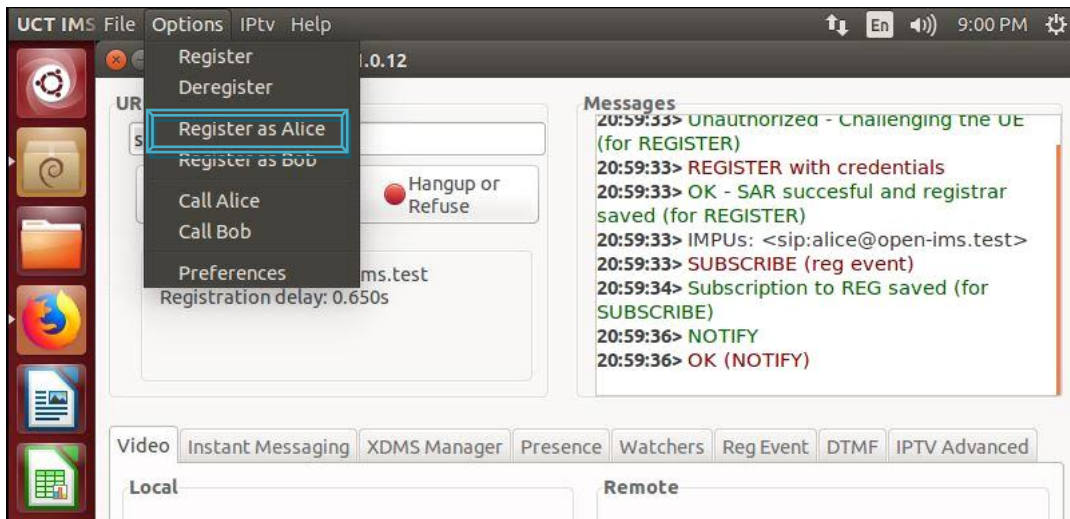


Figure IV.9 : Enregistrement de l'utilisateur Alice dans le réseau.

**Pour l'utilisateur Bob:**

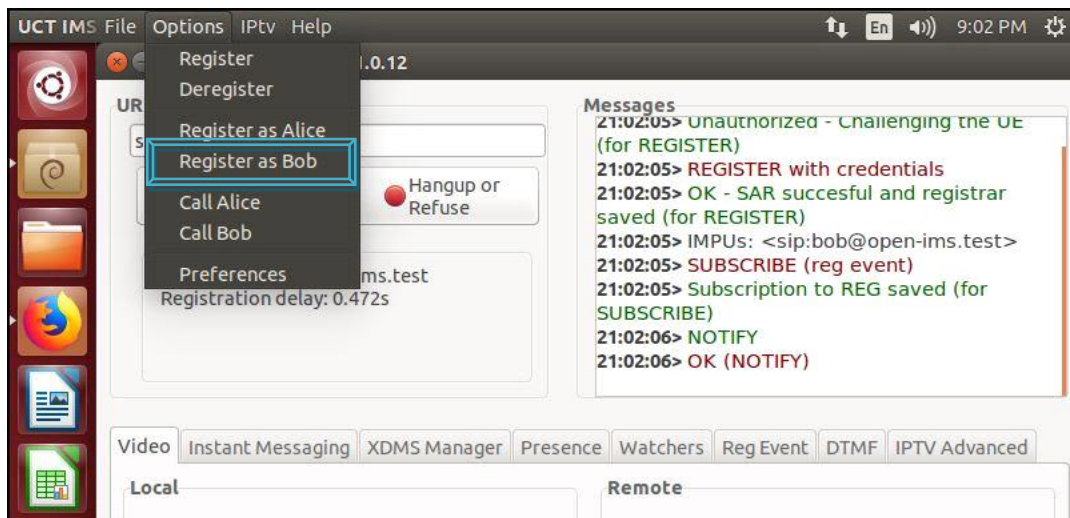


Figure IV.10 : Enregistrement de l'utilisateur Bob dans le réseau.

Les figures ci-dessus montrent la procédure d'enregistrement qui est basé principalement sur l'échange des messages de signalisation SIP entre P-CSCF et UE.



Grâce à notre analyseur réseau UCT IMS client on peut observer la procédure d'enregistrement IMS. On constate bien que l'équipement utilisateur (UE) envoie une première demande d'enregistrement au proxy CSCF via la requête « REGISTER ». Le P-CSCF doit d'abord utiliser d'autres entités S-CSCF et I-CSCF pour authentifier l'identité de l'utilisateur final sur la base de son profil stocké dans la base de données FHoSS. Ensuite, pour confirmer que la demande d'enregistrement a réussi et que le client peut établir une session voix, vidéo ou data, un second message "REGISTER" est envoyé avec les nouveaux paramètres qui sera acquitté par une réponse "200 OK".

Une fois nous avons enregistré les utilisateurs Alice et bob dans logiciel UCT IMS Client, nous remarquons qu'en accédant à l'interface du HSS que ces utilisateurs sont enregistrés dans notre plateforme IMS, comme montre la figure IV.11.

### Public User Identity - Search Results

ID	Identity	Implicit-Set ID	Type	Reg. Status	Barring
1	sip:alice@open-ims.test	1	Public_User_Identity	Registered	false
2	sip:bob@open-ims.test	2	Public_User_Identity	Registered	false

Figure IV.11 : Registre de plateforme IMS.

#### IV.4.1.2 Test d'appel vocal

Maintenant, après que l'utilisateur a été enregistré dans le réseau d'IMS déployé dans le nuage, on a fait le test d'appel entre les deux utilisateurs entre Alice et bob (Alice appelle bob) et illustré par les captures de la figure IV.12. Cette méthode SIP sert à la fois pour initier une session voix ou une session vidéo pour un client déjà enregistré. La requête "INVITE" est envoyée par le premier client «Bob» pour lancer un appel téléphonique avec le deuxième client «Alice».

Les paramètres de session sont négociés à l'aide du protocole SDP, et son message sera encapsulé dans une requête SIP "INVITE". Par la suite, les deux participants (Alice et Bob) négocient les paramètres de la session (qualité, encodage média et capacité du terminal à utiliser) et réservent des ressources via des messages "SIP/SDP".

Une fois tous les paramètres de la session sont négociés et mis en place, les deux UE échangent un message «200 OK», puis ils échangent un message «ACK» qui indique que la création de la session vocale a réussi. À cet instant la session est déjà établie entre les deux clients, le trafic audio est acheminé entre eux en utilisant RTP comme protocole de transport.

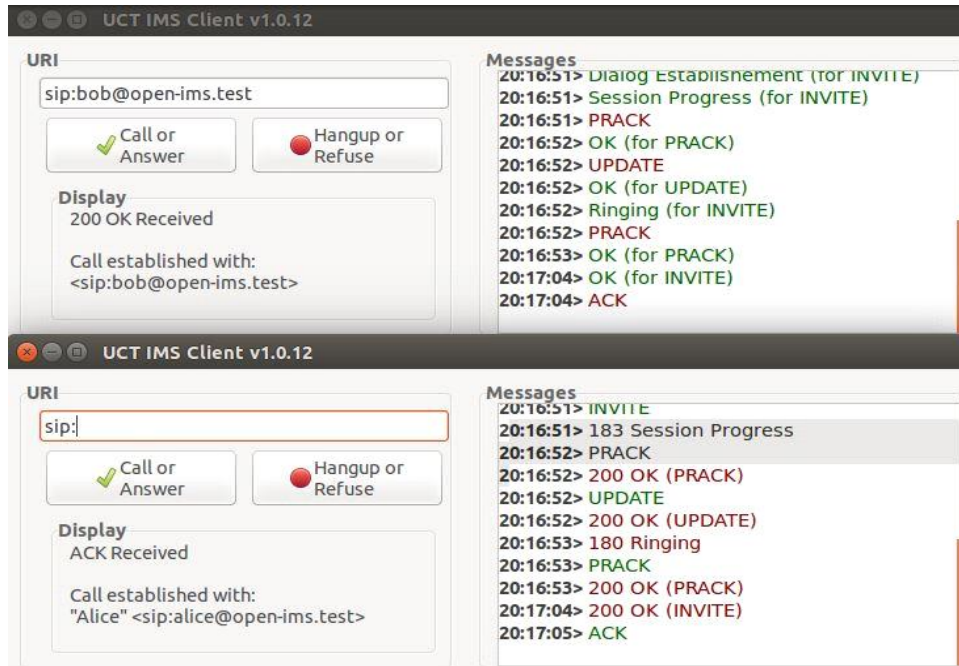


Figure IV.12 : Alice appelle Bob.

## Fin d'appel

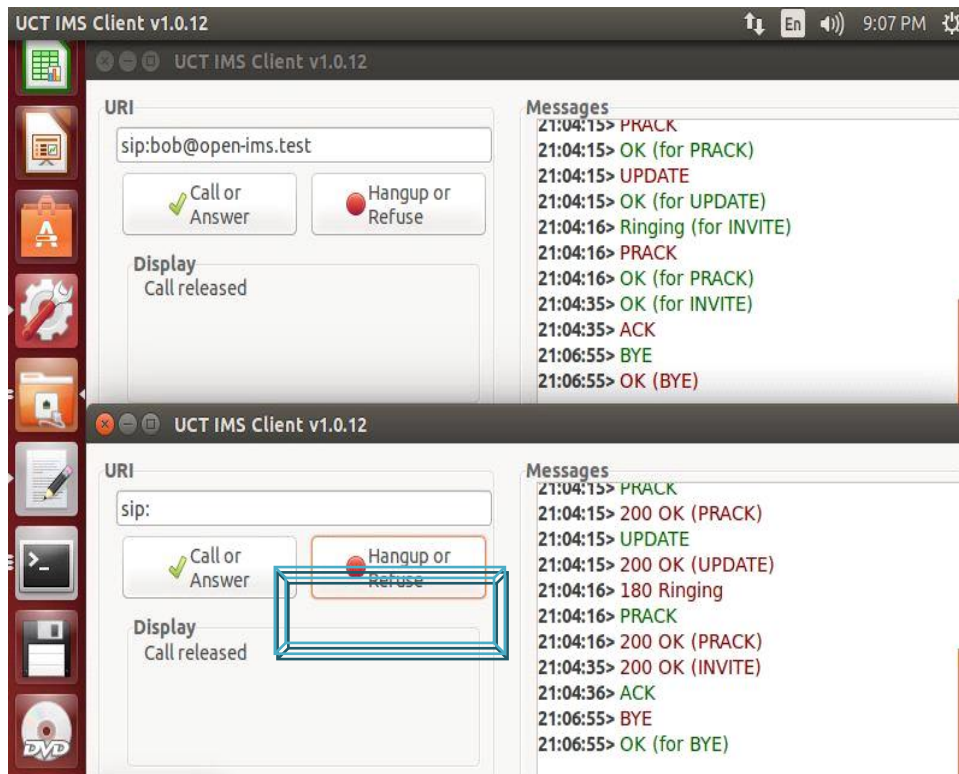


Figure IV.13 : Fin d'appel entre Alice et Bob.

Quand on raccroche ou bien terminer l'appel, on remarque que, à la fin de la session les deux clients échangent un message "BYE" confirmé avec une réponse "200 OK" (Figure IV.13).

### IV.4.1.3 Test de session data (message)

L'établissement d'une session de données entre deux utilisateurs s'effectue en deux requêtes qui s'échangent entre eux. La première requête est envoyée par Alice à Bob contenant son message instantané, elle est dite requête MESSAGE, Bob va recevoir cette requête émise et sera responsable de lui indiquer l'accusé de réception de ce message, pour cela Bob va renvoyer à Alice une requête dite requête 200 OK. L'établissement d'une session de données (messages) entre Alice et Bob est représenté par la figure suivante.

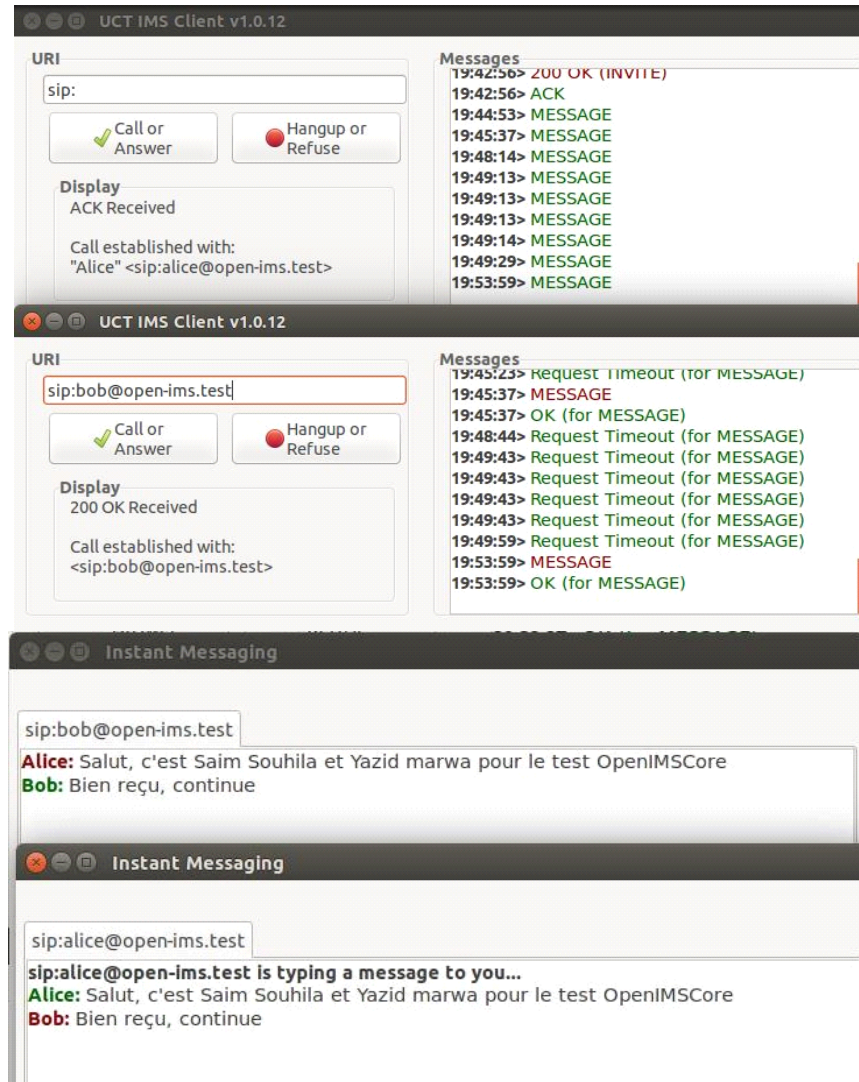


Figure IV.14 : Établissement d'une session de données entre Alice et Bob.

### IV.4.2 Cas de deux clients à configurer

Il faut accéder à l'interface web du FHOSS et insérer le serveur d'application comme suit : la première étape a consisté à créer et configurer deux nouveaux abonnés sur OpenIMSCore «**Souhila**» et «**Marwa**».

**Note:** Dans notre cas, le logiciel UCT IMS Client n'est pas utilisable car il ne permet pas la création de nouveaux utilisateurs et comprend par défaut deux utilisateurs standards Alice et Bob. Quant à la deuxième étape, elle s'occupe de l'enregistrement des nouveaux utilisateurs sur le réseau. La troisième étape consiste à simuler un appel vocal dans sa section de contrôle puis à établir une session.

#### IV.4.2.1 Configuration des deux abonnés IMS

Après configuration, on peut maintenant l'intégrer dans OpenIMSCore. Pour cela, il faut accéder à l'interface web du FHoSS et suivre les quatre étapes suivantes :

- **Etape 1 : Création d'une IMPU [Public User Identity] :**

L'identité publique (IMPU) de l'utilisateur est l'équivalent d'un numéro de téléphone. Ainsi, il permet de contacter l'utilisateur et c'est cette adresse qui est à communiquer.

Tout d'abord, Nous allons commencer par créer une identité publique (IMPU) pour les deux nouveaux utilisateurs « souhilasaim » et « marwayazid ».

- [sip:souhilasaim@open-ims.test](mailto:sip:souhilasaim@open-ims.test)
- [sip:marwayazid@open-ims.test](mailto:sip:marwayazid@open-ims.test)

**Note :** L'identité de l'utilisateur doit absolument respecter cette syntaxe: **sip:utilisateur@domaine**. Soit dans notre cas, pour le domaine **open-ims.test** et pour les utilisateurs « souhilasaim » et « marwayazid ».

Pour l'utilisateur «souhilasaim»

### Public User Identity -IMPU-

ID	3
Identity*	sip:souhilasaim@open-ims.test
Barring	<input type="checkbox"/>
Service Profile*	default_sp
Implicit Set	3
Charging-Info Set	default_charging_set
Can Register	<input checked="" type="checkbox"/>
IMPU Type*	Public_User_Identity
Wildcard PSI	
PSI Activation	<input type="checkbox"/>
Display Name	
User-Status	REGISTERED

Mandatory fields were marked with "\*\*"

Save Refresh Delete

**Add IMPU(s) to Implicit-Set**

IMPU Identity  Add

**List IMPUs from Implicit-Set**

ID	IMPU Identity	Delete
3	sip:souhilasaim@open-ims.test	<input type="checkbox"/>

**Add Visited-Networks**

Select Visited-Network...  Add

**List of Visited Networks**

ID	Identity	Delete
1	open-ims.test	<input type="checkbox"/>

**Associate IMPI(s) to IMPU**

IMPI Identity  Add

Warning: This IMPI will be associated with all the corresponding IMPUs (within the same implicit-set)!

**List of associated IMPIs**

ID	IMPI Identity	Delete
5	souhilasaim@open-ims.test	<input type="checkbox"/>

**Push Cx Operation**

Apply for  User-Data

Execute  PPR

Figure IV.15 : Configuration de l'IMPU souhilasaim



Pour l'utilisateur «marwayazid»

## Public User Identity -IMPU-

The screenshot displays the configuration page for a Public User Identity (IMPU). The main form includes the following fields and values:

- ID: 4
- Identity\*: sip:marwayazid@open-ims.test
- Barring:
- Service Profile\*: default\_sp
- Implicit Set: 4
- Charging-Info Set: default\_charging\_set
- Can Register:
- IMPU Type\*: Public\_User\_Identity
- Wildcard PSI:
- Display Name:
- User-Status: REGISTERED

Below the form, there are buttons for 'Save', 'Refresh', and 'Delete'. A note states: 'Mandatory fields were marked with "\*\*'.

On the right side, there are several sections:

- Add Visited-Networks:** A dropdown menu for 'Select Visited-Network...' and an 'Add' button.
- List of Visited Networks:** A table with columns 'ID', 'Identity', and 'Delete'. It contains one entry: ID 1, Identity open-ims.test.
- Associate IMPI(s) to IMPU:** An input field for 'IMPI Identity' and an 'Add' button.
- Warning:** A red box containing the text: 'Warning: This IMPI will be associated with all the corresponding IMPUs (within the same implicit-set)!'
- List of associated IMPIs:** A table with columns 'ID', 'IMPI Identity', and 'Delete'. It contains one entry: ID 6, IMPI Identity marwayazid@open-ims.test.
- Push Cx Operation:** A section with 'Apply for' set to 'User-Data' and an 'Execute' button labeled 'PPR'.

At the bottom left, there are two more sections:

- Add IMPU(s) to Implicit-Set:** An input field for 'IMPU Identity' and an 'Add' button.
- List IMPUs from Implicit-Set:** A table with columns 'ID', 'IMPU Identity', and 'Delete'. It contains one entry: ID 4, IMPU Identity sip:marwayazid@open-ims.test.

Figure IV.16 : Configuration de l'IMPU marwayazid.

### ▪ Etape 2 : Création d'une IMPI [Private User Identity]:

Il s'agit dans cette étape, d'attribuer aux utilisateurs « souhilasaim » et « marwayazid » une identité privée.

Comme précédemment, une syntaxe est à respecté pour l'IMPI: **utilisateur@domaine**. Donc, les identités privées des deux utilisateurs sont dans notre cas:

- [souhilasaim@open-ims.test](mailto:souhilasaim@open-ims.test)
- [marwayazid@open-ims.test](mailto:marwayazid@open-ims.test)

Pour assurer la sécurité de l'IMPI, Nous avons choisi une clé secrète (équivalent d'un mot de passe) pour notre utilisateur.

Pour l'utilisateur «souhilasaim»

La figure suivante représente une capture de configuration de l'IMPI pour l'utilisateur souhilasaim.

**Private User Identity -IMPI-**

The screenshot shows the configuration page for a Private User Identity (IMPI) for the user 'souhilasaim'. The main configuration area includes fields for ID (5), Identity\* (souhilasaim@open-ims.test), and Secret Key\* (souhila). Under Authentication Schemes\*, 'All' is selected, and 'Digest-AKAv1-MD5' is set as the default. Other fields include AMF\* (0000), OP\* (a long hex string), and SQN\* (000000001ac). Below the main form are fields for Early IMS IP, DSL Line Identifier, and a GUSS 'Configure' button.

Below the main form, a note states: "Mandatory fields were marked with '\*'. Key in this form is considered in hex representation if its value is 16 bytes long or else in ASCII representation." At the bottom of this section are 'Save', 'Refresh', and 'Delete' buttons.

On the right side, there are several sub-sections:

- Associate an IMSU:** A form with an 'IMSU Identity' field and an 'Add/Change' button.
- Associated IMSU:** A table with columns 'ID', 'IMSU Identity', and 'Delete'. It contains one entry with ID '3' and IMSU Identity 'souhilasaim'.
- Create & Bind new IMPU:** A section with a green plus icon.
- Associate IMPU(s):** A form with an 'IMPU Identity' field and an 'Add' button. A warning message below reads: "Warning: The current IMPI will be associated with all the corresponding IMPUs (within the same implicit-set)".
- List of associated IMPUs:** A table with columns 'ID', 'IMPU Identity', and 'Delete:'. It contains one entry with ID '3' and IMPU Identity 'sip:souhilasaim@open-ims.test'.
- Push Cx Operation:** A form with 'Apply for' set to 'User-Data' and an 'Execute' button labeled 'PPR'.
- RTR Operation:** A form with 'Apply for' set to 'IMPU(s) of crt IMPI' and a list of identities containing 'sip:souhilasaim@open-ims.test'. It also has a 'Reason' dropdown, a 'Reason Info' field, and 'Execute' buttons for 'RTR-All' and 'RTR-Selected'.

Figure IV.17 : Configuration de l'IMPI pour souhilasaim.

**Note :** Une fois sauvegardé, nous allons dans la zone "Associate IMPU(s)", c'est là que l'on peut faire une association entre IMPU et IMPI.

**Pour l'utilisateur «marwayazid»**

De la même façon on fait la configuration de l'IMPI pour le deuxième utilisateur marwayazid, comme montre les captures de la figure IV.18.

### Private User Identity -IMPI-

ID	5
Identity*	marwayazid@open-ims.test
Secret Key*	yazid
<b>Authentication Schemes*</b>	
Digest-AKAv1 (3GPP)	<input type="checkbox"/>
Digest-AKAv2 (3GPP)	<input type="checkbox"/>
Digest-MD5 (FOKUS)	<input type="checkbox"/>
Digest (CableLabs)	<input type="checkbox"/>
SIP Digest (3GPP)	<input type="checkbox"/>
HTTP Digest (ETSI)	<input type="checkbox"/>
Early-IMS (3GPP)	<input type="checkbox"/>
NASS Bundled (ETSI)	<input type="checkbox"/>
All	<input checked="" type="checkbox"/>
Default	Digest-AKAv1-MD5
AMF*	0000
OP*	00000000000000000000000000000000
SQN*	0000000000a4
Early IMS IP	
DSL Line Identifier	
GUSS	Configure

**Associate an IMSU**

IMSU Identity  Add/Change

**Associated IMSU**

ID	IMSU Identity	Delete
4	marwayazid	<input type="checkbox"/>

**Create & Bind new IMPU** +

**Associate IMPU(s)**

IMPU Identity  Add

Warning: The current IMPI will be associated with all the corresponding IMPUs (within the same implicit-set)!

**List of associated IMPUs**

ID:	IMPU Identity:	Delete:
4	sip:marwayazid@open-ims.test	<input type="checkbox"/>

**Push Cx Operation**

Apply for: User-Data ▼

Execute: PPR

**RTR Operation**

Apply for: IMPU(s) of crt IMPI ▼

sip:marwayazid@open-ims.test

Select Identities

Reason: Select Reason... ▼

Reason Info

Execute: RTR-All RTR-Selected

Mandatory fields were marked with "\*".

Key in this form is considered in hex representation if its value is 16 bytes long or else in ASCII representation.

Save Refresh Delete

Figure IV.18 : Configuration de l'IMPI pour marwayazid.

▪ **Etape 3 : Création d'un IMSU [IMS Subscription]:**

Cette étape est la dernière étape de la configuration des utilisateurs (Figure IV.19 et IV.20). Il est nécessaire à présent de créer une souscription utilisateur, ou IMSU (pour IMS Subscription).

### IMS Subscription -IMSU-

ID	3
Name*	souhilasaim
Capabilities Set	cap_set1 <span>▼</span>
Preferred S-CSCF	scscf1 <span>▼</span>
S-CSCF Name	
Diameter Name	

Mandatory fields were marked with "\*".

Save Refresh Delete

**Create & Bind new IMPI** +

**Associate IMPI(s)**

IMPI Identity  Add

**List of associated IMPIs**

ID	IMPI Identity	Delete
5	souhilasaim@open-ims.test	<input type="checkbox"/>

Figure IV.19 : Configuration d'IMS Suscription pour souhilasaim.

## IMS Subscription -IMSU-

ID	4
Name*	marwayazid
Capabilities Set	cap_set1
Preferred S-CSCF	scscf1
S-CSCF Name	
Diameter Name	

Mandatory fields were marked with "\*"

Create & Bind new IMPI

Associate IMPI(s)

IMPI Identity	<input type="text"/>	<input type="button" value="Add"/>
---------------	----------------------	------------------------------------

List of associated IMPIs

ID	IMPI Identity	Delete
6	marwayazid@open-ims.test	<input type="button" value="Delete"/>

Figure IV.20 : Configuration d'IMS Suscription pour **marwayazid**

Enfin, nous allons associer l'IMSU à l'IMPI créée à l'étape 2.

### IV.4.2.2 Configuration et utilisation d'un client IMS

#### a) Configuration d'un client IMS sur Windows

Nous allons configurer pour l'utilisateur « souhilasaim », vous pouvez répéter la même procédure pour l'utilisateur « marwayazid »

##### ▪ Etape 1 : Téléchargement de l'application

Boghe IMS est disponible en téléchargement sur le site Web. Nous l'avons téléchargé sur pc.



Figure IV.21: Boghe IMS Client

##### ▪ Etape 2 : Paramétrage

Une fois l'application est lancée. Nous allons paramétrer les renseignements de l'utilisateur pour qu'il soit authentifié, après on clique sur « SignIn ». La figure IV.22 montre un exemple d'inscription Boghe IMS Client pour l'utilisateur souhilasaim.

Dans le menu Tools >option >network, puis vous remplissez les champs pour configurer le réseau

P-CSCF et le port , une fois vous terminez vous mettez « Save », voir le capture de la figure IV.23.



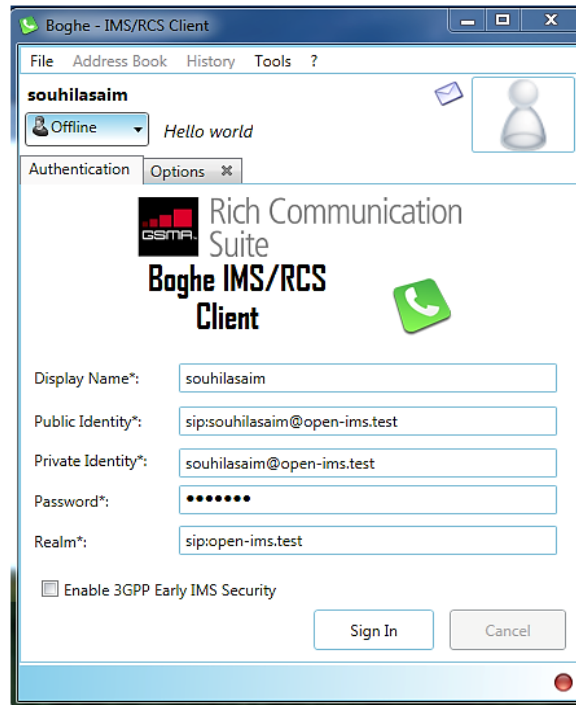


Figure IV.22 : L'inscription Boghe IMS Cleint.

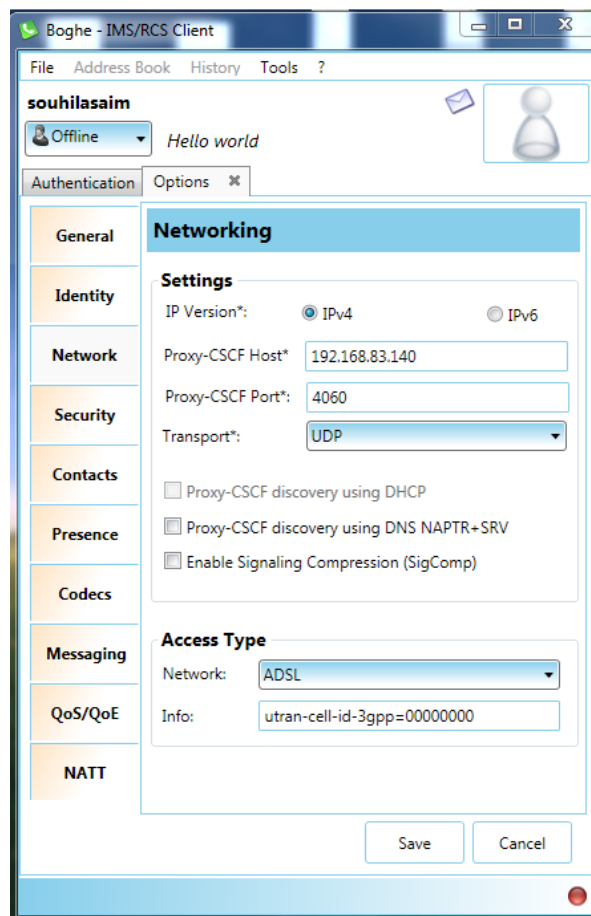


Figure IV.23 : configuration de Networking IP P-CSCF et le port.

Si vous obtenez une fenêtre équivalente à la capture de la figure IV.24, cela montre que l'utilisateur que vous avez configuré est enregistré sur l'IMS Core (le point vert signifie une connexion), si vous avez un point rouge c'est le contraire (l'utilisateur n'est pas encore connecté).

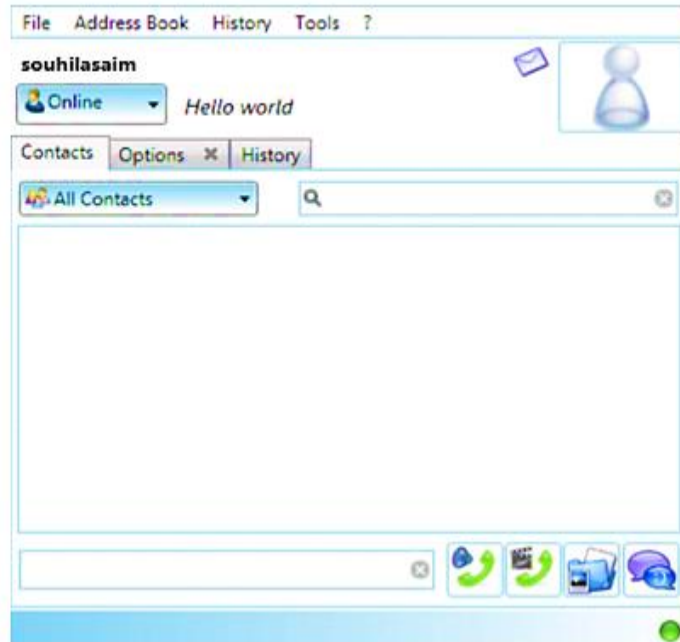


Figure IV.24 : Boghe-IMS client.

- **Etape 3 : L'ajout des contacts**

Pour pouvoir appeler, il faut créer des contacts. Dans les onglets **Address Book > Add Contact** ajouter votre contact, dans cet exemple je vais créer un contact **marwayazid** qui est notre second utilisateurs IMS.

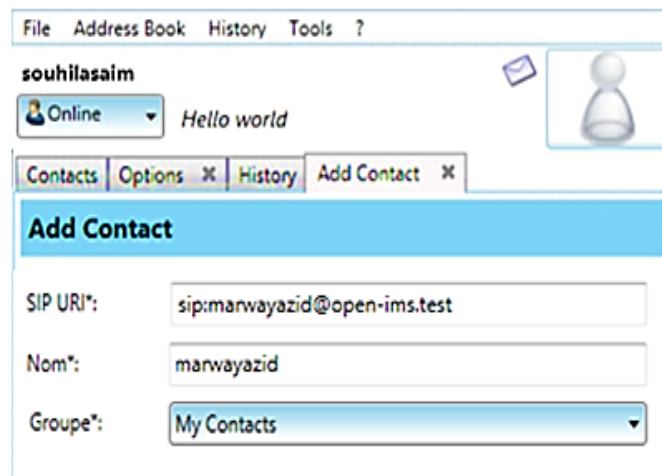


Figure IV.25 : Ajouter un contact Boghe IMS client.

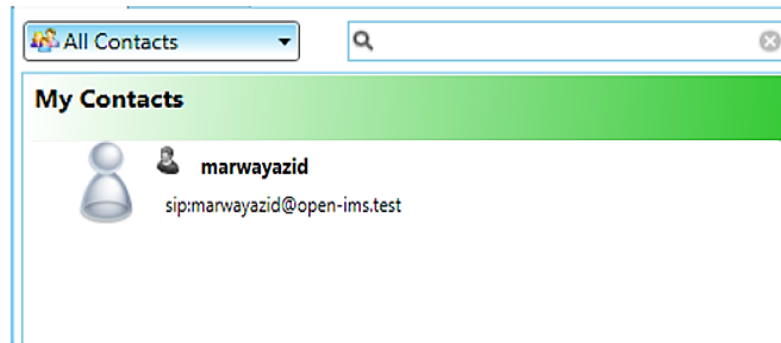


Figure IV.26 : Contact de marwayazid.

### b) Configuration d'un client IMS sur Smartphone Android

IMS Droid est une application téléchargeable sur les Smartphone Android, permet de faire des tests.

#### ▪ Etape 1 : Téléchargement de l'application.

Sur un Smartphone Android, nous avons téléchargé l'application

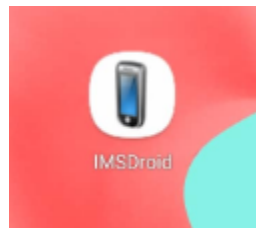


Figure IV.27 : Logo IMS Droid.

#### ▪ Etape 2 : Paramétrage

Après le lancement de l'application téléchargée, nous avons pu créer deux utilisateurs « souhilasaim » et « marwayazid », comme la figure IV.28 montre.

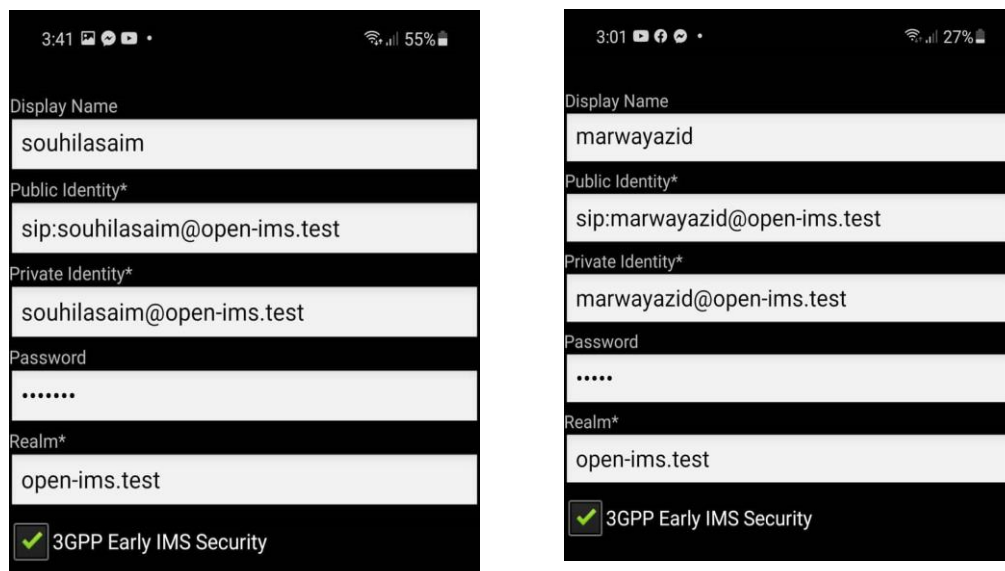


Figure IV.28: L'inscription sur IMS Droid.

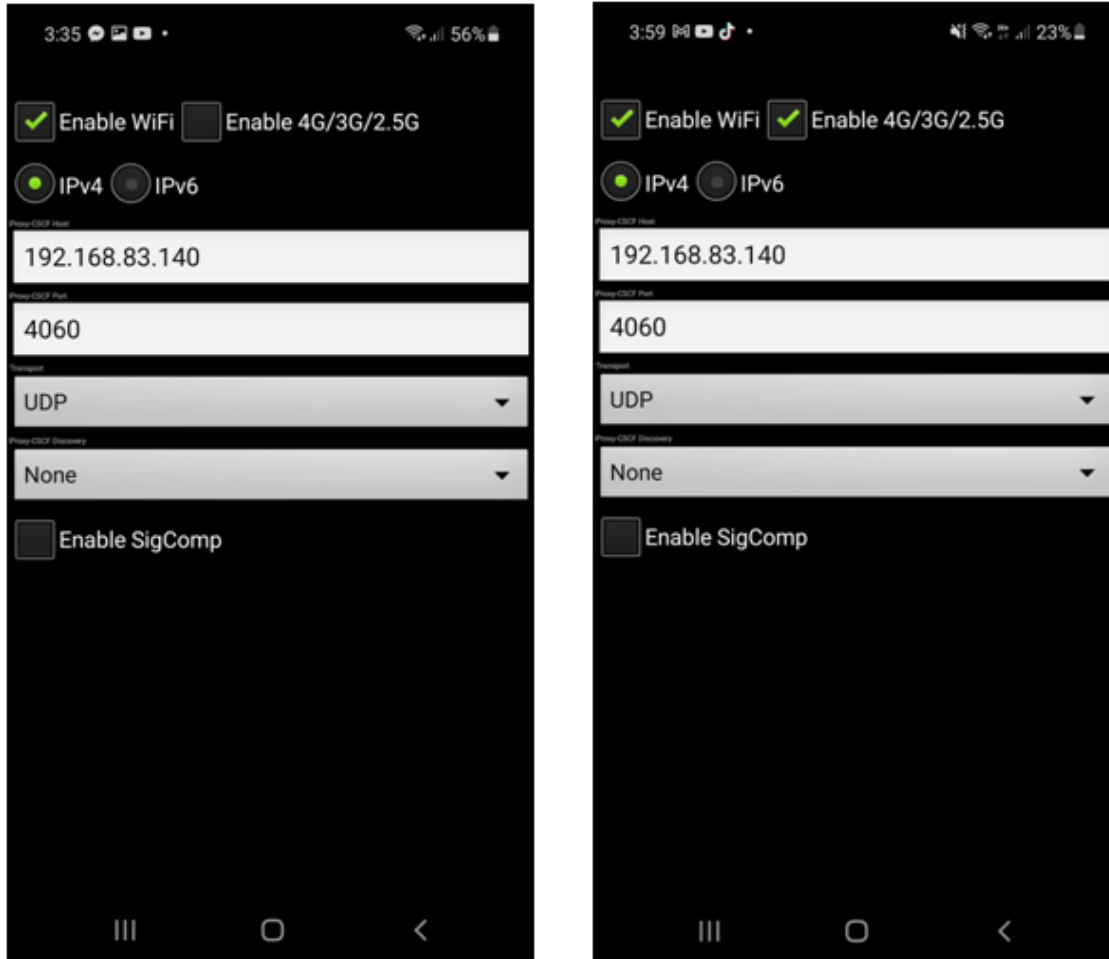


Figure IV.29 : Configuration networking IMS Deroid.

Une fois que nous avons configuré les utilisateurs « souhilasaim » et « marwayazid » dans l'application Boghe IMS, sous Windows et dans le Smartphone via l'application IMSdroid (figure IV.29), nous avons remarqué lors de l'accès à l'interface du HSS que ces utilisateurs sont enregistrés dans notre plateforme IMS.

### Public User Identity - Search Results

ID	Identity	Implicit-Set ID	Type	Reg. Status	Barring
1	sip:alice@open-ims.test	1	Public_User_Identity	Registered	false
2	sip:bob@open-ims.test	2	Public_User_Identity	Registered	false
3	sip:souhilasaim@open-ims.test	3	Public_User_Identity	Registered	false
4	sip:marwayazid@open-ims.test	4	Public_User_Identity	Registered	false

Rows per page  
 1 20 ▾

Figure IV.30 : L'enregistrement des utilisateurs.

- **Etape 3 : Ajout de contact**

Nous avons ajouté « marwayazid » à l'utilisateur « souhilasaim » et c'est pareil pour « souhilasaim ».

### Test d'appel

Après la configuration des utilisateurs sur les applications, « souhilasaim » sur l'application Boghe sous Windows et « souhilasaim », « marwayazid » sur l'application IMSdroid sur le Smartphone. Dans cette partie, nous avons fait un test d'appel entre les deux utilisateurs « souhilasaim » et « marwayazid », le test a été effectué avec succès.

Les deux figures qui suivent, montrent l'appel sortant de « marwayazid », vers « souhilasaim » et prouve que l'appel a bien marché.



Figure IV.31: Test d'appel entre deux utilisateurs.

### Appel vidéo :

Les deux captures de la figure IV.32 représentent l'appel vidéo fait entre les deux usagers.

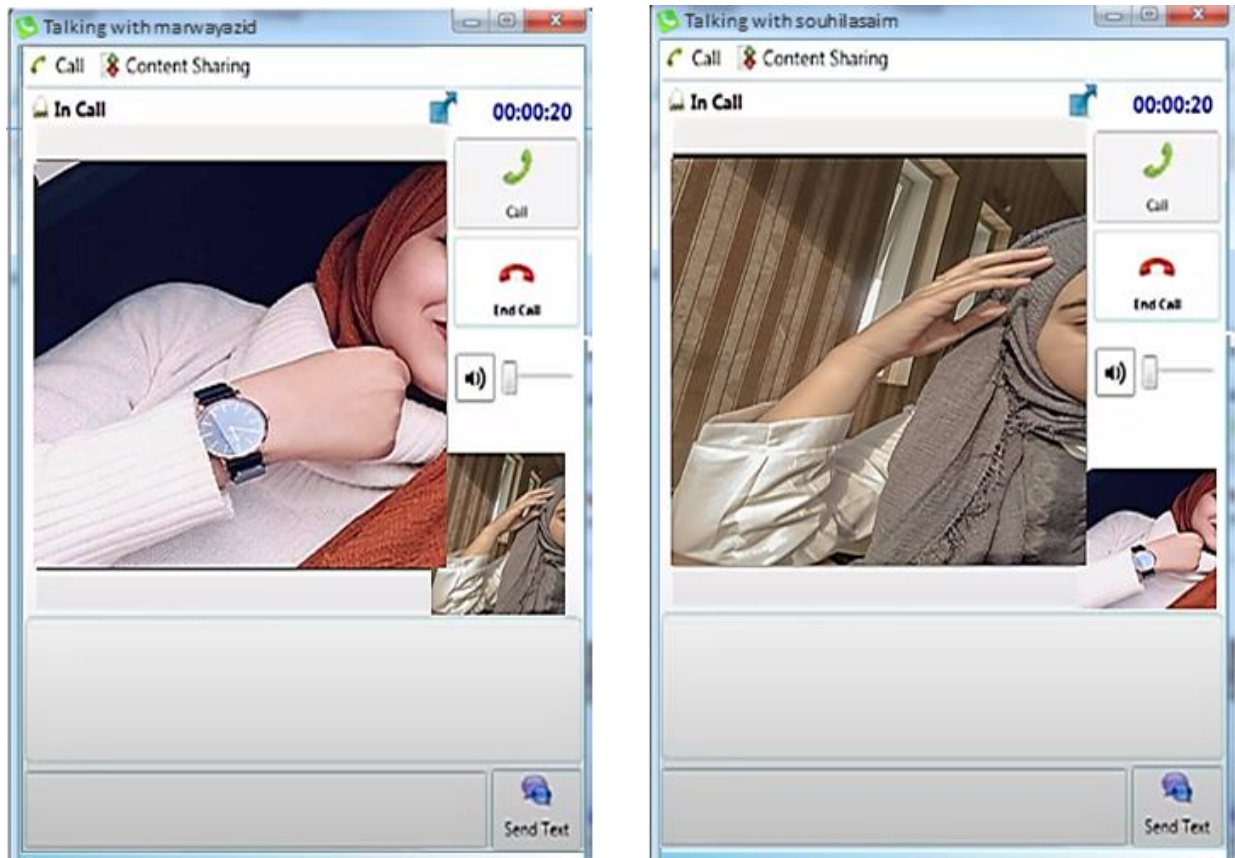


Figure IV.32 : Appel vidéo entre deux utilisateurs.

## IV.5 Conclusion

Au cours de ce dernier chapitre, on a mise en œuvre le réseau IMS par deux principaux éléments de la plateforme Open IMS Core qui sont ; La fonction de routage CSCF et la base de données HSS.

Notre plateforme a permis au client enregistré dans la base HSS, d'établir des appels audio, aussi d'envoyer des messageries instantanées et même de faire passer des communications vidéo à haute résolution.

## Conclusion générale

Depuis l'avènement des téléphones mobiles, il y a eu cinq générations de réseaux mobiles : 1G, 2G, 3G, 4G et la 5G. Le réseau 4G est un réseau full IP, la voix est transmise par commutation de paquet contrairement au réseau des générations précédentes, Il faut savoir que jusqu'à aujourd'hui la voix ne circule pas sur le réseau 4G sans la VoLTE, Cela signifie que lorsqu'un utilisateur passe un appel sur son Smartphone, celui-ci bascule automatiquement vers un réseau mobile 2G ou 3G.

La VoLTE, objet de notre projet de fin d'études est l'avenir des services vocaux qui migrent des services vocaux à commutation de circuits vers les communications par paquets, Elle permet de réaliser les appels téléphoniques sur le réseau 4G. Cette solution s'appuie sur un cœur réseau en IMS pour gérer les sessions IP d'application multimédia,

L'apport principal de l'IMS est défini comme la clé de la convergence vers le tout IP des réseaux fixes et mobile et voix/donnée. Ce fut une expérience bénéfique et très utile pour nous de pouvoir établir des sessions multimédia avec la fourniture de nouveaux services.

Ce travail nous a permis de mettre en lumière nos connaissances théoriques dans le domaine des réseaux et de comprendre l'architecture de l'IMS avec ses couches et protocoles utilisés (SIP, DAIEMTRE), Pour cela, nous utilisons la plate-forme "Open IMS Core", qui est une implémentation open source du cœur du réseau IMS, composée de P-CSCF, I-CSCF, S-CSCF et HSS. Cette réalisation, nous a aidé de faire des tests en conditions réelles sur les appels audio et vidéo et l'envoi de la messagerie instantanée, en même temps nous a permis de voir la traçabilité et le comportement des différents serveurs xCSCF, pour comprendre l'enregistrement des utilisateurs dans IMS et la signalisation, et le flux d'appels entre deux utilisateurs. Nous avons également eu la chance d'avoir une vision sur la transition vers cette solution VoLTE qu'est l'avenir des services vocaux.

## Bibliographie

- [1] Emmanuel TONYE Landry EWOUSSOUA, « *Planification et ingénierie des réseaux de télécoms* », Master pro 2 en télécommunications, Université de Yaoundé I, Ecole nationale supérieure polytechnique, Camerone, 2014.
- [2] Hermann Orly GBILIMAKO, « *Etude et mise en place d'une plateforme IMS sécurisée* », Mémoire de fin de cycle pour l'obtention du master professionnel en Réseaux Télécommunication, ISI de la Direction Générale de l'Enseignement Privé, Sénégal, 2015.
- [3] Boumechache Younes, Messaoudi Fares, « *Etude de la communication sans fils multi- porteuse UPMC* », Mémoire de fin d'études En vue de l'obtention du diplôme de Master Académique en Electronique des systèmes embarqués, Université Mohamed Larbi Ben M'hidi - Oum El bouaghi, 2021.
- [4] Yasser BOUSLAH, Monaim JOUINI, « *Dimensionnement et planification d'un réseau 3G/4G* », Licence Appliquée en Sciences et Technologies de l'Information et de la Communication en Réseaux et Systèmes des Télécommunications, Institut supérieur des études technologiques et communications de Tunis, 2015.
- [5] Orange Developer , « *Généralités et architecture de la 4G* », Documentation technique Orange Developer, <https://developer.orange.com/od-uploads/Generalites-et-architecture-de-la-4G.pdf>
- [6] Maxime Blondet, « *5G : déploiement, usages, forfaits... tout ce qu'il faut savoir sur le nouveau réseau mobile* », Mis à jour le 11 avril 2022, <https://blog.ariase.com/mobile/dossiers/5g>.
- [7] WikiMemoires, « *Évolution LTE, Architecture de LTE et Interface radio* », Informatique et Télécommunications, juillet 19, 2013, <https://wikimemoires.net/2013/07/evolution-lte-architecture-de-lte-et-interface-radio/>
- [8] Frédéric Launay, « *L'architecture du réseau de mobiles 4G* », février 2021, <https://blogs.univ-poitiers.fr/f-launay/tag/4g/>
- [9] BOUCHENTOUF Hadjer, BOUDGHENE STAMBOULI Riyad, « *Etude des performances des réseaux 4G (LTE)* », Mémoire de master en réseaux mobiles et services de télécommunication, Université de Tlemcen, 2013.
- [10] Mohamed Salem, « *LTE 4G Network Architecture* », mise à jour le 1 décembre 2008, <https://mobilepacketcore.com/lte-4g-network-architecture/>
- [11] Pierrick Labbe, « *VoLTE : tout savoir sur la technologie des appels 4G/5G* », 25 février 2022 , <https://www.meilleure-innovation.com/tout-ce-que-vous-devez-savoir-sur-la-volte/>



- [12] Varga, Pal, et al. «*Complex solution for volte monitoring and cross-protocol data analysis*». NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018.
- [13] Frédéric launay, « Technologie de transport de la voix en 4G », Université de Poitiers, 20 mars 2014, <https://blogs.univ-poitiers.fr/f-launay/2014/03/20/technologie-de-transport-de-la-voix-en-4g-csfb-part-2/>
- [14] nexcom, « *Quelles solutions pour la voix sur LTE (VoLTE)* », 16 janvier 2012, <https://www.nexcom.fr/quelles-solutions-pour-la-voix-sur-lte-volte/>
- [15] Yatebts, « *Resources for MNO* », <https://yatebts.com/documentation/resources-for-mno/>
- [16] Antoine CROCHET-DAMAIS, « IMS pour IP Multimedia Subsystem », <http://www.journal-dunet.com/solutions/0611/061115-ip-multimedia-subsystem.shtml>
- [17] Roshani, M., & Khorsandi, S. « *Performance analysis of the internet-protocol multimedia-subsystem's control layer using a detailed queueing Petri-net model* », International Journal of Communication Systems, 32(4), e3885. (2019).
- [18] « *The IP Multimedia Subsystem in Next Generation Networks* », [http://www.tele.pw.edu.pl/~mareks/auims/IMS\\_an\\_overview-1.pdf](http://www.tele.pw.edu.pl/~mareks/auims/IMS_an_overview-1.pdf)
- [19] BAHA Rachid, FARAJ Abderrahim et NIHARMINE Lahcen, « *Etude de l'architecture IMS et configuration d'OpenSer comme serveur de présence au dessus de l'OpenIMS* », Rapport de stage, Institut national de poste et télécommunications, Maroc, 2008.
- [20] RANDRIAMALALA Harinirina Maminomena, « *Le protocole SIP applique au système de signalisation de l'IP Multimedia Subsystem* », Mémoire d'ingénieur en Systèmes de Traitement de l'Information (STI), Université D'Antananarivo, école supérieure polytechnique, Madagascar, 2011.
- [21] « L'architecture IMS », <https://sites.google.com/site/bhsidali/project-definition>
- [22] MROUEH Lina & LABAKY Elie, « *Etude des procédures d'enregistrement et d'établissement de session en IMS* », 3<sup>ème</sup> Année du cycle ingénieur, 2006.
- [23] TAKH Houda et DAHMOUNI Nor El Islam, « *Etude et Amélioration de la (QoS) de la voix dans les réseaux 4G-LTE* », Mémoire de Master en Systèmes des Télécommunications, Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj, 2019.
- [24] Pujolle G., « *Les Réseaux* », Edition Eyrolles, 2008.
- [25] Ouakil L. et Pujolle G., « *Téléphonie sur IP* », Edition Eyrolles, 2007.

- [25] Znaty S. et Dauphin J.L., «*Transcription of SIP: Session Initiation Protocol* », Etudes et Formations en Télécommunication, 2005, <https://pdf4pro.com/view/sip-session-initiation-protocol-efort-com-2a94b6.html>
- [26] Saida KHAZRI, «*Déploiement d'IMS et provisionnement de la QoS dans le nuage informatique*», Mémoire de maîtrise électronique, Montréal, École de technologie supérieure, 2015.
- [27] Christopher Cox, «*An Introduction to LTE: LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications*», 2e Edition, Chris Cox Communications Ltd, UK (WILEY). ISBN : 978-1118818039, 2014.
- [28] <http://openimscore.sourceforge.net/docs/OSIMS-Raute.gif>