

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abou-Bakr Belkaid- TLEMCEM  
Faculté des Sciences et de la Technologie  
Département de télécommunication

## *Mémoire de fin d'études*

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

**Spécialité** : Réseaux et Télécommunications

**Par** : Fatmi Frid Nihad

Hachid Rafika

### **Thème**

**Les réseaux NGN**

**Implémentation de la solution OpenIMSCore**

Soutenu le : 12.-09-2020, devant le jury composé de :

MERZOUGUI Rachid	Professeur	Univ. Tlemcen	Président
ZERROUKI EL-hadj	MCB	Univ. Tlemcen	Examineur
Mr. MOUSSAOUI Djilali	MAA	Univ. Tlemcen	Encadreur de mémoire
Mr. MEHIAOUI SidAhmed	Chef de subdivision Réseaux core	Algérie Télécom	Co-Encadreur de mémoire

**Année universitaire 2019/2020**

## *Remerciement*

*Nous remercions ALLAH de nous avoir donné la force, santé, le courage et la patience pour l'élaboration de ce modeste travail.*

*Nous tenons à remercier notre encadreur à qui je dois beaucoup de respect Mr **MOUSSAOUI DJILLALI** pour son orientation et ses précieux conseils pendant cette période.*

*Nos remerciements les plus sincères vont aussi à Mr **MEHIAOUI SID AHMED** notre encadreur au sein de la société d'Algérie Telecom, pour la qualité de son encadrement exceptionnel, pour sa patience, ses encouragements et la confiance qu'il nous a toujours témoignée, sa disponibilité, ses directives précieuses et son appui considérable dans notre démarche*

*Nos remerciements s'adressent aussi à tout le personnel d'Algérie Télécom pour leur accueil.*

*Nous tenons à remercier aussi les membres du jury d'avoir bien accepté de consacrer leurs temps afin d'évaluer notre travail. Aux enseignants de notre université et département de télécommunication.*

*Aussi un grand merci à nos familles qui nous encouragent tout le temps dans notre vie, merci pour tous.*

*Enfin, on remercie tous ceux qui nous ont aidés de près ou de loin dans l'élaboration de ce travail.*

# *Dédicace*

*Je dédie ce travail :*

*A mes très chers parents, source de vie, d'amour et  
d'affection.*

*A ma chère sœur « Samira »*

*A mon meilleur frère « Sohaib »*

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

*A mes oncles et mes tantes ainsi leurs épouses, époux et  
enfants spécialement « Rania »*

*A ma très chère cousine « Nadia »*

*Toutes mes amies particulièrement « Farah Rania Asma  
Nesrine Rajae »*

*A « Rafika » chère amie avant d'être binôme*

*A tous mes enseignants et toute la section réseaux et  
télécommunications*

*A tout ceux qui mon aidée de près et de loin pendant tout la  
durée de mon parcours éducatif.*

*Nihad*

# *Dédicace*

*Je dédie ce modeste travail :*

*À ma très chère mère: qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie.*

*À Mon très cher père: qui a toujours été là pour moi, aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement et le respect que j'ai toujours pour vous.*

*À mes chers frères  
«Abdelkader, Abdelmalik, Mohamed, Rachid ».*

*À mes chères sœurs «Malika, Fadela, Nora, Yasmine, Zahira ».*

*À tous les enfants de ma famille.*

*À mes chères amies qui j'ai passé des meilleurs moments de ma vie et gardé de très bon souvenirs.*

*À Ma chère binôme « Fatmi Frid Nihad » et à toute sa famille.*

*À toute la promotion Télécommunication 2019/2020 que je leurs souhaite un bon avenir.*

*À tout ceux qui mon aidée de près et de loin pendant tout la durée de mon parcours éducatif.*

*Rafika*

## Résumé

Durant ces dernières années l'architecture de l'internet s'est développée par l'introduction de nouvelles technologies afin d'assurer une adaptation aux nouveaux besoins et l'objectif pour les opérateurs est de réaliser des économies en ayant à terme un seul réseau pouvant supporter différents services (voix /video /data , fixes et mobiles), alors qu'assez souvent aujourd'hui les grands opérateurs doivent exploiter, maintenir et faire évoluer en parallèle plusieurs réseaux basés sur des technologies disparates (quasiment un réseau par type de service).

Pour cela une nouvelle vision a été adoptée par les institutions de standardisation dans le domaine des télécommunications concernant les prochains réseaux ; une architecture appelée NGN (Next Network Génération).

Parmi les approches clés dans les réseaux NGN c'est la solution l'IMS (IP Multimedia Subsystem) où elle présente une meilleure solution tout IP pour les opérateurs afin d'offrir des services voix et multimédia dans un réseau convergé Fixe/Mobile.

### **Mot clés :**

NGN, IMS, IP/MPLS, OpenIMSCore, SIP,.....

## Abstract

In recent years the architecture of the Internet has developed through the introduction of new technologies to ensure adaptation to new needs and the objective for operators is to achieve savings by having a single network that can support different services (voice/video/data, fixed and mobile), whereas quite often today the large operators must operate, maintain and develop in parallel several networks based on disparate technologies (almost one network per type of service).

For this a new vision has been adopted by the standardization institutions in the field of telecommunications concerning the next networks; an architecture called NGN (Next Network Generation).

Among the key approaches in NGN networks is the IMS (IP Multimedia Subsystem) solution where it presents a better all-IP solution for operators to offer voice and multimedia services in a Fixed/Mobile converged network.

### **Keywords:**

NGN,IMS,IP/MPLS,OpenIMSCore, SIP .....

## Table des matières :

<i>remerciement</i> .....	1
<i>Dédicace</i> .....	2
<i>Dédicace</i> .....	3
<i>Résumé</i> .....	4
<i>Abstract</i> .....	4
Table des matières : .....	5
Liste des figures : .....	8
Liste des tableaux : .....	9
Abréviations .....	10
Introduction générale.....	13

## Chapitre I : Généralités sur les réseaux NGN

I.1 Introduction : .....	16
I.2 Idée générale : .....	16
I.3 Définition du réseau NGN: .....	17
I.4 Architecture des réseaux NGN : .....	18
I.4.1 Access (couche d'accès): .....	19
I.4.1.1 Couches Accès Opérateurs Fixes : .....	20
a MSAN : .....	20
b FTTH: .....	21
I.4.1.2 Couches Accès Opérateurs Mobiles : .....	24
a LTE : (La quatrième génération des téléphones mobiles).....	24
I.4.2 Couche Aggregation .....	26
I.4.3 Intelligent Service Edge : .....	28
I.4.4 La couche Core IP/MPLS : .....	29
I.4.5 Policy / service layer : .....	30
I.5 Aperçu sur la technologie IP/MPLS: .....	31
I.6 Type de NGN : .....	33
I.7 Evolution du NGN téléphonie vers NGN multimédia (IMS) : .....	33
I.7.1 NGN Téléphonie .....	33
I.7.2 NGN Multimédia .....	36
I.7.3 Convergence fixe-mobile: .....	37
I.8 Conclusion: .....	38

## Chapitre II : L'IMS

II.1	Introduction :	40
II.2	Objectif :	40
II.3	Définition de L'IMS :	40
II.4	Standardisation de L'IMS :	43
II.4.1	Fonctionnement du comité TISPAN :	43
II.4.1.1	La première publication « Release 1 » :	43
II.4.1.2	La seconde publication « Release 2 » :	43
II.5	Architecture de L'IMS :	44
II.5.1	La couche " Access"(physique) :	45
II.5.2	La couche "Transport" :	45
II.5.3	La couche "Session control" :	46
II.5.3.1	Bloc de contrôle des sessions :	46
II.5.3.2	Bloc des bases de données :	48
II.5.3.3	Bloc de l'interconnexion avec les autres réseaux :	48
II.5.3.4	Bloc de traitement du média :	49
II.5.4	La couche "Application" :	50
II.5.4.1	Les serveurs d'applications :	50
II.6	Les protocoles utilisés dans L'IMS et principes de fonctionnement:	51
II.6.1	Protocole SIP :	51
II.6.1.1	Description du protocole SIP :	51
II.6.1.2	Architecture de protocole SIP :	51
II.6.1.3	Responsabilités du SIP :	53
II.6.1.4	Les différentes requêtes (méthodes) de protocole SIP :	54
II.6.1.5	Les statuts de réponses :	55
II.6.2	Protocole DIAMETER :	56
II.6.2.1	Introduction :	56
II.6.2.2	Description du protocole DIAMETER :	56
II.6.2.3	Les responsabilités de Diameter :	57
II.6.2.4	Types de nœuds et Agents DIAMETER :	57
II.6.2.5	Messages DIAMETER :	59
II.6.2.6	Son rôle dans les réseaux NGN & IMS :	60
II.7	Signalisation dans L'IMS :	61
II.7.1	Type de signalisation en IMS :	61
II.8	Etude comparative des solutions IMS sur le marché : [10].	61
II.8.1	Solutions :	61

II.8.1.1 IMS AAA JUNIPER : .....	62
II.8.1.2 IMS par Ericsson: .....	63
II.8.1.3 OpenIMSCore:.....	63
II.8.2 Etude comparative des solutions :.....	64
II.9 Conclusion .....	65

### **Chapitre III : Mise en service d'une plate forme OPENIMSCORE**

III.1 <u>Introduction</u> :.....	67
III.2 Architecture de la solution : .....	68
III.3 Installation et configuration d'OpenIMSCore .....	69
III.3.1 Les pré-requis : .....	69
III.3.2 Récupération du code source d'Opensource IMSCore (Via SVN).....	70
III.3.3 Compilation d'OpensourceIMSCore : .....	71
III.3.4 Paramétrage de la Configuration d'IMS :.....	72
III.3.5 Lancement des serveurs d'OpenIMS: .....	74

### **Chapitre IV : Test et exploitation de la plateforme OpensourceIMSCore**

IV.1 Scénario: .....	79
IV.2 Configuration des abonnés IMS:.....	79
IV.3 Configuration et Utilisation d'un client IMS: .....	83
IV.4 Test et Fonctionnement : .....	88
IV.4.1 Test d'enregistrement .....	88
IV.4.2 Test d'appel:.....	89
IV.4.3 Test de la messagerie instantanée :.....	93
Conclusion générale : .....	95
Références:.....	96



## Liste des figures :

Figure I.1: L'idée générale de réseaux NGN.....	17
Figure I.2: Principe de consolidation des réseaux.....	17
Figure I.3 : Architecture de réseau NGN.....	18
Figure I.4 : Couche d'accès.....	19
Figure I.5 : Position de MSAN dans NGN.....	20
Figure I.6 : Architecture de FTTH.....	21
Figure I.7 : Architecture P2P - Point à Point Passif.....	22
Figure I.8 : Architecture PON.....	22
Figure I.9 : Architecture de LTE.....	24
Figure I.10 : Couche agrégation network IP/MPLS.....	27
Figure I.11 : Intelligent Service Edge.....	29
Figure I.12 : Core IP/MPLS.....	29
Figure I.13 : Policy/ Service Layer.....	31
Figure I.14: IP/MPLS.....	32
Figure I.15 : Services dans le RTC.....	33
Figure I.16 : Services dans le NGN téléphonie.....	34
Figure I.17 : Exemple d'architecture NGN téléphonie.....	35
Figure I.18 : Protocoles de contrôle (MGCP, MEGACO) versus protocoles de signalisation (SIP-T, BICC).....	36
Figure I.19 : Exemple d'architecture multimédia.....	37
Figure II.1 : Vue simplifiée d'IMS par TISPAN.....	41
Figure II.2 : IP MultiMedia Subsystem.....	42
Figure II.3 : Architecture de l'IMS.....	45
Figure II.4 : Fonctionnellement, les CSCF suivent les paradigmes de l'Internet.....	48
Figure II.5 : Architecture de SIP.....	52
Figure II.6 : Principe de Protocole SIP.....	53
Figure II.7 : Enregistrement d'un utilisateur.....	54
Figure II.8 : les nœuds DIAMETER.....	58
Figure II.9 : Mécanisme de gestion des erreurs.....	59
Figure II.10 : structure du message Diameter.....	60
Figure II.11 : Architecture de la solution IMS AAA de JUNIPER.....	62
Figure II.12: Architecture OpenIMSCore.....	63
Figure III.1: Opensource IMS.....	67
Figure III.2: la plate-forme d'architecture.....	68
Figure III.3: VMware Workstation 15 Player.....	70
Figure III.4: Démarrage de P-CSCF.....	75
Figure III.5: Démarrage d'S-CSCF.....	76
Figure III.6: Démarrage d'I-CSCF.....	76
Figure III.7: Démarrage de FHoSS.....	77
Figure IV.1: Le scénario.....	79
Figure IV.2: interface de connexion au HSS.....	80
Figure IV.3: page d'accueil de HSS.....	80
Figure IV.4: Public User Identity-IMPU-rafika.....	81
Figure IV.5: Private User Identity –IMPI-rafika.....	82
Figure IV.6: IMS Subscription-IMSU-rafika.....	83
Figure IV.7: config networking IP P-CSCF et le port.....	84
Figure IV.8: Boghe-IMS client.....	85
Figure IV.9: ajouter un contact –rafika.....	85
Figure IV.10: Contact de Mohamed.....	86
Figure IV.11: IMSDroid.....	86
Figure IV.12: Test d'enregistrement.....	89
Figure IV.13: Test d'appel.....	89
Figure IV.14: Message de Nihad.....	93

Figure IV.15: Message de Rafika ..... 94

**Liste des tableaux :**

Tableau I. 1 : Les Protocoles recommandés pour différents services..... 27  
Tableau II. 2: Méthode de base ..... 55  
Tableau II . 3: Méthodes SIP utilisées par IMS ..... 55  
Tableau II . 4: Etude comparative des solutions. .... 64

## **Abréviations :**

**3GPP** : 3rd Generation Partnership Project.

**AAA** : Authorization Authentication Accounting.

**ATM** : Asynchronous transfer Mode.

**ADSL** : Asymmetric Digital Subscriber Line.

**API** : Application Protocol Interface.

**AVP** : Attribute Value Pairs.

**BGP** : Border Gateway Protocol

**BTS** : Base station ( Base Transceiver Station ).

**BRAS** : Broadband Remote Access Server.

**BICC** : Bearer Independent Call Control

**CDMA** : Code division multiple access

**CAP** : Camel Application Part

**DSLAM** : digital subscriber line access multiplexer

**DSR** : Diameter Signaling Router .

**DRF** : Diametre Routing Function .

**EDGE** : Enhanced Data rate for GSM Evolution

**EoMPLS** : Ethernet over MPLS

**EVPL** : ligne privée virtuelle business ethernet (Ethernet Virtual Private Line)

**EIR** : Equipment Identity Register

**E-LAN** : multipoint-to-multipoint

**FRR** : Fast Re route

**FMC** : Fixed Mobile Convergence

**GTP** : GPRS Tunneling Protocol

**HSPA** : High Speed Packet Access

**H-VPLS** : Hierarchical Virtual Private LAN Service.

**IPTV** : Internet Protocol Television.

**IEEE** : Institute of Electrical and Electronics Engineers.

**IETF** : Internet Engineering Task Force..

**IM-SSF** : IP Multimedia-Service Switching Function.

**INAP** : Institut national d'administration publique.

**IPoE** : Internet Protocol over Ethernet.

**ISG** : Integrated Services Gateway.

**ISDN** : Integrated Services Digital Network ou RNIC .

**ISUP** : Institut de Statistique de l'Université de Paris.

**L2TP** : Layer 2 Tunneling Protocol.

**MSAN** : Multi Service Access Node.

**MAP** : Mobile Application Part ..

**MEGACO** : Media Gateway Control Protocol.

**MSTP** : Multiple Spanning Tree Protocol. .

**NPVR** : Network Personal Video Recorder.

**PABX (PBX ou IPBX)** Private Automatic Branch eXchange

**PIM-SSM** : PIM Source-Specific Multicast.

**PIM** : Protocol-Independent Multicast.

**PSTN** : public switched telephone network

**PLMN** : Public Land Mobile Network

**P-CSCF** : Proxy-CSCF

**PDA** : Personal Digital Assistant

**PPPoE** : point-to-point protocol over Ethernet

**PDF** : Policy Decision Function

**POTS** : Postural orthostatic tachycardia syndrome

**QoS** : Qualité de Service.

**QoE** : Quality of Experience.

**RFC** : Requests Ffor Comments

**RI** : Réseaux Intelligent

**RSVP-TE** : Resource Reservation Protocol - Traffic Engineering

**RTP** : Real Time Protocol

**RTCP** : Real Time Control Protocol

**RSVP**: Resource Reservation Protocol

**SCS** :Service Capability Server .

**SDC** :Signaling Delivery Controller .

**SDP** :Session Description Protocol

**SPAN** : Services and Protocols for AdvancesNetworks.

**SSL** : Secure Socket Layer.

**SCE** : Service Control Engine.

**SCP** : Service Control Point.

**SCTP** : Stream Control Transmission Protocol.

**SRP** : Specialized Resource Point.

**SIP-T** : SIP for Telephones.

**SOAP** : Simple Object Access Protocol.

**TISPAN** : Telecommunications and Internet converged Services and Protocols for Advanced Networking.

**TTL** : Time To Live.

**TIPHON** :Telecommunications and Internet Protocol Harmonization Over Networks. .

**TLS** : Transport Layer Security.

**TTS** : Text To Speech.

**UMTS** : Universal Mobile Telecommunication Service.

**USIM** : Universal Subscriber Identity Module.

**UTRAN** : UMTS Terrestrial Radio Access Network.

**URI** : Uniform Resource Identifier.

**USIM** : Universal Subscriber Identity Module.

**VPN** : Virtual Private Network..

**VoLTE** : Voice over LTE via IP Multimedia Subsystem.

**WIMAX** : Worldwide Interoperability for Microwave Access.

**ZTD** : Zone Très Dense.

## INTRODUCTION GENERALE :

L'évolution de la technologie et des réseaux mobiles a toujours été influencée par une forte demande des utilisateurs en applications multimédia (Données et voix). Les réseaux fixes et mobiles ont connu une évolution majeure ces dernières décennies afin de satisfaire à ces demandes si fortes des consommateurs.

Du côté des réseaux mobiles, on est passé des réseaux 1G aux réseaux 4/5G (réseau sans fil) afin d'avoir un débit de transfert de données considérables. Tandis que du côté des réseaux fixes, les technologies xDSL permettant d'avoir un transfert de données à haut débit ainsi que les réseaux FTTH.

L'utilisation du protocole IP (Internet Protocol) pour la voix, les données, le multimédia est en train d'entraîner la convergence dans les réseaux ; que ce soit le fixe, le mobile, le sans fil et autres.

La convergence des réseaux et le moyen par lequel les opérateurs faciliteront à leurs clients un accès facile à leurs services et leurs proposant des applications innovantes (VoIP, visioconférence, vidéo à la demande, IPTV, la visiophonie,...) . C'est ce défi de convergence entre fixe et mobile que relève la technologie IMS en permettant d'être joignable où que l'on soit, sur un ordinateur comme sur un mobile ou autre terminal bénéficiant de l'étendue de l'offre multimédia.

Ce mémoire est organisé en quatre chapitres :

Le premier chapitre définit la technologie NGN en abordant les différentes couches d'architecture NGN ainsi que leurs types puis présenter IP/MPLS et son principe de fonctionnement. Cette partie donne une idée sur l'évolution du NGN téléphonie vers NGN multimédia IMS .

Le deuxième chapitre, sera consacré à la solution IMS, son standardisation et les protocoles utilisés ainsi que leurs principes de fonctionnement (SIP ,DAIMETRE)

Dans le troisième chapitre et afin de mettre en pratique les aspects théoriques de la technologie IMS nous allons présenter la solution open source OPENIMSCORE et son implémentation dans un environnement linux.

Le dernier chapitre sera consacré à l'exploitation et le paramétrage de cette plateforme en faisant des tests réels d'appels audio/vidéo et de messagerie instantanée.

### **Problématique:**

Le monde de la technologie et de l'informatique s'est développé très récemment, et le domaine de télécommunication s'est développé rapidement au cours des dernières années. Les réseaux fixes et mobiles ont connu des évolutions importantes pour répondre aux demandes croissantes de leurs utilisateurs en offrant un très haut débit Internet à leurs clients.

Il y a eu beaucoup d'efforts déployés par les opérateurs mobiles et fixes où ils ont investi dans l'infrastructure du réseau mais il n'ont pas bénéficié d'autres services à valeur ajoutée tel que la visiophonie, visioconférence, vidéo à la demande, IPTV,...ect ,contrairement à d'autres fournisseurs (boîtes) qui fournissent ces services en utilisant les infrastructures internet des opérateurs tel que viber, skype, messenger, zoom, google meet, netflix,.....etc, à noter que ces fournisseurs tiers ne garantissent aucune qualité de service à ces utilisateurs.

A cet effet les opérateurs Mobiles et fixes sont obligés de profiter de ces valeurs ajoutées et offrir les services mentionnés ci dessus à leurs clients en garantissant une très bonne qualité de service où la solution est de migrer vers un réseau NGN Multimedia y compris un cœur IMS.

En plus auparavant le service voix dépend du type d'accès par exemple dans le mobile 2G et 3G on trouve la partie accès Radio et la partie core BSC/MSC et chez les opérateurs fixe les MSANs dans la partie accès et la partie core le Soft Switch. Par contre dans la solution IMS toute la partie contrôle de la voix est géré par une seule plateforme IMS CORE ; donc chez le même opérateur opérant sur le Mobile et le fixe l'IMS représente une solution de convergence de tous les clients indépendamment du type d'accès Fixe (xDSL, FTTX, Wimax, 4G LTE fixe,...) ou bien mobile (4G et 5G).

En plus l'un des avantages de la solution IMS c'est qu'un client a une seule entité qui peut l'utiliser à accéder à plusieurs services (voix/visiophonie, vidéo à la demande, webmeting , IP-TV, ....).

### **L'objectif :**

En raison des problèmes rencontrés par les opérateurs mentionnés au paragraphe précédent l'objectif de notre projet est de proposer des solutions pour créer une plate-forme de réseaux de nouvelles générations NGN ( Next Génération Network )orientée multimédia IMS( IP Multimedia Subsystem): une nouvelle architecture basée sur des nouveaux concepts de technologie, supporte un réseau tout IP.

# *Chapitre I*

## ***GENERALITES SUR LES RESEAUX NGN***



## **I.1 Introduction :**

Le sigle NGN est l'abréviation de l'anglais Next Generation Network, ce qui signifie réseau de nouvelle génération. Ce terme générique désigne la transformation des architectures et mécanismes des réseaux cœur RTC (Réseau Téléphonique Commuté) et GSM pour concilier la fiabilité et la maîtrise de ces réseaux de téléphonie avec la souplesse et l'ouverture de l'Internet. Cette transformation est motivée par un ensemble de facteurs :

- L'évolution des réseaux d'accès et l'arrivée du haut débit.
- La généralisation du protocole IP comme protocole de transport unique.
- L'évolution des usages vers des services multimédia convergents voix/donnée (notamment via Internet) et fixe/mobile.

Le choix d'un cœur de réseau paquet pour le NGN a nécessité l'introduction de nouveaux types de protocoles de communication, notamment pour le transport des données, et pour l'établissement des sessions de communication.

Les premiers déploiements que l'on peut qualifier de pré-NGN ont commencé dès 1999 pour des offres de transit de voix sur IP. Avec l'expansion des réseaux d'accès haut-débit de type xDSL ou UMTS, le NGN a petit à petit fait son apparition dans les foyers et permis la diffusion de nouveaux services comme la voix sur IP, la visiophonie, la messagerie instantanée et les services de Présence.

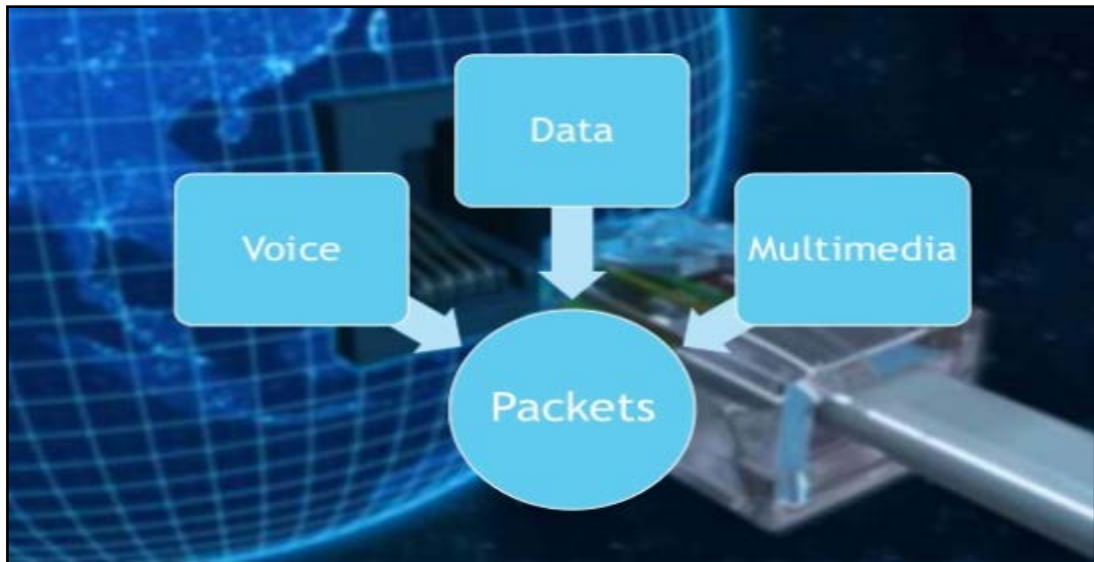
De nombreux travaux sont en cours dans les organismes de normalisation pour définir les architectures et les mécanismes NGN, notamment à l'IETF (pour la définition des nouveaux protocoles), au 3GPP (pour l'UMTS, la téléphonie mobile de troisième génération), à l'ETSI (pour l'évolution du réseau téléphonique commuté dans le groupe TISPAN) et à l'ITU [1].

## **I.2 Idée générale :**

Aujourd'hui, la téléphonie, Internet et les réseaux mobiles cellulaires continuent d'être des domaines différents, chacun a ses propres protocoles et services.

L'idée générale derrière le NGN est qu'un réseau transporte tous les types de données et fournit des services (voix, données et toutes sortes de médias comme une vidéo) en les encapsulant dans des paquets, semblables à ceux utilisés sur Internet.

Les NGN sont généralement construits autour du protocole Internet (IP), et par conséquent le terme toute IP est aussi parfois utilisé pour décrire la transformation vers NGN.

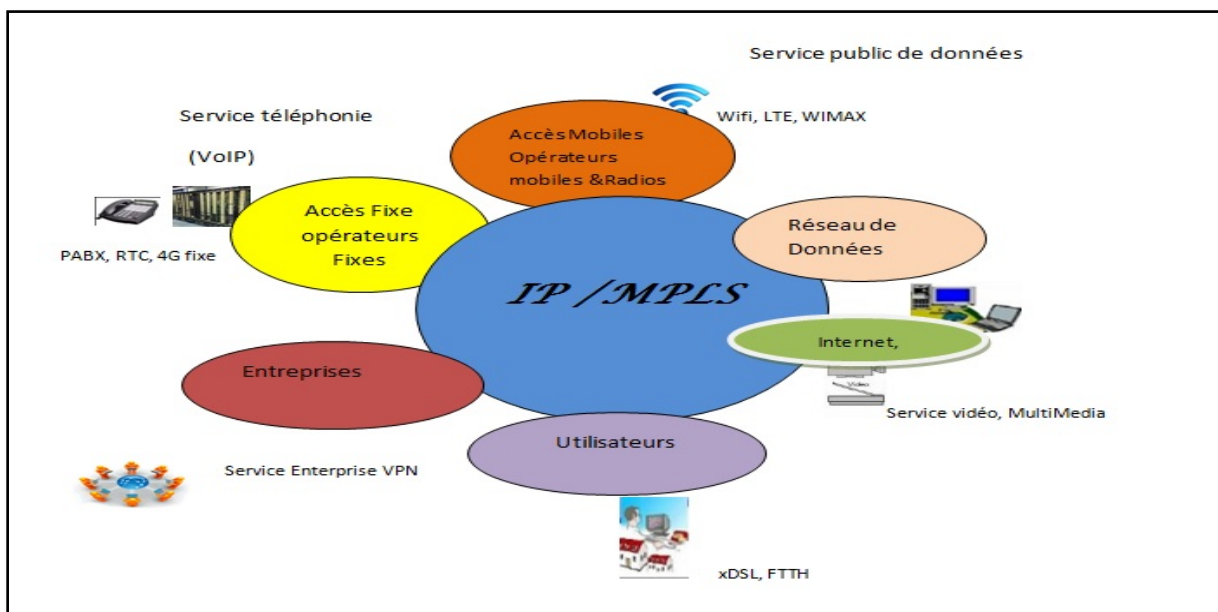


**Figure I.1: L'idée générale de réseaux NGN**

### **I.3 Définition de réseau NGN:**

Les NGN sont définis comme un réseau de transport en mode paquet permettant la convergence des réseaux Voix/Données et Fixe/Mobile, ces réseaux permettant de fournir des services multimédia accessibles depuis différents réseaux d'accès.

Afin de s'adapter aux grandes tendances qui sont la recherche de souplesse d'évolution de réseau, la distribution de l'intelligence dans le réseau, et l'ouverture à des services tiers, les NGN sont basés sur une évolution progressive vers le « tout IP » et sont modélisés en couche indépendantes dialoguant via des interfaces ouvertes et normalisées [2].



**Figure I.2 : Principe de consolidation des réseaux**

## I.4 Architecture des réseaux NGN :

Le NGN se compose de six couches : Accès, Agrégation, iPDWDM, Intelligent Service Edge, IP/MPLS Core et Policy/Service.

- **Access (couche d'accès)** : Fournit l'accès aux clients résidentiels et professionnels par DSL, fibre, câble ou sans fil.
- **Carrier Ethernet Aggregation (Agrégation network IP/MPLS)** : regroupe le réseau d'accès dans un réseau Ethernet et assure l'inter-connectivité avec la périphérie IP/MPLS et le cœur IP/MPLS.
- **IPODWDM optical network (réseau optique IPODWDM)** : permet des services d'agrégation optique avec multiplexage Ethernet intelligent en utilisant IP/MPLS sur le multiplexage de division de longueur d'onde dense (IPODWDM).
- **Intelligent Service Edge** : Interfaces des services avec le noyau IP/MPLS ; c'est l'avantage du fournisseur pour les services d'abonnés résidentiels et professionnels.
- **Core IP/MPLS** : Fournit un routage IP/MPLS évolutif dans le réseau central.
- **Policy/service layer** : assure la gestion de la politique sur les services a large bande pour contrôler la prestation des services – un élément – clé du cadre d'échange de services.

La figure I. 3 présente les différentes couches de réseau NGN avec les différentes entités fonctionnelles [3] [4].

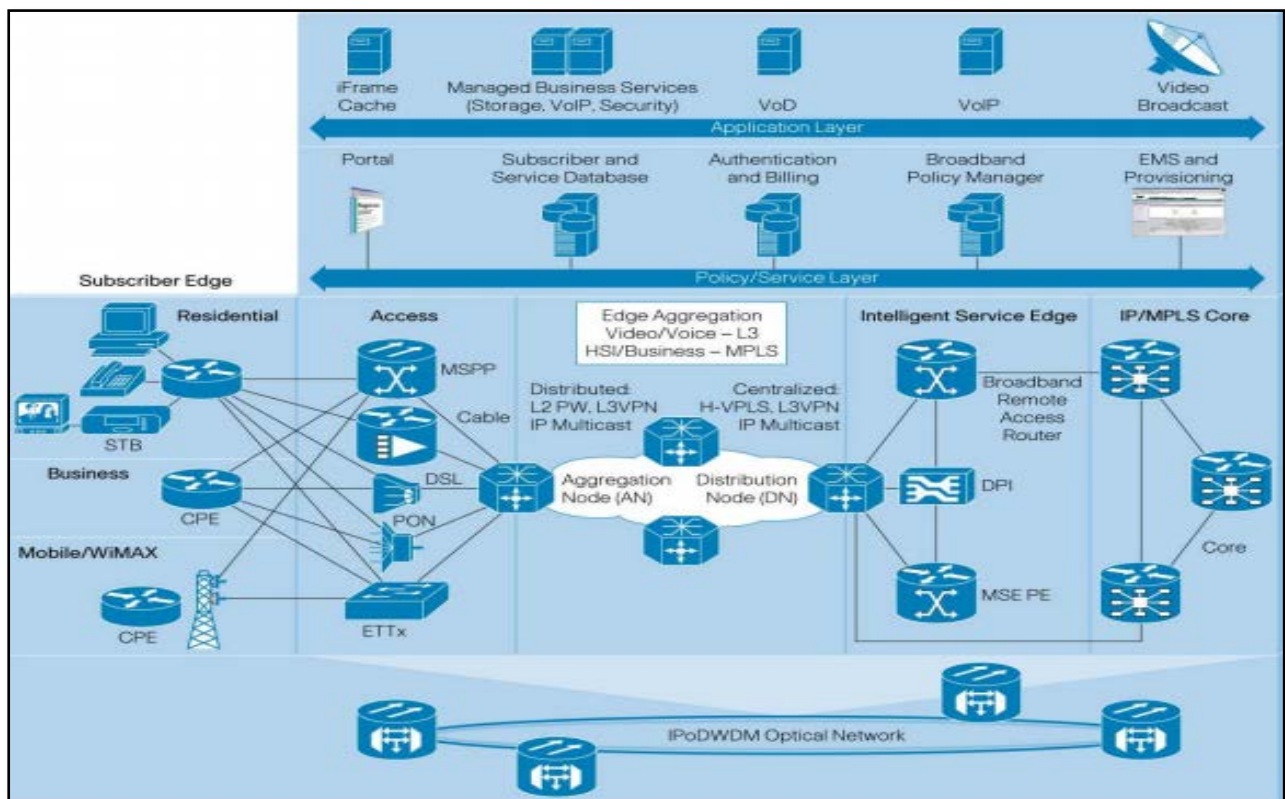


Figure I.3 : Architecture de réseau NGN

## I.4.1 Access (couche d'accès):

La composante d'accès du réseau fournit un accès physique filaire ou sans fil aux abonnés. Ce réseau doit assurer le transport de tous les types de réseaux et de dispositifs d'accès, y compris les réseaux DSL(câble), PON(FTTH),MSAN , LTE (4G). En outre, les services doivent être conçus en fonction du type de client et le type de réseau d'accès.

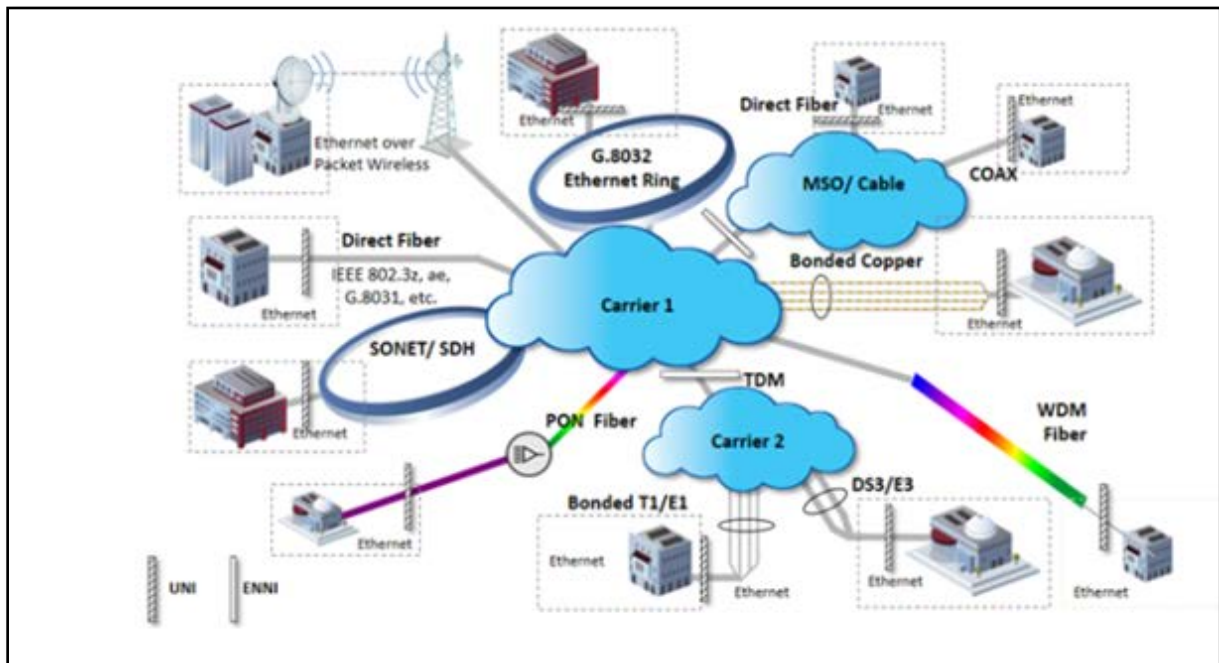


Figure I.4: Couche d'accès

### I.4.1.1 Couches Accès Opérateurs Fixes :

Les opérateurs fixes déploient plusieurs solutions fixes à leurs clients tel que les MSANs(xDSL) et le FTTH et aussi des solutions sans fil tel que 4G fixe et le Wimax.

#### a MSAN :

Définition de MSAN (Multi Service Access Node) :

C'est une technologie télécom d'accès qui permet de rapprocher les équipements des clients d'un opérateur fixe afin d'offrir les services voix et data à des débits plus élevés. Les MSANs supportent plusieurs types de cartes POTS (voix) COMBO (voix/data) en utilisant plusieurs technologie xDSL pour raccorder les clients résidentiel et professionnel tel que ADSL+, VDSL, SHDSL....ect. A travers cet équipement l'opérateur peut offrir une diversité de service à ces clients comme triplay (voix, Internet, IPTV..).

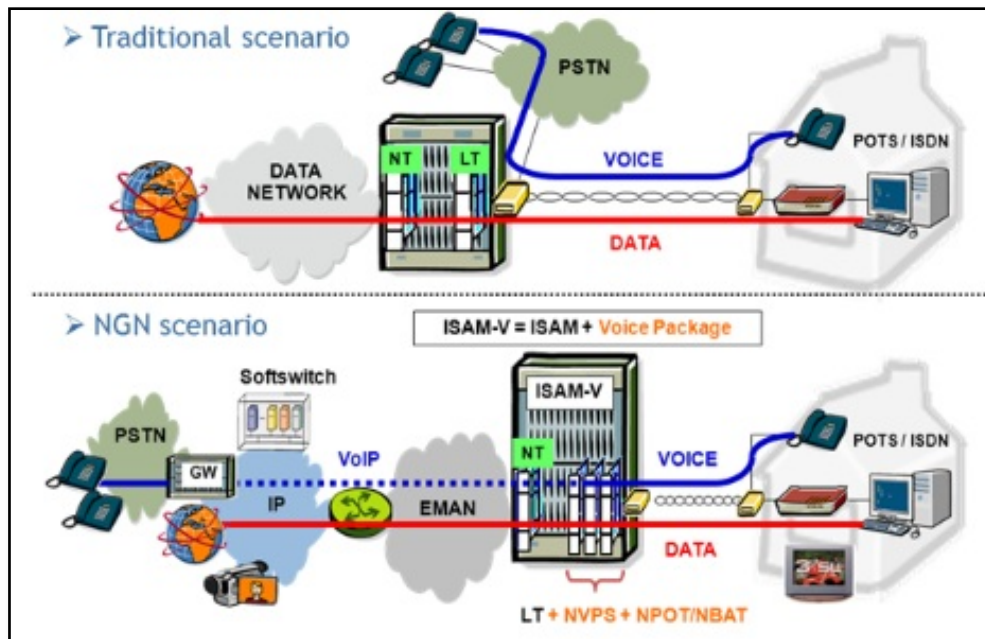


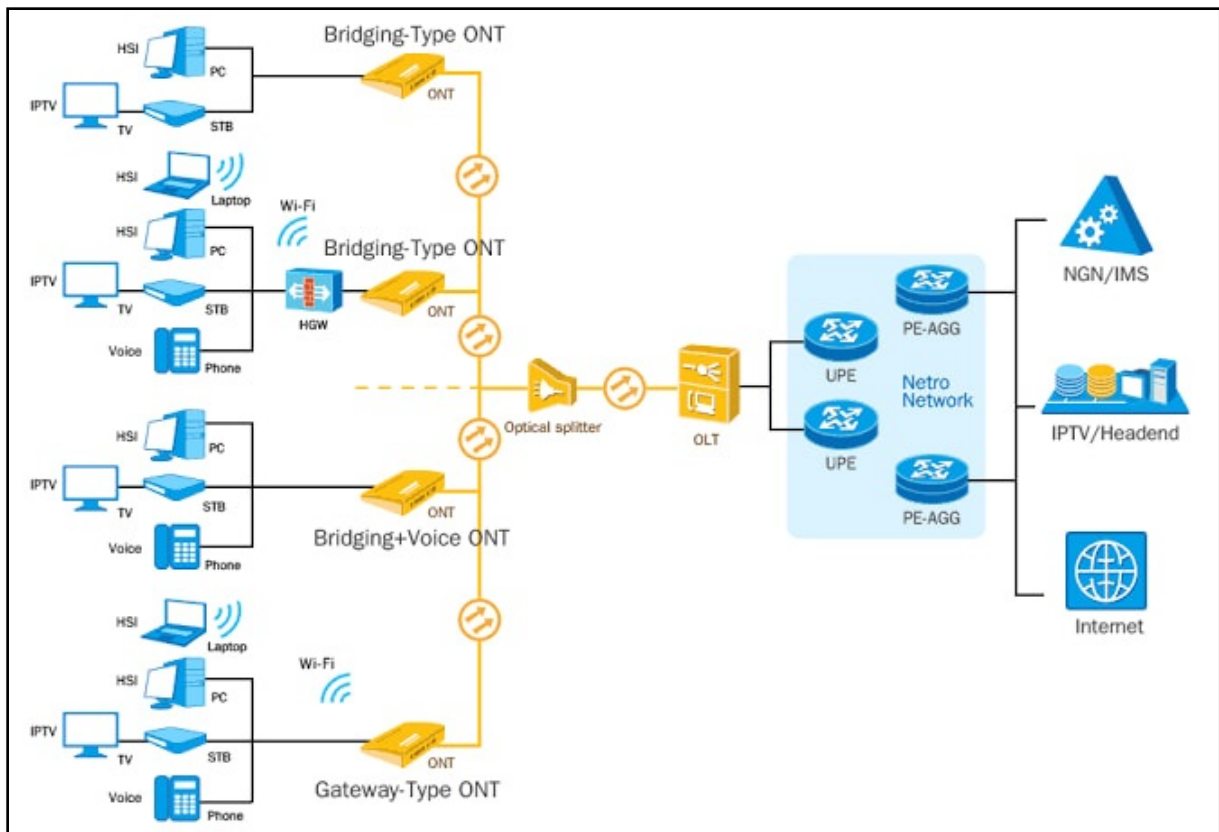
Figure I.5: Position de MSAN dans NGN

- **FTTH :(Fibre To The Home)**

Le FTTH (Fiber to the Home - Fibre jusqu'à l'abonné) correspond au déploiement de la fibre optique depuis le nœud de raccordement optique (lieu d'implantation des équipements de transmission de l'opérateur) jusque dans les logements ou locaux à usage professionnel. Le FTTH permet donc de bénéficier de tous les avantages techniques de la fibre sur l'intégralité du réseau jusqu'à l'abonné. Il se distingue d'autres types de déploiement qui combinent l'utilisation de la fibre optique avec des réseaux en câble ou en cuivre[5].

Le déploiement de la partie terminale des réseaux (boucle locale) s'entend :

- dans les rues (déploiement horizontal)
- puis dans les immeubles (déploiement vertical dans les immeubles collectifs)
- enfin jusque dans les logements (raccordement final).



**Figure I.6: Architecture de FTTH**

L'objectif de FTTH est d'utiliser la transmission et la réception des données sur les câbles fibres dans l'ensemble du chemin de la source à la limite destination. Pour ce faire, connecter le câble à fibre optique à la limite du client. Le réseau soutient la livraison de la fibre à domicile, les entreprises, les bureaux et autres, Puis il y a des types qui sont :

- Fibre à la bordure.
- Fibre optique dans le bâtiment.
- Fibre à la maison.

Son réseau FTTH se compose d'un total d'éléments qui sont :

- OLT (Terminal de Ligne Optique) Optical Line Terminal : Les deux fenêtres dans la zone centrale sont considérées comme le dispositif de base et peuvent accueillir un grand nombre d'utilisateurs.
- ONT (Terminal de Réseau Optique) Optical Network Terminal : Il s'agit de l'appareil que vous avez à la maison et qui se connecte à l'écran et qui est la principale source du Service pour votre appareil personnel, par exemple : TV, téléphone, VoIP, Routeur.
- ODN (Réseau de Distribution Optique) Optical Distribution Network : Les parties sont entre celle qui est à l'utilisateur et celle qui est à la centrale et se compose de : Câbles à fibre optique, répartiteur.

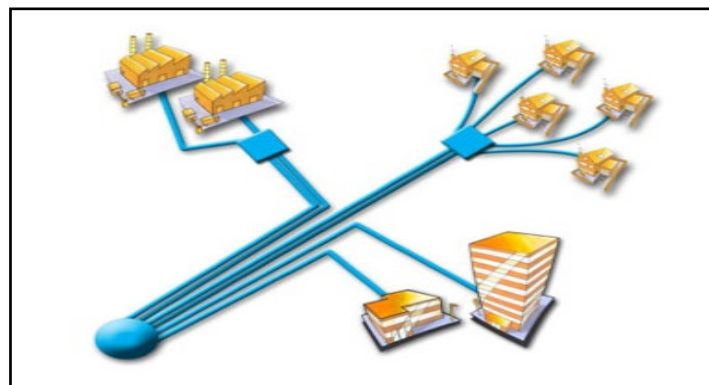
- **Architecture des réseaux FTTH :**

Plusieurs architectures coexistent pour raccorder le NRO ( le nœud de raccordement optique) à l'abonné. Les principales sont le P2P et le PON.

- P2P – Point à Point passif

Le réseau point à point comprend au moins une fibre continue et non partagée entre le NRO et l'utilisateur.

Cette architecture est utilisée uniquement par Free dans les ZTD. Elle demande un investissement plus important puisque une fibre doit être tirée du NRO jusqu'au domicile du client mais elle permet une bande passante maximale avec un débit garanti [6].

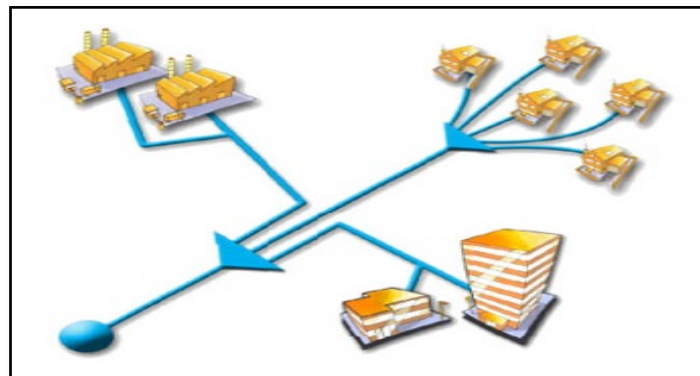


**Figure I.7: Architecture P2P - Point à Point Passif**

- PON – Passive Optical Network ou Point à Multipoint passif

Une architecture PON est un réseau qui utilise un système de couplage passif (coupleur optique, splitter) grâce auquel une seule fibre partant du NRO peut relier jusqu'à 128 utilisateurs.

Le trafic de chaque abonné est isolé via du multiplexage et permet des économies dans le déploiement. L'inconvénient est que la bande passante de la fibre est partagée entre plusieurs abonnés [6].



**Figure I.8: Architecture PON**

#### **I.4.1.2 Couches Accès Opérateurs Mobiles :**

Actuellement les opérateurs mobiles ont déployé la technologie 4G presque dans tous leurs réseaux et prochainement vers la 5G, dans cette partie nous allons présenter un aperçu sur la technologie 4G.

##### ***a* LTE : (La quatrième génération des téléphones mobiles).**

##### Définition :

La LTE (Long Term Evolution) est un projet mené par l'organisme de standardisation 3GPP visant à rédiger les normes techniques de la future quatrième génération en téléphonie mobile. Elle permet le transfert de données à très haut débit, avec une portée plus importante, un nombre d'appels par cellule supérieur (zone dans laquelle un émetteur de téléphonie mobile peut entrer en relation avec des terminaux) et une latence plus faible. En théorie, elle permet d'atteindre des débits de l'ordre de 50 Mbps en lien ascendant et de 100 Mbps en lien descendant, à partager entre les utilisateurs mobiles d'une même cellule.

Pour les opérateurs, la LTE implique de modifier le cœur du réseau et les émetteurs radio. Il faut également développer des terminaux mobiles adaptés. En termes de vocabulaire, le futur réseau s'appelle EPS (Evolved Packet System). Il est constitué d'un nouveau réseau d'accès appelé LTE (Long Term Evolution) et d'un nouveau réseau cœur appelé SAE (System Architecture Evolution) ou EPC (Evolved Packet Core) [7].

##### Caractéristiques de LTE :

- Amélioration de l'interface radio afin d'augmenter le débit montant/descendant, et la capacité, ainsi que la performance en bordure de cellule.
- Réduction du délai d'accès : le délai d'aller-retour est inférieur à moins de 10ms et d'initialisation est inférieur à 100 ms afin de supporter des services interactifs et temps réel.
- Mobilité : la performance de LTE est optimisée dans le cas où la vitesse est inférieure à 15km/h. LTE supporte la vitesse de 120 à 350 km/h (voire 500 km/h, selon la bande utilisée)
- Flexibilité du spectre radio : LTE peut-être déployé dans des bandes allant de 1,25 MHz à 20 Mhz, et la bande appariée et non appariée de la 3G. Cela permet à l'opérateur de déployer LTE sur la bande existante, de ne pas demander le permis de nouvelle bande.
- Architecture « tout IP », il y a une partie significative du travail de 3GPP pour convertir l'architecture réseau du cœur vers une architecture tout IP qui est envisagée pour simplifier l'interfonctionnement avec les réseaux filaires et les réseaux sans fils non-3GPP.
- Architecture simplifiée permet d'améliorer l'extensibilité des réseaux.
- Compatibilité avec les réseaux 3G existants. Il faut que LTE supporte le handover (est une fonction importante qui maintient une connectivité sans faille lors du passage d'une station de base à une autre) avec les réseaux existants tels que UMTS/HSPA et



GSM/GPRS/EDGE. De plus, il faut supporter le handover inter-domaines entre sessions de commutation de paquets et de circuits [8].

### Architecture de LTE :

La figure I-9 présente l'architecture générale d'un réseau LTE que se compose d'un réseau d'accès et d'un réseau cœur (Il y a trois nœuds principaux : MME au plan contrôle, S-GW et P-GW au plan utilisateur). .

L'évolution majeure de l'ePC est la séparation des plans contrôle et usage pour les équipements cœur. A l'image du NGN (Next Generation Network, évolution portée par la Release 4 3GPP) pour le circuit, les flux « contrôle » et « usage » ne seront plus, dans la plupart des cas, à destinations des mêmes équipements.

Au niveau du cœur de réseau, il y a une séparation des équipements selon leurs fonctions : le MME (Mobility Management Entity) traite uniquement de la signalisation (signalisation avec les antennes-relais, et avec les terminaux), alors que les S-GW (Serving-Gateway) et P-GW(Packet-Gateway) agrègent et font transiter les données utilisateurs, toujours encapsulées dans des tunnels GTP. Le HLR hérite d'une nouvelle dénomination : HSS (Home Subscribers Server), mais conserve des fonctionnalités équivalentes. L'authentification au réseau LTE doit obligatoirement se faire avec une carte USIM (introduite avec les réseaux mobiles de 3ème génération).

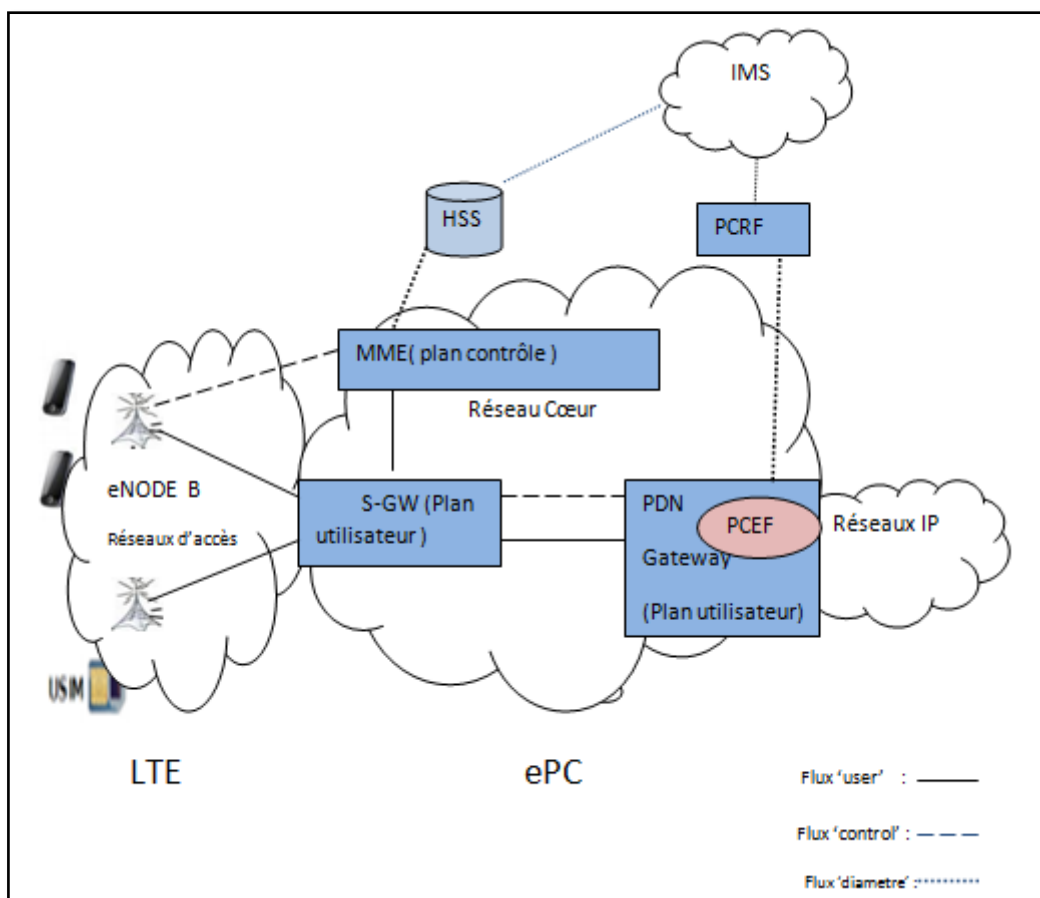


Figure I.9: Architecture de LTE

## Nœuds principaux:

- **Entité eNODE B :** L'eNodeB est responsable de la transmission et de la réception radio avec l'UE. l'eNodeB s'occupe de : la modulation/démodulation, le codage/ décodage des informations transmises sur l'interface radio.
- **Entité S-GW( Serving Gateway):** La Serving Gateway sera responsable de l'acheminement des flux « utiles » dans le réseau cœur (les communications voix, le trafic data, etc.). Les fonctions de l'entité Serving GW incluent :
  - Point d'ancrage pour le handover inter-eNodeB.
  - Point d'ancrage pour le handover LTE et les réseaux 2G/3G.
  - Interception légale .
  - Routage des paquets et relai des paquets.
  - Comptabilité par usager pour la taxation inter-opérateurs .
  - Marquage des paquets dans les sens montant et descendant .
- **Entité P-GW(Packet Data Network Gateway):** P-GW est responsable du lien avec les autres réseaux (publics ou privés), et notamment avec le monde Internet.

Il fournit des connexions entre réseau LTE et d'autres réseaux IP, PSTN, non-3GPP. L'allocation d'adresse IP pour l'UE, filtrage des paquets pour chaque utilisateur (Policy Enforcement Point), et le support de la tarification d'une session sont des autres fonctions du P-GW. P-GW peut se connecter avec les réseaux PSTN et réseaux IP grâce à l'IMS.

- **Entité HSS:** (Home Subscriber Server) : Le HSS est responsable d'à peu près les mêmes fonctionnalités que le HLR (base des profils des abonnés, avec leurs droits et leurs caractéristiques). Le HSS inclut en plus un lien possible avec le monde IMS, pour la gestion des services de voix enrichis.
- **MME:** (Mobility Management Entity) : Se compose des fonctions principales dans le plan de contrôle. Il sert à gérer des sessions : signalisation, mobilité, et négociation des qualités de service, à fournir des procédures de sécurité telles que : initiation, et négociation de chiffrement/protection d'intégrité, et à mettre à jour la position de l'UE, gestion de contrôle et d'authentification Sélection du S-GW et du P-GW.
- **Entité PCEF :** Le PCEF (Policy and Charging Enforcing Function), module fonctionnel logé dans la PDN Gateway, applique les règles fixées par le PCRF.
- **Entité PCRF :** Le PCRF réalise deux fonctions :
  - Elle fournit au PDN-GW les règles de taxation lorsqu'un default bearer ou un dedicated bearer est activé ou modifié pour l'usager. Ces règles de taxation permettent au PDN-GW de différencier les flux de données de service et de les taxer de façon appropriée.
  - Elle permet de demander au PDN GW d'établir, de modifier et de libérer des dedicated bearer sur la base de QoS souhaitée par l'usager.

Le PCRF dialogue alors avec le PDN-GW pour créer le dedicated bearer correspondant.

**Entité IMS :** L'IMS (IP Multimedia Subsystem), bien que ne faisant pas partie véritablement de la 4G, est un ensemble d'éléments permettant d'offrir des services multimédia sur les réseaux IP (et donc entre autre sur le réseau mobile). L'IMS permettra des services interpersonnels multimédia riches : voix sur IP, conférence vidéo, agenda enrichi, messagerie instantanée, sonnerie sur plusieurs terminaux, etc.

- **Bearer :** Le bearer est un circuit virtuel qui s'établit sur le plan utilisateur (user plane) entre l'UE et la PGW.

## **I.4.2 Couche Agrégation :**

La couche d'agrégation Carrier Ethernet est la fondation des réseaux NGN, parfois appelée Ethernet Transport.

Elle assure le transport Ethernet pour tous les types de services, de clients et de technologies d'accès, et elle détermine les vitesses de réseau de 1 Gbps à 100 Gbps. La conception de l'Ethernet porteur permet d'optimiser tous les services indépendamment, en prenant en charge plusieurs technologies de couche 2 et de couche 3 dans le transport Ethernet réseau. Ces technologies et/ou protocoles comprennent :

- Routage de couche 3 avec PIM-SSM
- VPN MPLS de couche 2/3 et VPN multicast (RFC 2547bis)
- H-VPLS
- EoMPLS (Pseudowires)
- IEEE 802.1q, 802.1ad, 802.1ah
- IPoDWDM

L'une des raisons pour lesquelles il est essentiel de prendre en charge plusieurs protocoles dans le réseau d'agrégation est que les différents clients, services et applications ont des exigences différentes qui ne peuvent pas être et une approche unique et universelle de la conception des réseaux. Une autre raison pour laquelle les multiples protocoles et les technologies doivent être soutenus, car les fournisseurs de services ont des approches uniques pour l'architecture et la conception des réseaux. La flexibilité de la conception de l'Ethernet à porteur IP NGN permet les fournisseurs de services à concevoir le réseau selon leurs propres directives de conception et leur propre architecture, pas ceux d'un vendeur particulier.

Tous les protocoles spécifiés précédemment peuvent être utilisés pour n'importe quel service, à l'exception des services résidentiels service de diffusion vidéo. En raison des exigences de qualité d'expérience critique (QoE) pour la vidéo.

La technologie de diffusion optimale est la multicast IP de couche 3 avec PIM-SSM sur MPLS avec Fast Re route (FRR). Cela permet d'obtenir une architecture hautement évolutive et fiable pour service de télédiffusion. De même, le service de vidéo résidentielle en gros devrait utiliser la couche 3 multicast sur un VPN MPLS (RFC 2547bis) pour assurer à la fois l'évolutivité et la séparation logique de d'autres réseaux de vente au détail et de clients.

Si les fournisseurs de services sont libres de choisir les protocoles de transport qui conviennent le mieux à leur réseau l'architecture et les applications, Cisco propose des protocoles recommandés

pour optimiser le service livraison (tableau 1). En général, le transport pseudo-filaire EoMPLS est recommandé pour de nombreux services qui nécessitent un transport Ethernet avec une qualité de service différenciée. Comme EoMPLS utilise le pseudo fil IETF, il est non seulement évolutif, mais il offre également des caractéristiques de qualité de service améliorées [3] [4].

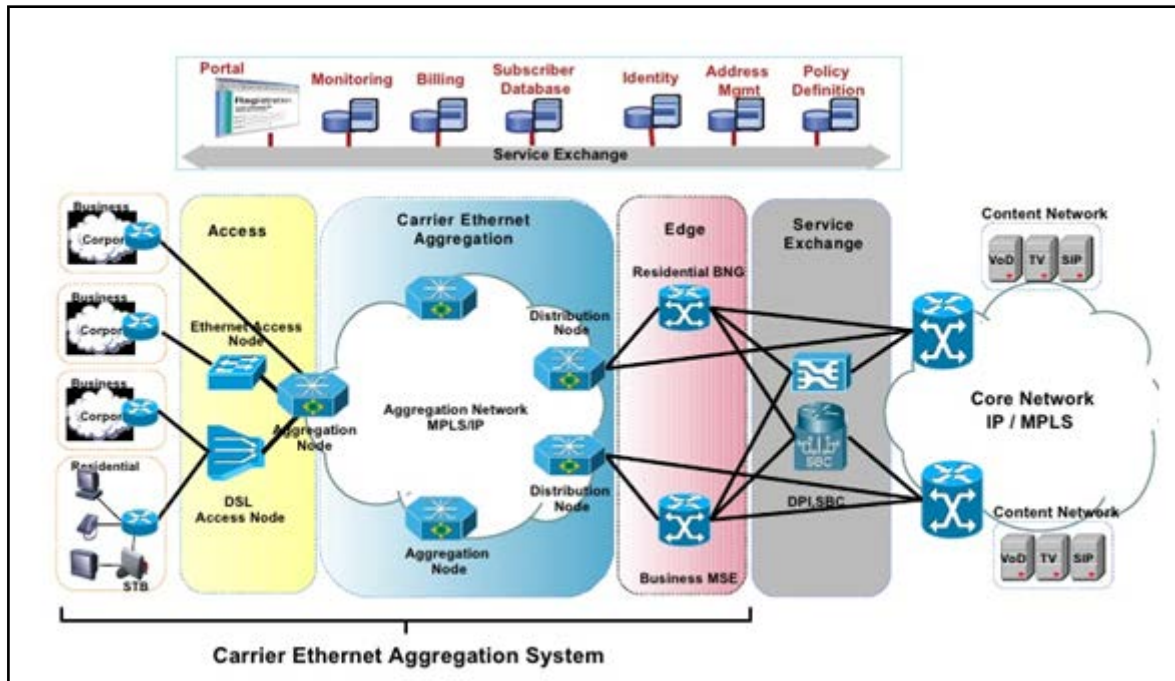


Figure I.10: Couche agrégation network IP/MPLS

Tableau I.1 : Les Protocoles recommandés pour différents services

Service	les protocoles de transport recommandés	fonction de transport
<b>Internet résidentiel à haut débit</b>	EoMPLS ou IEEE 802.1ad	Acheminement du trafic Internet du réseau d'accès vers le Routeur d'accès à distance à large bande pour AAA et service contrôle. Fournir un accès Internet de qualité, à plusieurs niveaux, basé sur des quotas et sur l'utilisation.
<b>VoIP résidentielle</b>	EoMPLS ou routage IP de couche 3 sur MPLS FRR	Connecter le trafic de signalisation au softswitc et le trafic RTP au Internet ou réseau IP central Fournir la QoS
<b>IPTV résidentielle</b>	Couche 3 PIM SSM sur MPLS FRR	Service de diffusion télévisuelle avec une extensibilité massive, rapide la reprise après les échecs, et une excellente qualité d'éducation
<b>VOD résidentielle</b>	Routage IP de couche 3 sur MPLS FRR	Service de vidéo à la demande avec une extensibilité massive, une la reprise après les échecs, et une excellente qualité d'éducation.
<b>ligne privée business ethernet (EPL)</b>	EoMPLS ou IEEE 802.1ad	Transport du circuit Ethernet à plein débit sans multiplexage statistique. Cela nécessite la quali de service.
<b>ligne privée virtuelle</b>	EoMPLS ou IEEE 802.1ad	Transport de la connexion virtuelle Ethernet av

<b>business ethernet (EVPL)</b>		CIR/EIR et le gain de multiplexage statistique.
<b>entreprise MPLS VPN</b>	MPLS ou IEEE 802.1ad	Transport de l'abonné Connexion virtuelle Ethernet à Routeur MSE qui est le fournisseur d'accès au VPN MPLS service. Le CIR/EIR garantit la largeur de bande
<b>Entreprise E-LAN</b>	H-VPLS ou IEEE 802.1ad	Service de réseau local virtuel multipoint pour les clients professionnels. Le service CIR/EIR garantit la largeur de bande
<b>transport mobile</b>	EoMPLS ou IEEE 802.1ad	Pseudo fils de liaison pour la 3G, le WiMAX et le Wi-Fi réseaux.
<b>Internet à haut débit résidentiel en gros</b>	EoMPLS ou IEEE 802.1ad	La liaison pseudo-filaire entre le réseau d'accès et le fournisseur de services de détail.
<b>IPTV et VoD en gros</b>	RFC 2547bis MPLS VPN avec Multicast	Réseau IP privé avec multidiffusion qui interconnecte le fournisseur de services de détail avec le réseau d'accès.
<b>les services de gros aux entreprises</b>	EoMPLS or IEEE 802.1ad	Assurer le transport entre l'entreprise cliente et détaillant fournisseur de services avec des garanties de largeur de bande EIR/CIR.

### I.4.3 Intelligent Service Edge :

C'est à la périphérie du service intelligent que de nombreux services de réseau sont terminés et gérés. Ils existe trois fonctions principales sont :

- Agrégation des services d'accès à distance à large bande
- Fournisseur multiservices de routage en périphérie
- Inspection approfondie des paquets (DPI)

Les points sont destinés à gérer les services de réseau et le prochain est fait à ces points :

Premièrement, la passerelle de réseau à large bande est chargée de gérer et de surveiller Internet haute vitesse et de fournir des services de gros aux fournisseurs de sous-services par l'intermédiaire des fonctions de la passerelle des services intelligents (SAI) des services Internet et VoIP.

Le trafic des abonnés est transporté sur le réseau d'accès et d'agrégation Ethernet et terminé sur le routeur d'accès à distance à large bande . Les fonctions fournies par la passerelle du réseau à large bande comprennent :

- Terminaison des services Internet résidentiels à haut débit
- Terminaison, routage ou tunnel de l'Internet à haut débit de gros en utilisant le VPN L2TP ou MPLS
- RADIUS, AAA, et contrôle dynamique des abonnés et des politiques pour les sessions PPPoE et IPoE.

Le trafic des entreprises est transporté à travers le réseau Ethernet des opérateurs jusqu'à l'extrémité multiservice où Les services VPN MPLS, les services Frame Relay existants et les services ATM sont supprimés.

Le deuxième est Multiservice Edge et reçoit des flux de trafic d'affaires où le routage IP virtuel exécute un relais de trame et ATM-à-MPLS

Troisièmement, La fonction d'inspection approfondie des paquets (DPI) met en œuvre la gestion du trafic de la couche application et le contrôle de la fourniture de services Internet de qualité supérieure. Elle effectue des tâches de la surveillance du flux , et fait également partie intégrante du cadre d'échange de services [3] [4].

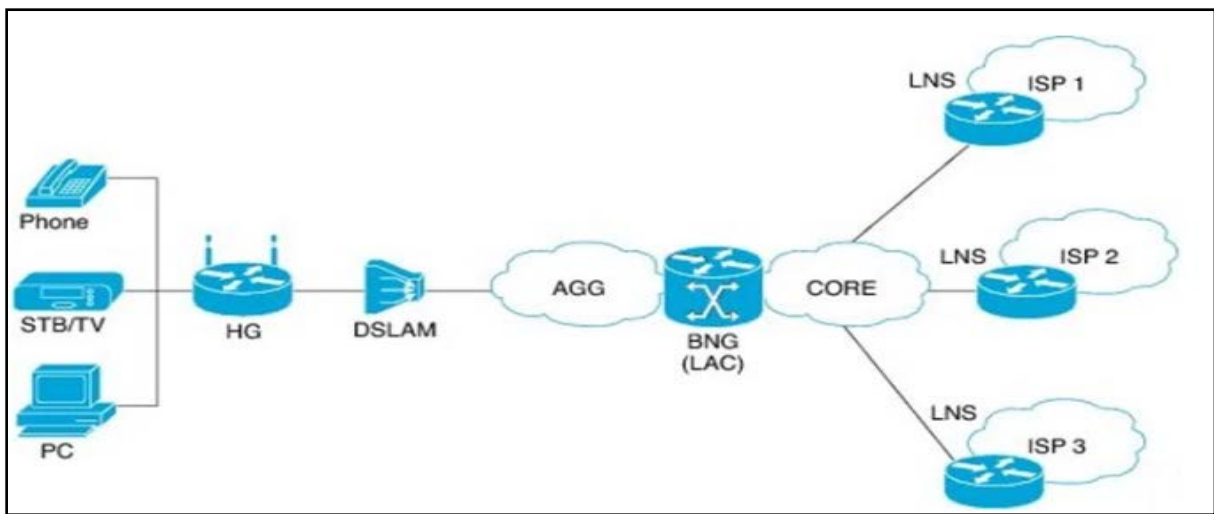


Figure I.11: Intelligent Service Edge

#### I.4.4 La couche Core IP/MPLS :

Le cœur IP/MPLS est le réseau de base qui interconnecte tous les réseaux d'agrégation. il est considéré le backbone chez un réseau opérateur.

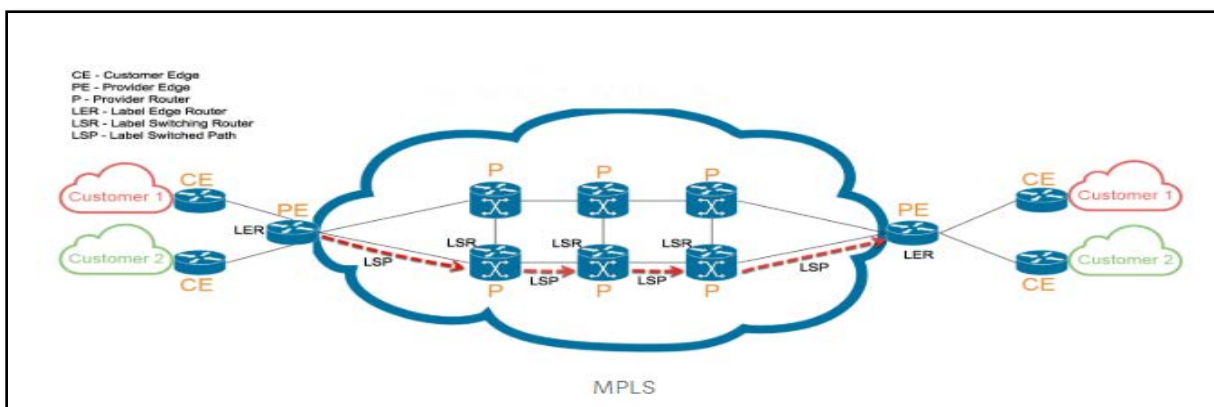


Figure I.13: Core IP/MPLS

**CE** : Customer Edge, ce sont les routeurs présent dans les réseaux du client. Ils sont interconnectés avec un ou plusieurs PE.

**P** : Provider Router, il s'agit d'un routeur de cœur de réseau. Terme utilisé lorsqu'on parle d'un réseau fournissant des services, en faisant abstraction des protocoles réseaux utilisés.

**PE** : Provider Edge Router, il s'agit d'un routeur situé à la périphérie du réseaux. Terme utilisé lorsqu'on parle d'un réseaux fournissant des services, en faisant abstraction des protocoles réseaux utilisés.

**LER** : Label Edge Router, routeur MPLS situé au extrémité du réseau IP/MPLS.

**LSR** : Label Switching Router, routeur MPLS situé dans le coeur du réseau MPLS.

**LSP** : Label Switched Path, chemin créé à travers le réseau entre deux machines [9].

### **I.4.5 Policy / service layer :**

Les services de réseau sont passés de Triple Play (Vidéo , Voix, Data) à un réseau multiservices via n'importe quel écran de distance et via n'importe quel Médias filaires ou sans fil ou n'importe quel service et écran sur les réseaux câblés et mobiles, ainsi que le soutien de la manipulation de plus d'un réseau multifournisseurs.

Dans ce cas, une méthode est nécessaire pour surveiller les abonnements des utilisateurs et est considéré comme le cadre d'échange de services est l'élément clé des réseaux Ethernet Cisco Carrier.

La SEF se compose de deux couches principales :

- Policy-Management Layer : les services sont mis en place selon les profils de l'abonné et les serveurs sont utilisées pour mettre en œuvre ces orientations.
- La couche Packet-Forwarding and Processing provient de Integrated Services Gateway (ISG) et de Service Control Engine (SCE)

Integrated Services Gateway (ISG) est une partie logicielle qui est placée dans les ordinateurs et les commutateurs pour permettre des services de gestion et de surveiller les abonnements des utilisateurs.

Service Control Engine (SCE) est un moteur DPI pour la configuration, le contrôle et la surveillance de service[3] [4].

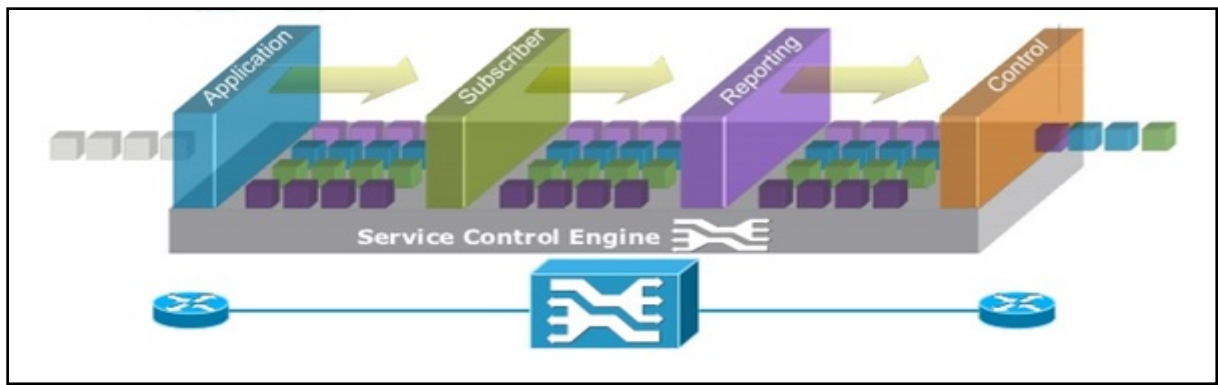


Figure I.13: Policy/ Service Layer

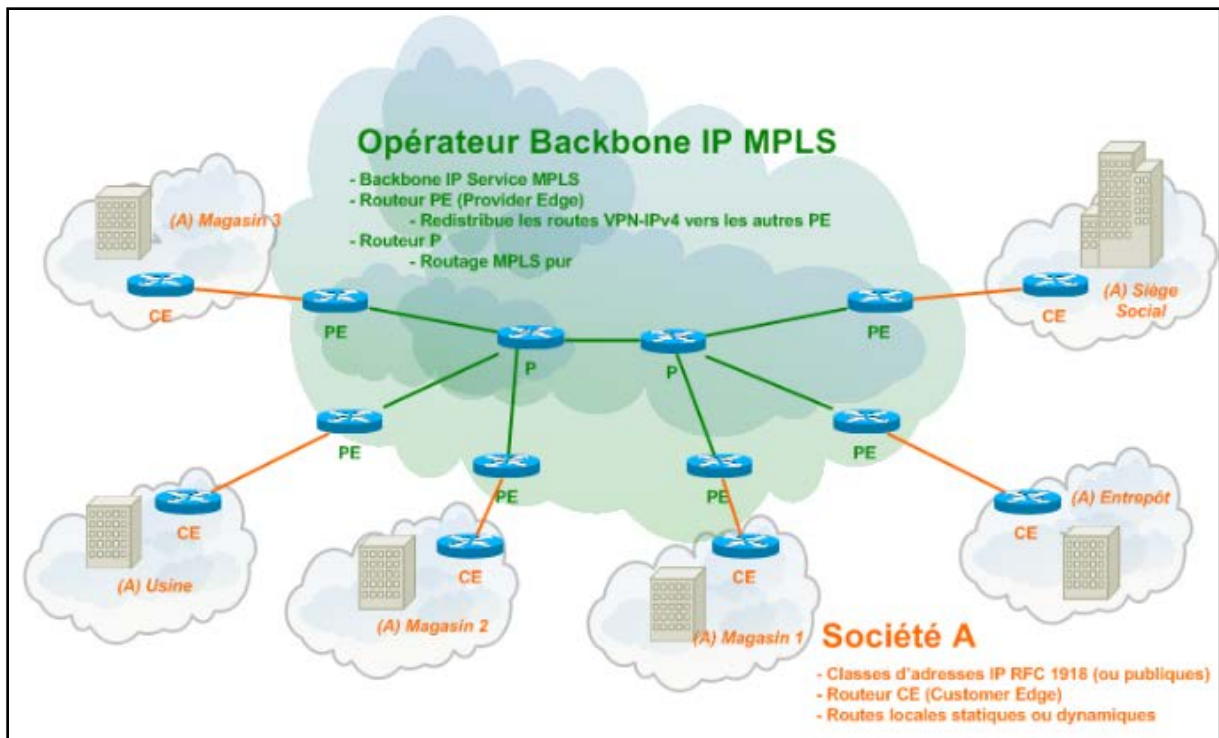
## I.5 Aperçu sur la technologie IP/MPLS:

IP/MPLS (IP multi-protocol label switching) est un support et une technologie d'entreprise qui permet une commutation très rapide des données. Généralement, avec les routeurs IP, les paquets doivent être examinés pour les adresses source et destination, afin que la fonction de contrôle du routeur puisse déterminer, via une table de routage, l'interface optimale pour envoyer les paquets à la destination. Malheureusement, cela prend du temps, mais les ingénieurs IP/MPLS ont trouvé une alternative, l'encapsulation du paquet IP dans un paquet avec une étiquette d'en-tête, d'où la commutation de l'étiquette de nom.

Cela signifie que le routeur ne transmet plus les paquets sur la base d'une recherche longue et dépendante du logiciel dans la table de routage, mais qu'il commute rapidement les paquets sur la base de l'étiquette. Cela offre d'énormes avantages en termes de performances et de flexibilité. La partie multiprotocole du nom provient du fait qu'en encapsulant les paquets avec une étiquette MPLS, tout peut être transporté sur le réseau MPLS, quel que soit le protocole sous-jacent.

MPLS possède également des caractéristiques très intéressantes telles que les VPN aux niveaux 2 et 3. L'intérêt de l'IP/MPLS est que les entreprises peuvent étendre un réseau local sur de grandes distances et connecter ainsi des bureaux distants comme s'ils étaient reliés entre eux. De même, elles peuvent prendre en charge les VPN de la couche 3 en connectant des bureaux distants, des tiers et des partenaires à l'aide du routage d'adresses, quel que soit le schéma d'adresse privé utilisé par chaque entité. Par exemple, un bureau pourrait utiliser l'espace d'adressage privé 172.16.10.x et un autre bureau distant pourrait se voir attribuer la même adresse, mais avec MPLS, ils pourraient tous deux communiquer sans avoir à ré-adresser leurs systèmes IP respectifs [10].





**Figure I.14: IP/MPLS**

L'opérateur fournit alors un routeur PE (Provider Edge) qui va permettre une connectivité au réseau public IPv4 pour transmettre les paquets d'un PE à un autre PE en passant par les routeurs du backbone opérateur P (Provider), qui ne connaissent pas les routes privées de la société A.

Pour pouvoir communiquer entre eux, les PE ont besoin de connaître les routes privées. Les routes privées IPv4 du CE apprises par le PE vont être transmises aux autres routeurs PE du VPN grâce à BGP et son extension multi protocole VPN-IPv4.

Ces routes, une fois apprises par BGP, peupleront les tables de transfert du routeur PE afin que celui-ci sache comment contacter un autre routeur PE du VPN.

**Remarque** : un VPN contient au moins deux routeurs PE. Il peut cependant en contenir plus que deux et ainsi permettre de créer un ou plusieurs VPN pour une même entité [11].

**VPN** : Un réseau privé virtuel (*Virtual Private Network*) est un tunnel sécurisé à l'intérieur d'un réseau (Internet notamment). Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente de celle de votre ordinateur [12].

La gestion des VPN dans le backbone est assurée par l'opérateur par le biais des PE.

**BGP** : ( Border Gateway Protocol )est le protocole de routage complexe qui est au coeur du fonctionnement d'Internet [13].

## I.6 Les Type de NGN :

Il existe trois types de réseau NGN : NGN Classe 4, NGN Classe 5 et NGN Multimédia. Les NGNs Classe 4 et Classe 5 sont des architectures de réseau offrant uniquement les services de téléphonie. Il s'agit donc de NGN téléphonie. Dans le réseau téléphonique commuté (RTC), un commutateur Classe 4 est un centre de transit. Un commutateur Classe 5 est un commutateur d'accès aussi appelé centre à autonomie d'acheminement. Le NGN Classe 4(respectivement NGN Classe 5) émule donc le réseau téléphonique au niveau transit(respectivement au niveau accès) en transportant la voix sur un mode paquet. Quant au NGN Multimédia, c'est une architecture offrant les services multimédia (messagerie vocale/vidéo, conférence audio/vidéo, tonalité ou sonnerie de retour (Ring-backbone) voix/vidéo) puisque l'utilisateur a un terminal IP multimédia. Cette solution est plus intéressante que les précédentes puisqu'elle permet à l'opérateur d'innover en termes de services par rapport à une solution NGN téléphonie qui se cantonne à offrir des services de téléphonie [14].

## I.7 Evolution du NGN téléphonie vers NGN multimédia (IMS) :

### I.7.1 NGN Téléphonie

❖ Services dans le RTC vs Services dans le NGN Téléphonie :

Dans le contexte du Réseau Téléphonique Commuté, le commutateur réalise deux fonctions essentielles :

- La commutation de la voix (Media)
- Le contrôle de l'appel (établissement /libération d'appel)

Les services à valeur ajoutées ont mis en œuvre par le réseau intelligent à travers les entités SCP (Service Control Point) / SRP (Specialized Resource Point).

Les services complémentaires sont mis en œuvre directement par le commutateur d'accès (Class 5 Switch) [14].

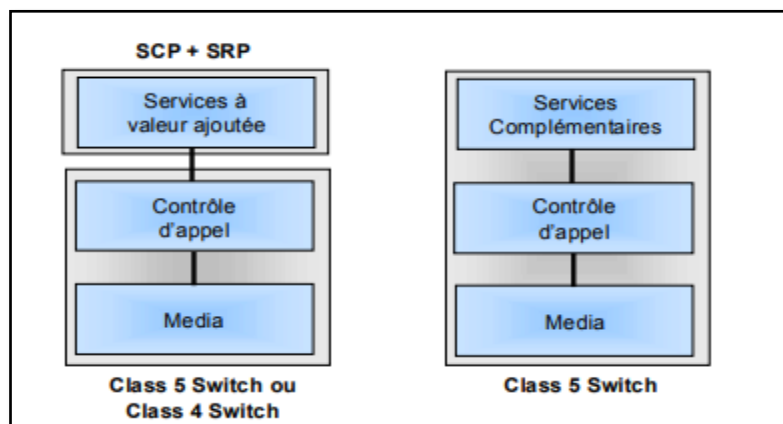
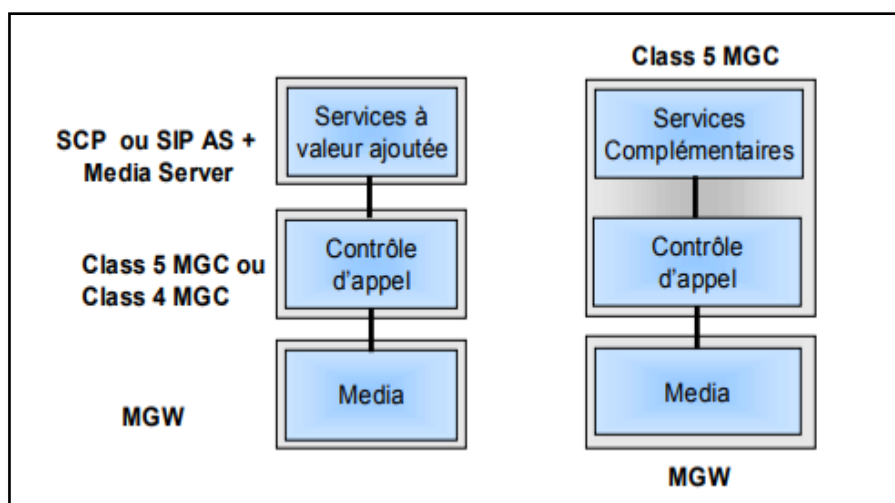


Figure I.15: Services dans le RTC

Dans le monde NGN, la commutation de la voix est réalisée par le MGW entre le réseau téléphonique commuté et le réseau de transport du NGN. Dans le réseau de transport, ce sont les commutateurs ATM / Routeurs IP qui assurent le transport de la voix paquetées jusqu'au MGW de sortie qui commute la parole reconvertie, sur un circuit de parole sortant. Le contrôle de l'appel (établissement/libération d'appel) est pris en charge par le MGC. Un MGC Class 4 émule le point sémaphore d'un Class 4 Switch . Un MGC Class 5 émule le point sémaphore d'un Class 5 Switch.

Les services à valeur ajoutée sont pris en charge par le SCP légataire du réseau intelligent ou par un serveur d'application SIP et par un serveur de media (appelé Multimedia Resource Function) qui fonctionne en voix sur IP (il émet des annonces vocales et collecte l'information de l'utilisateur sur des canaux RTP/UDP/IP) [14].

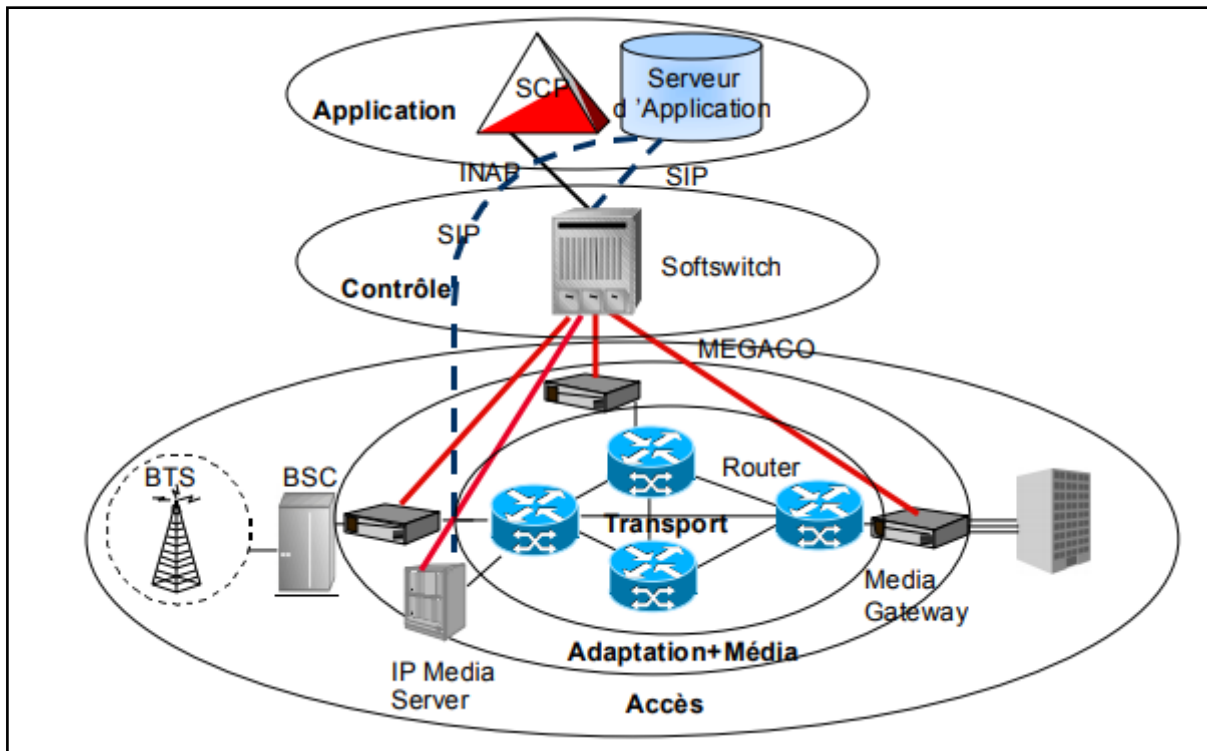


**Figure I.16: Services dans le NGN téléphonie**

#### ❖ Architecture NGN Téléphonie

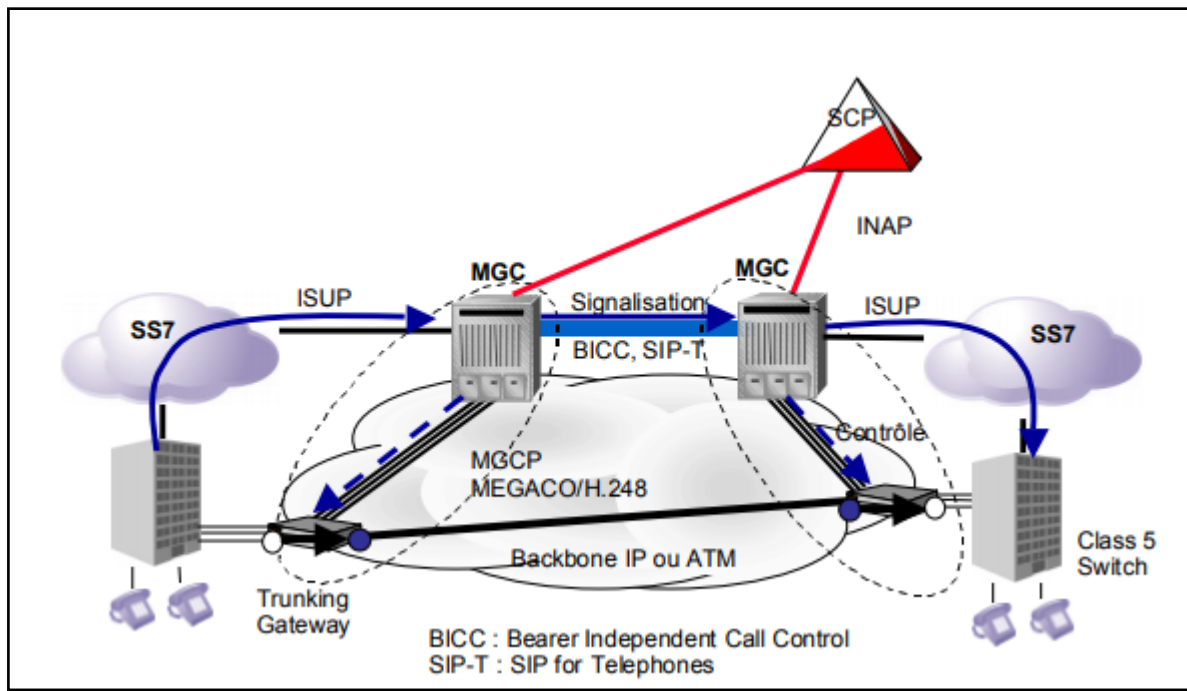
La figure I .17 montre un exemple d'architecture NGN Téléphonie. Les équipements existants (e.g., commutateur d'accès téléphonique ou BTS/BSC du réseau GSM) sont reliés à une couche de transport IP ou ATM par le biais de MGWs (couche d'adaptation). L'établissement des canaux de communication IP ou ATM entre les MGWs est la responsabilité du MGC appartenant à la couche contrôle.

Le MGC est un serveur d'appel qui contient l'intelligence liée au contrôle de l'appel et pour ce faire possède un modèle d'appel complet. Le MGC identifie les usagers, détermine le niveau de service pour chaque usager et l'acheminement de trafic. Par ailleurs, il fournit toutes les informations permettant la taxation des appels et la mesure des performances du réseau. Aussi, le MGC s'interface aux serveurs d'applications .Le MGC a différentes appellations :L'ITU-T (International Telecommunications Union -Telecommunications Sector) le nomme Media Gateway Controller (MGC), l'IETF (Internet Engineering Task Force) qui normalise les aspects relatifs à l'Internet a utilisé le terme Call Agent initialement et l'appelle désormais MGC. Le Soft switch Consortium considère le terme Softswitch. Enfin, dans les solutions des fournisseurs tels que Nortel et Ericsson, le MGC est appelé respectivement Call Server et Telephony Server.



**Figure I.17: Exemple d'architecture NGN téléphonie**

Dans l'architecture NGN Téléphonie, le protocole de contrôle tel que MGCP ou MEGACO ne fait que décrire les interactions entre le MGC et le MGW. Si un MGC doit contrôler un MGW qui est sous la responsabilité d'un autre MGC, il est nécessaire que les MGCs s'échangent de la signalisation. Deux protocoles de signalisation peuvent être utilisés : SIP-T (Session Initiation Protocol for Telephones) et BICC (Bearer Independent Call Control). SIP-T est une proposition de l'IETF a lorsque BICC est spécifié par l'ITU-T. La figure 18 montre l'interface de contrôle qui est mise en œuvre par le protocole MGCP ou MEGACO /H.248, et l'interface de signalisation réalisée par le protocole SIP-T ou BICC. Une fois la connexion établie, le MGW convertira les signaux audio transportés dans les circuits de parole (terminaison circuit) en paquets IP qui seront transportés dans le réseau IP (terminaison IP) ou en cellules ATM dans le cas d'un transport ATM [14].



**Figure I.18: Protocoles de contrôle (MGCP, MEGACO) versus protocoles de signalisation (SIP-T, BICC).**

## I.7.2 NGN Multimédia

Les besoins qui ont amené IMS sont :

- Mutualisation de la plateforme chez les opérateurs
- Accès au service à travers n'importe quel support
- Modification du business chez les opérateurs

NGN multimedia ou IMS (IP Multimedia Subsystem). Le Multimédia NGN permet d'offrir des services multimédia à des usagers disposant d'un accès large bande tel que xDSL, câble, WiFi / WiMax, EDGE/UMTS, etc.

L'IMS introduit une nouvelle entité fonctionnelle dans le réseau, appelée CSCF (Call State Control Function). Elle joue le rôle de Proxy Server SIP, et ses principales fonctions sont :

La localisation des usagers en traduisant l'adresse SIP de destination en une adresse IP

- Le routage des messages SIP pour l'établissement, la modification et la libération de sessions multimédias.
- Le maintien des informations d'état de la session afin de pouvoir invoquer les services souscrits par les usagers, afin de contrôler la session pendant sa durée de vie, et pour la facturation de la session[14].

Le domaine IMS doit inter fonctionner avec le RTCP/GSM afin de permettre aux utilisateurs IMS d'établir des appels avec le RTCP/GSM. L'architecture d'interfonctionnement présente un plan de contrôle (signalisation) et un plan d'utilisateur (transport). Dans le plan utilisateur, des entités

passerelles (IMS-MGW, IMS - Media Gateway Function) sont requises afin de convertir des flux RTP en flux TDM. Ces passerelles ne traitent que le média. Des entités sont responsables de créer, maintenir et libérer des connexions dans ces passerelles; il s'agit de contrôleurs de passerelles (MGCF, Media Gateway Control Function). Par ailleurs, ce même MGC termine la signalisation ISUP du côté RTC/GSM qu'il convertit en signalisation SIP qui est délivrée au domaine IMS [14].

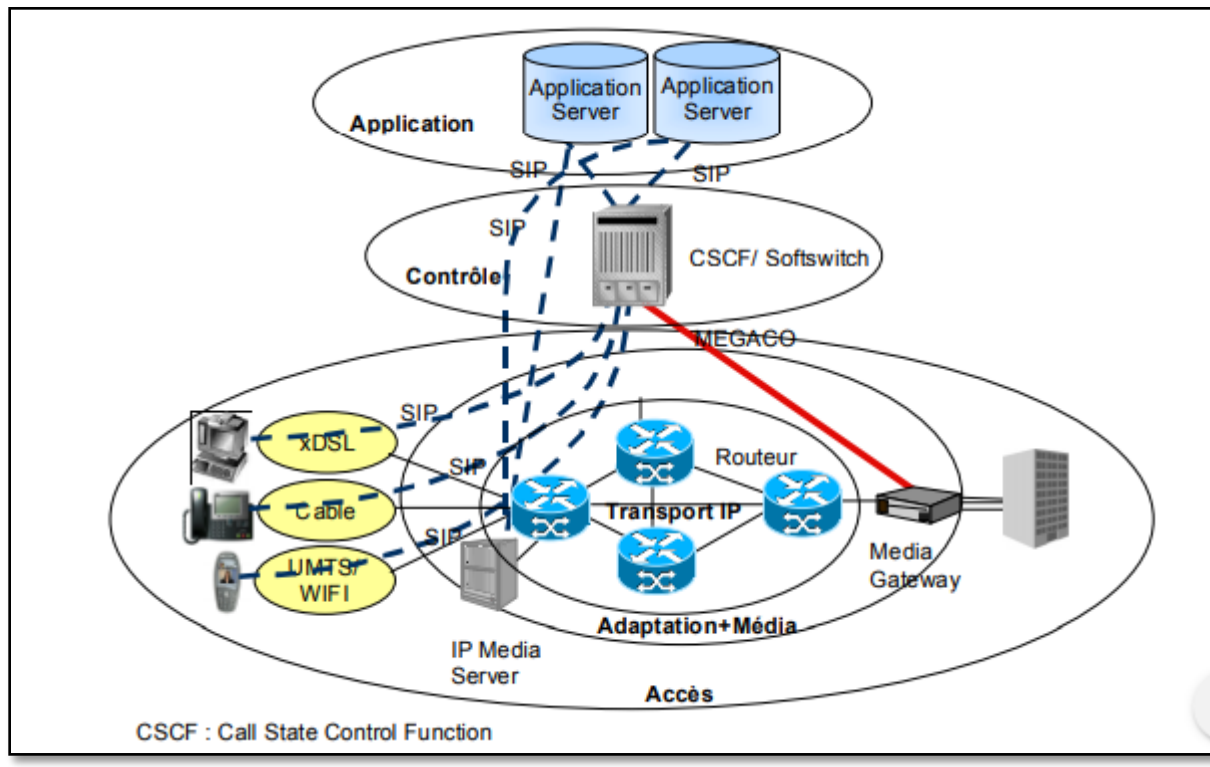


Figure I.19: Exemple d'architecture multimédia

### I.7.3 Convergence fixe-mobile:

La convergence fixe-mobile constitue un premier pas vers un concept de communication globale, dans laquelle seule prime le service au client au meilleur coût, les techniques mises en œuvre n'étant qu'accessoires. Dès lors, cette longue marche se décline en un grand nombre d'initiatives, avec comme points forts la généralisation de la mobilité, la notion de communication personnelle et la multiplicité des accès.

l'évolution vers une architecture tout-IP pour la prestation de ces services semble être la meilleure des options disponibles (aujourd'hui) mais introduit de nouvelles exigences pour les infrastructures de réseau. L'architecture IP Multimedia Subsystem (IMS), permettant de répondre à ces attentes, semble besoins mis en évidences. IMS devrait contribuer largement à la convergence fixe-mobile et l'utilisation de service en toute mobilité [15].

L'IMS est la prochaine grande étape dans la technologie des réseaux de télécommunication. Christophe : « Si les téléphonies fixe et mobile transitaient jusqu'à présent par deux réseaux technologiquement distincts, ce n'est plus le cas avec l'IMS : désormais, elles tourneront sous une seule et même technologie. »

Cette évolution offre de nombreuses possibilités, surtout pour les entreprises. Techniquement, il sera bien plus simple d'implémenter des services FMC (Fixed Mobile Convergence, convergence fixe/mobile). Christophe pense, par exemple, à un service où le numéro mobile servira de ligne virtuelle pour la centrale de l'entreprise. De plus, l'IMS n'offre pas que des possibilités sur le plan vocal. Christophe : « Il permettra aussi l'intégration d'autres applications, comme la vidéo et la messagerie instantanée. Grâce à l'IMS, nous pourrions offrir une alternative professionnelle à des acteurs phares tels que WhatsApp et Skype, qui proposent de l'audio, de la vidéo et d'autres médias via internet. Nous pourrions en outre garantir la qualité du service aux clients. » [16].

## **I.8 Conclusion:**

Globalement, l'évolution vers les NGN représente encore à ce jour un sujet relativement amont, notamment du point de vue des opérateurs (et dans une moindre mesure des purs fournisseurs de services). Il ressort de la présente étude que la conjoncture actuelle influe fortement sur les positions vis-à-vis des NGN : les acteurs sont confrontés à des problématiques de financement et de pérennité, ce qui les met dans un contexte peu favorable à des évolutions techniques et à l'apparition de nouveaux business models. Cela explique une certaine frilosité des acteurs interrogés vis-à-vis des solutions NGN (vision orientée vers une « transition douce » plutôt qu'une « révolution » des réseaux et services), mais qui pourrait se débloquer rapidement si le contexte économique évolue. A noter aussi que l'évolution vers les NGN ne revêt pas un caractère obligatoire, malgré l'opinion exprimée dans le sens contraire par certains acteurs très engagés dans les NGN.

# Chapitre II

## *IP Multimedia Subsystem*



## **II.1 Introduction :**

IMS est une architecture fonctionnelle des réseaux de nouvelle génération (NGN) permettant l'introduction progressive des applications voix et données multimédia dans les réseaux fixes et mobiles. Ces réseaux tout IP, et donc fondés sur les protocoles issues de l'internet, devrait permettre une convergence complète en fusionnant des domaines Internet de cellulaire, accessible qu'elle que soit la nature du réseau d'accès, tout en permettant la création de services innovants [17], tels les communications multimédias enrichies [18].

IMS est défini dans le 3<sup>rd</sup> Generation Partnership Project (3GPP) et a été introduit dans la version 5 d'UMTS (Mars 2003) [19].

Historiquement, IMS s'est d'abord focalisé sur le développement et le déploiement de nouveaux services dans les réseaux mobiles. Cette norme a par la suite été étendue par l'institut européen des normes de télécommunications (ETSI) dans le cadre de ses travaux sur les réseaux de prochaine génération (NGN). Par la suite, le TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking), organisme de standardisation de l'ETSI, a normalisé IMS en tant que sous système de réseaux NGN [20].

De manière générale, le 3GPP décrit le point de vue des opérateurs de téléphonie mobile (support de nouvelles applications) ; alors que TISPAN s'occupe de la convergence vers le domaine de l'internet. Il est également à noter que la plupart des protocoles IMS sont normalisés par l'Internet Engineering Task Force (IETF) [20].

## **II.2 OBJECTIF :**

L'intérêt principal de la promesse de convergence de l'IMS est avant tout au niveau de l'administration réseau. En effet un réseau tout IP est bien plus facile à administrer et cela se traduit par un gain de temps et d'argent.

De plus, le recours au protocole internet (IP) permet une interopérabilité entre les différents services même si les utilisateurs les utilisent depuis des réseaux différents. De même, IMS est une architecture horizontale ce qui permet une implémentation de service simplifié.

Ceci permet un renouveau des secteurs des télécommunications et de leurs acteurs. Outre le fait de replacer les opérateurs au centre du monde des services, il permettra aussi dans un futur proche, la commercialisation d'une multitude de nouveaux services qui sont autant de marchés à conquérir.

Enfin, via les protocoles SIP et IP, l'IMS permettra une réduction des coûts de déploiement des réseaux grâce à des plateformes standardisées et normalisées [21].

## **II.3 Définition de L'IMS :**

Le sous-système multimédia IP ou IMS est un cadre architectural basé sur des normes pour la fourniture de services de communication multimédia tels que la voix, la vidéo et la messagerie texte sur les réseaux IP.

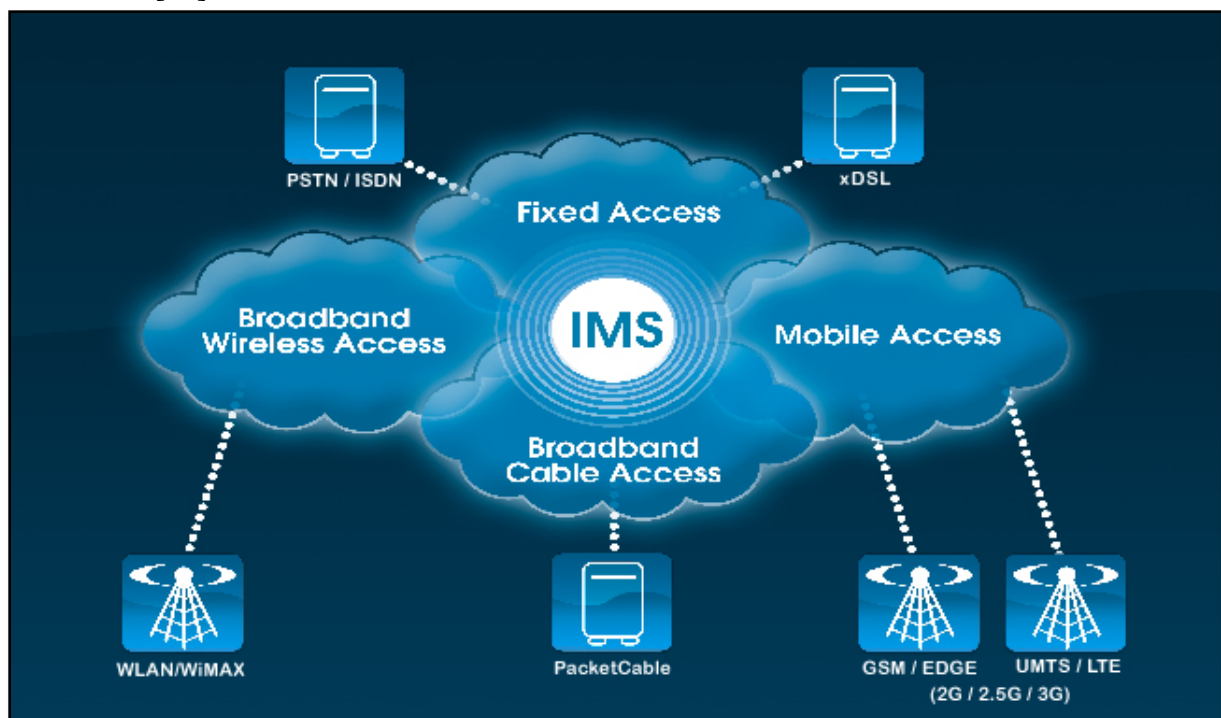
Il est défini comme la clé de la convergence vers le tout IP des réseaux et services télécoms [22]. IMS est une architecture de service standardisée définie par le 3GPP, l'ETSI et l'IETF basée sur le protocole SIP pour l'initialisation de sessions multimédias, utilisé pour la visioconférence ou la voix sur IP.

Ainsi, l'IMS et le protocole SIP peuvent permettre aux clients professionnels de connecter facilement leurs téléphones mobiles au système téléphonique PBX (autocommutateur privé) de leur entreprise.

L'IMS est adapté aussi bien aux réseaux filaires qu'aux réseaux mobiles. Ce qui fait de lui une architecture de référence pour la convergence fixe mobile [23].

Avec la technologie IMS, un seul terminal serait en mesure d'être utilisé pour accéder à internet, regarder la télévision et en même temps servir de téléphone en utilisant un seul protocole de communication. Tous les équipements de communication seront en mesure de traiter l'information qu'ils transmettent en utilisant un langage et un protocole uniformisé.

Un des groupes de travail de l'ETSI, TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) a normalisé IMS comme NGN. Si 3GPP est plus axé sur le point de vue opérateur mobile, TISPAN ajoute des spécifications plus du point de vue filaire, pour étendre l'intégration des réseaux fixes, afin de permettre la convergence fixe/mobile [24].

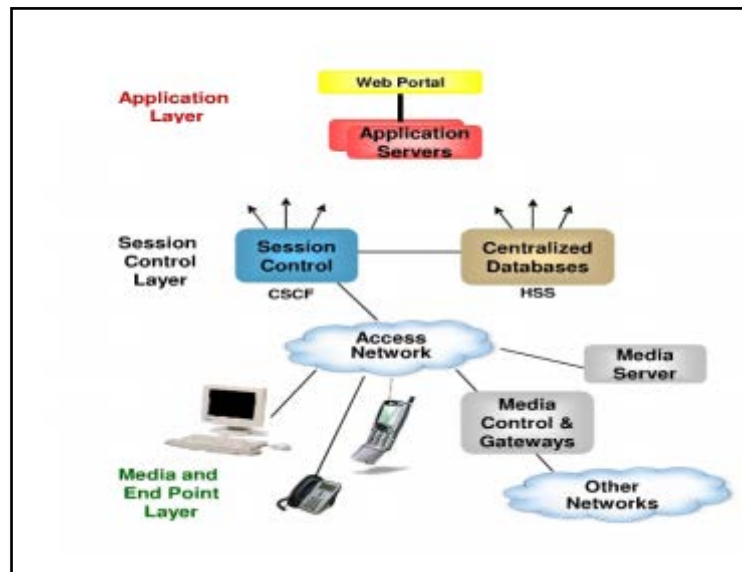


**Figure II.1: Vue simplifiée d'IMS par TISPAN**

IMS est :

- Infrastructure de services de contrôle à domicile.
- Une architecture de téléphonie Voip et de services multimédias.
- Définie avec les interfaces de normes ouvertes : 3GPP et 3GPP2.
- Basé sur les protocoles IETF ( SIP,Diameter,RTP...).

- Une solution pour la transparence des services.
- Capacité à interagir avec le RTPC et les services existants [25].



**Figure II.2 : IP MultiMedia Subsystem**

Les concepts de L'IMS tournent autour des principes suivants :

- **Indépendance de l'accès :**  
L'IMS fonctionne avec tous les types de réseaux (fixe ou mobile), incluant des fonctions de commutation de paquets, comme le GPRS, l'UMTS, les réseaux sans fil WiMAX, LTE, les réseaux fixes xDSL, en câble coaxial ou en fibres optiques... Les systèmes plus anciens de commutation de circuits (POTS, GSM) sont supportés grâce à des passerelles. Des interfaces ouvertes entre les couches de contrôle et de services permettent de multiplexer les appels et sessions venant de différents réseaux d'accès.
- **Des architectures de réseaux différentes:**  
l'IMS permet aux opérateurs et aux fournisseurs de services d'utiliser les architectures des réseaux subjacents.
- **Terminaux et mobilité des utilisateurs :**  
Le réseau mobile fournit la mobilité des terminaux (handhover, roaming) alors que la mobilité de l'utilisateur (utilisation de réseaux différents) est fournie par l'IMS et protocole SIP.
- **Services basés sur des protocoles IP variés :**  
IMS facilite l'offre de presque tous les services basés sur IP. Parmi ceux-ci : la voix sur IP (VoIP), la voix sur réseau mobile LTE (VoLTE); le Push to talk sur téléphones cellulaires les jeux multi-joueurs, la vidéoconférence, la messagerie instantanée, les services communautaires, les informations de présence et partage de contenus [26].

## II.4 Standardisation de L'IMS :

La standardisation de l'IMS est passée par des étapes.

L'IMS a été standardisé par l'organisme 3GPP dans la Release 5 de l'UMTS (Universal Mobile Télécommunication Service), et ensuite développé dans les versions suivantes.

TISPAN est un comité technique de normalisation de l'ETSI (European Telecommunications Standards Institute) qui a été mis en place en septembre 2003 par le biais de la fusion de deux autres groupes préalablement existants :

- SPAN (Services and Protocols for Advanced Networks).
- TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) : créé en 1997 comme un projet de l'ETSI projet pour étudier la voix sur IP (VoIP) ensuite étendu à l'étude de tous les services de télécommunication sur IP.

L'objectif de TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) est de produire des spécifications pour la distribution des services de téléphonie, de voix sur IP et plus largement des services multimédia dans le contexte de l'émergence d'une nouvelle génération de réseau (NGN, Next Generation Network) basée sur le protocole IP [27].

### II.4.1 Fonctionnement du comité TISPAN :

Le comité de normalisation TISPAN est organisé en groupes de travail et avec un plan prévisionnel de développement comportant plusieurs étapes de publication des spécifications. Ces applications sont appelées « release » [27].

#### II.4.1.1 La première publication « Release 1 » :

Fournit un schéma d'ensemble du système défini par TISPAN sous le nom de « Next Generation Network » (NGN). En particulier, le document TS 180 001 explique que l'objectif principal de TISPAN NGN est d'élaborer un système succédant à l'ancien réseau commuté de téléphonie (RTC/RNIS ; l'abréviation anglaise PSTN/ISDN sera quelque fois utilisée dans la suite de ce document) en permettant son remplacement en totalité ou partiellement. Ce document stipule :

- Nouveau système utilisera l'architecture appelée IMS (IP Multimedia Subsystem) définie par le groupe 3GPP.
- l'objectif de distribuer des services multimédias sur les accès fixes à large bande, comme par exemple l'ADSL.

Par ailleurs, le choix de l'architecture IMS définie par le groupe 3GPP permet également de réaliser un progrès significatif dans la voie de la convergence des réseaux pour l'accès fixe et ceux de l'accès Mobile (FMC) [27].

#### II.4.1.2 La seconde publication « Release 2 » :

Outre l'évolution et l'enrichissement des fonctionnalités déjà définies en release 1, cette release va vers la distribution des services vidéo et audio étendus à la notion d'IPTV. Cette notion d'IPTV est au monde de la diffusion des services de télévision ce que la voix sur IP fut pour le monde de

la téléphonie commutée. En effet, le déploiement des services de télévision sur des réseaux en mode paquets IP ouvre de nouvelles perspectives de marché et d'exploitation avec comme pour la voix sur IP deux possibilités :

- l'une dans le domaine de l'Internet libre et sans qualités de service
- l'autre dans le domaine des réseaux gérés par opérateurs garantissant un niveau de qualité de service.

La notion d'IPTV sera limitée dans trois types de services :

- le service dit « broadcast » permettant à l'utilisateur de recevoir des émissions en diffusion sans pouvoir agir sur la linéarité du déroulement de cette diffusion.
- le service dit « VoD » proposant de choisir un contenu quelconque dans une bibliothèque sans contrainte horaire.
- le service dit NPVR qui n'est autre qu'une fonction d'enregistrement et de restitution (magnétoscope) agissant dans le réseau opérateur au lieu d'être dans le domaine physique de l'utilisateur.

En plus, la release 2 introduira également la notion de « réseau domestique » [27].

## **II.5 Architecture de L'IMS :**

L'IMS a une architecture centralisée et divisée en plusieurs couches. Avant de pouvoir accéder aux plateformes de services, l'utilisateur doit s'authentifier auprès de l'opérateur. Pour cela le HSS (Home Subscriber Server) assure les fonctions d'authentification, de localisation, de proxy SIP... Le CSCF (Call Session Control Function) contrôle l'ouverture des sessions SIP et l'établissement des appels. On y trouve aussi les MGW (Media Gateway) et le MGCF (Media Gateway Control Function) qui vont permettre de s'interconnecter avec des réseaux RTC ainsi que le MRFC (Multimedia Resource Function Controller) qui contrôle les ressources utilisées par le client [23].

Comme on peut le voir sur le schéma ci-dessus, l'architecture IMS est découpée en quatre couches fonctionnelles avec des interfaces normalisées pour favoriser l'évolutivité, la flexibilité et l'extensibilité.

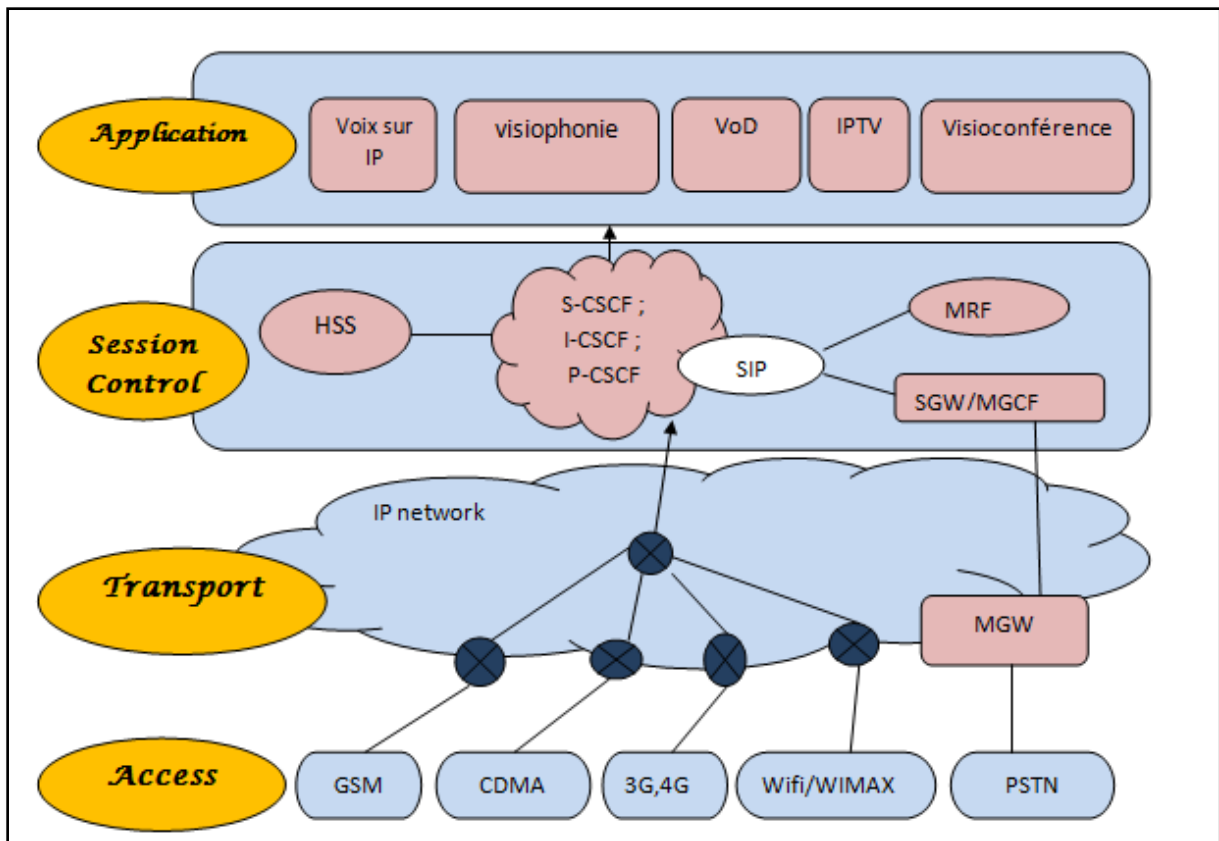


Figure II.3 : Architecture de l'IMS

### II.5.1 La couche " Access"(physique) :

La couche physique est une couche d'accès à l'architecture IMS. Elle définit la manière dont l'utilisateur se connecte au réseau. IMS permet un large choix de terminaux aux utilisateurs. En effet, tous les systèmes comme les ordinateurs, les téléphones mobiles, les téléphones fixes numériques, sont capables de se connecter à l'architecture IMS via le réseau [24]. Les téléphones traditionnels analogiques pourraient également se connecter à l'architecture IMS par le biais de passerelles, pour ainsi obtenir une adresse IP, condition nécessaire à une connexion au réseau cœur IMS. En regroupant différents types de réseaux d'accès au sein de cette couche, IMS offre un niveau d'abstraction à la manière dont l'utilisateur se connecte au réseau. Cette vision est à l'origine de l'idée de convergence des réseaux vers un réseau unique, prônée par l'IMS. Autrement dit, IMS est indépendant du réseau d'accès, qui n'est qu'un élément assurant la connectivité de l'utilisateur au réseau cœur.

La couche Accès peut représenter tout accès haut débit tel que : UTRAN (UMTS Terrestrial Radio Access Network), xDSL, réseau câble, WiMAX, CDMA, GSM, WiFi, etc... permet l'interopérabilité entre les différents médias d'accès et l'architecture IMS.

### II.5.2 La couche "Transport" :

La couche de transport est une couche générique IP. Elle est formée d'un maillage de commutateurs et de routeurs qui assurent, dans le réseau IP, le routage des données multimédias.

Cette couche permet la connectivité de bout en bout entre les différents interlocuteurs. Alors que la couche d'accès se contente de connecter un utilisateur au réseau IMS, la couche transport se charge de l'acheminement des données de l'utilisateur jusqu'à son (ou ses) correspondant(s). Cela comprend le transport de l'information par les routeurs et le choix de la route empruntée dans le réseau. C'est le réseau IP qui est utilisé dans cette couche. Un des principaux enjeux au niveau de cette couche est de réaliser la convergence entre réseau à routage par paquet et réseaux à routage par circuit ; autrement dit, entre le réseau téléphonique commuté et le réseau utilisant TCP/IP. On pense ici aux téléphones traditionnels analogiques. C'est à ce niveau donc, qu'interviennent les passerelles PSTN (Public Switched Telephone Network) [24].

### II.5.3 La couche "Session control" :

La couche de contrôle, souvent appelée noyau IMS, elle assure la gestion et le contrôle du réseau. Elle est en charge de tous les messages de signalisation dans le réseau, permettant d'ouvrir, de maintenir, de modifier et de terminer une session entre des utilisateurs. C'est la partie intelligente du modèle, qui offre toutes les fonctionnalités de gestion des utilisateurs et constitue la véritable base de l'IMS [28].

La couche de contrôle est constituée de différents blocs, qui sont les suivantes :

#### II.5.3.1 Bloc de contrôle des sessions :

Le contrôle d'appel initié par un terminal IMS doit être pris en charge dans le réseau nominal (réseau auquel l'utilisateur a souscrit à ses services IMS) car l'utilisateur correspondant peut souscrire à un grand nombre de services et certains d'entre eux peuvent ne pas être disponibles ou peuvent fonctionner différemment dans un réseau visité, notamment suite à des problèmes d'interaction de service. Cela a induit la définition d'entités suivantes [28].

**CSCF :** les serveurs CSCF (Call Session Control Function) établissent, supervisent et relâchent les sessions multimédias, qui utilisent le protocole de signalisation SIP pour communiquer. [24] Ils sont les organes de traitement des références dans l'architecture IMS et réalisent les fonctions permettant d'orienter et de contrôler une session. Concrètement, lorsqu'un utilisateur se connecte, il peut accéder à un réseau qui n'est pas celui de l'opérateur chez qui il a souscrit un service. Il faut donc que l'utilisateur emprunte le réseau pour assurer sa connectivité, tout en cherchant à se relier à des entités appartenant à son opérateur, pour avoir accès aux services de son contrat. Ils gèrent également les services utilisateurs [24].

la fonction CSCF peut jouer trois rôles distincts : Servir-CSCF (S-CSCF), Interroger-CSCF (I-CSCF), ou Proxy-CSCF (P-CSCF).

- *P-CSCF* : Le Proxy-CSCF (P-CSCF) est toujours le premier point de contact entre un terminal et le réseau IMS [24].  
Ses missions consistent notamment à contrôler l'accès et à établir une connexion sécurisée avec le terminal. Son adresse est découverte par l'utilisateur lors d'une phase de "CSCF discovery". Il agit comme intermédiaire entre l'abonné et l'I-CSCF.  
Le P-CSCF se comporte comme un Proxy Server SIP lorsqu'il relaye les messages SIP vers le destinataire approprié et comme un User Agent SIP lorsqu'il termine l'appel [28].

- *S-CSCF* : Le Serving-CSCF (S-CSCF) nœud central au niveau signalisation, il permet d'effectuer le contrôle de session et peut récupérer ou mettre à jour les profils utilisateurs en communiquant avec le HSS via DIAMETER. Il invoque les serveurs d'applications liées aux services demandés. L'association utilisateurs S-CSCF est stockée dans le HSS [29].

Dans un réseau d'opérateur, différents SCSCF peuvent présenter des fonctionnalités différentes.

- *I-CSCF* : L'Interrogating-CSCF (I-CSCF) : fournit une passerelle vers d'autres domaines IMS. Il est essentiellement utilisé pour cacher la topologie ou si plusieurs S-CSCF sont situés dans le même domaine [29].
  - L'I-CSCF est localisé dans le home network.
  - Fait une première autorisation pour l'accès au réseau IMS.
  - 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 (Protocole Diameter sur l'interface I-CSCF – HSS).
  - Peut inclure une fonctionnalité de masquage de l'architecture du réseau de l'opérateur par rapport au réseau visité [30].

### La fonction de contrôle des sessions d'appel (CSCF) :

Proxy SIP utilisé pour gérer les sessions SIP

- Coordonner avec d'autres éléments du réseau.
- Contrôle de session, contrôle des fonctionnalités, allocation des ressources,.....

#### • Trois saveurs de CSCFs

- service CSCF(S-CSCF) - Entité de contrôle de session pour les dispositifs d'extrémité.
- CSCF d'interrogation (I-CSCF) - Point d'entrée vers l'IMS à partir d'autres réseaux.
- Proxy CSCF (P-CSCF) - Point d'entrée dans l'IMS pour les appareils.

#### • Fonctionnellement, les CSCF suivent les paradigmes de l'Internet

- P-CSCF → I-CSCF → S-CSCF.
- Entités sans état à la périphérie du réseau, les entités étatiques au cœur.
- Un traitement simple à la périphérie, un traitement complexe au cœur.
- Sécurité.

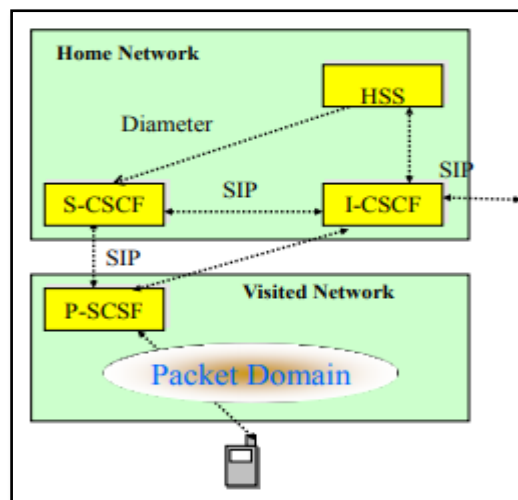


Figure II.4 : Fonctionnellement, les CSCF suivent les paradigmes de l'Internet



### II.5.3.2 Bloc des bases de données :

Le bloc des bases de données constitue d'entité suivante :

**HSS** : Un HSS (Home Subscriber Server) : base de données principale qui conserve toutes les informations du profil de l'utilisateur. Cet élément contient les données d'authentification des utilisateurs et donne des autorisations d'accès aux services en fonction des droits de l'utilisateur. Il fournit aussi des informations concernant l'emplacement d'un utilisateur [29].

Elle contient aussi toutes les informations nécessaires à un utilisateur pour ouvrir une session multimédia :

- des informations sur la localisation de l'utilisateur.
- le profil de l'utilisateur c'est à dire l'ensemble des services auxquels l'utilisateur est abonné.
- L'adresse du S-CSCF alloué à l'utilisateur.
- Des informations de sécurités [24].

### II.5.3.3 Bloc de l'interconnexion avec les autres réseaux :

L'interconnexion entre le domaine IMS et les autres réseaux est assuré a travers les entités suivants:

**Le BGCF**: Break Out Gateway Control Function : il est utilisé pour passer d'un réseau IMS à un réseau de commutation de circuit [29].

- L'entité BGCF détermine le saut suivant pour l'acheminement du message SIP.
- Elle doit choisir l'entité MGCF responsable de l'interfonctionnement avec les réseaux PSTN ou PLMN.
- Si l'entité d'interconnexion est située dans un réseau tiers, elle transmet le message SIP à une autre entité BGCF située dans ce réseau tiers.
- Un BGCF est utilisé pour les appels de l'IMS vers un téléphone dans un circuit Réseau commuté, tel que le PSTN ou le PLMN.
- Le BGCF transmet la signalisation au réseau PSTN/PLMN sélectionné.
- Si la rupture se produit dans le même réseau que le BGCF, ce dernier sélectionne un MGCF (Media Gateway Control Function) qui sera responsable de l'interfonctionnement avec le PSTN , et transmet la signalisation au MGCF. Sinon, il transmet la signalisation au BCGF d'un autre réseau d'opérateurs.
- Le MGCF reçoit alors la signalisation SIP du BGCF et gère l'interfonctionnement avec le réseau PSTN [28].

Pas de normes pour les critères que BGCF utilise pour la sélection, quelques facteurs possibles :

- Localisation actuelle de l'UE appelante
- Localisation de l'adresse du PSTN
- Politiques locales et accords commerciaux entre le réseau de pairs
- Minimiser la distance de parcours

- La voie la moins coûteuse

### **Le MGCF :**(Media Gateway Controller Function)

Contrôle une MGW (Media Gateway) permettant la conversion de flux multimédia entre un réseau IP et d'autres réseaux.

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. Il communique avec l'I-CSCF et le BGCF (SIP). Il contrôle les ressources du MGW avec une interface H.248 [24].

### **MGW :**

L'entité MGW effectue la conversion de protocoles relatifs aux flux Multimédias entre les deux terminaisons. Elle contient les traitements effectués sur les flux

Médias, comme le transcodage (modification du type de codec entre les deux terminaisons), L'annulation d'écho, l'émission des tonalités et des annonces [28].

### **II.5.3.4 Bloc de traitement du média :**

**MRF :** L'entité MRF (Multimedia Resource Function) fournit des fonctions liées aux médias tels que la diffusion de sons et d'annonces numériques, permet d'établir un pont de conférence entre les utilisateurs d'un réseau IMS. Son rôle est de gérer la signalisation vers tous les utilisateurs d'une conférence, en offrant des facilités d'exploitation, comme la sélection des types de flux. Il est aussi utilisé pour la lecture d'annonces (audio/ vidéo), conférence multimédia (par exemple le mixage de flux audio), conversion texte-parole (TTS) et reconnaissance vocale, transcodage en temps réel de données multimédias (c-à-d conversion entre différents codecs).

Le MRF comporte deux nœuds: le contrôleur et le processeur. Le contrôleur est situé dans la couche "Session Control" comme un agent utilisateur SIP. Le processeur est quand à lui situé dans la couche "Access" et fournit des services, telle que la compression de la voix (pour la conférence) et la vidéoconférence [31].

- MRFC (Multimedia Resource Function Controller): pour la partie signalisation, et plus précisément la négociation des paramètres sollicités par chaque utilisateur pour la mise en oeuvre de la conférence [28].
- MRFP (Multimedia Resource Function Processor) : pour la partie traitement des flux de données, c'est-à-dire l'application des demandes formulées par l'utilisateur dans les flux [28].

### **II.5.4 La couche "Application" :**

La couche application composée de serveurs d'application (AS) hébergeant les services gérés par l'infrastructure IMS, et d'un HSS recensant les utilisateurs IMS [29].

Elle consiste en la fourniture des services, qu'ils soient audio, vidéo ou textuels. Cette couche implémente tous les services que l'on peut proposer aux utilisateurs. Elle est la partie la plus ouverte du modèle, puisque le réseau IMS ne spécifie pas les services eux-mêmes, mais offre une plate-forme de déploiement unifiée, simple, rapide, productive et sécurisée pour la mise en place de nouveaux services. Tout service est exécuté par un serveur applicatif, en liaison avec les équipements de la couche de session par l'intermédiaire des protocoles SIP et Diameter, assurant ainsi la sécurité des utilisations. A noter qu'un serveur peut exécuter différents services comme de la téléphonie et un service de messagerie. L'avantage de cette flexibilité est de réduire la charge de travail au niveau de la couche de contrôle [ 28].

#### **II.5.4.1 Les serveurs d'applications :**

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 joue l'intermédiaire entre l'utilisateur et les services.

On distingue trois grandes familles de serveurs d'applications, qui sont :

- 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.

- IM-SSF (IP Multimedia-Service Switching Function): 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.

- 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 [28].

## **II.6 Les protocoles utilisés dans L'IMS et principes de fonctionnement:**

Les protocoles utilisés dans un réseau IMS peuvent remplir trois fonctions bien spécifiques à savoir l'authentification (Diameter), le transport des flux multimédia (RTP ou RTCP) et le transport de la signalisation (SIP). Dans cette section nous allons voir les protocoles SIP et Diameter.

### **II.6.1 Protocole SIP :**

#### **II.6.1.1 Description du protocole SIP**

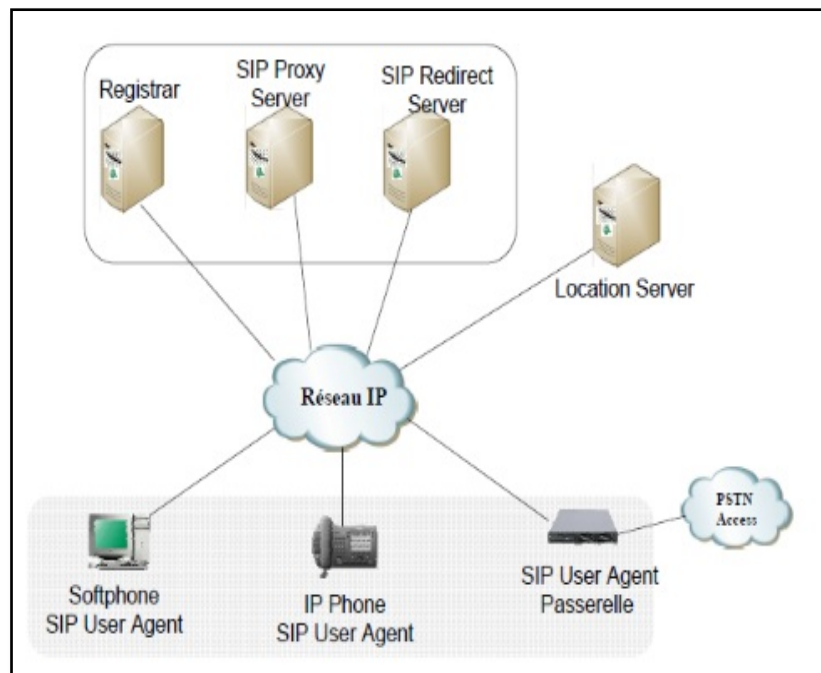
Le protocole SIP (Session Initiation Protocol) est un protocole de signalisation normalisé et standardisé par l'IETF ('Internet Engineering Task Force) (décrit par le RFC 3261 qui rend obsolète le RFC 2543, et complété par le RFC 3265), permettant l'établissement, la libération et la modification de sessions multimédias.

SIP (Session Initiation Protocol) est le protocole fédérateur de l'architecture IMS. Il est en quelque sorte la glue qui permet aux différents composants de communiquer entre eux de manière homogène. Son choix, par rapport à tout autre protocole de n'est pas anodin puisqu'il pérennise SIP au détriment de H.323, jugé trop lourd et trop coûteux. Il marque ainsi la confiance des industriels et du monde de la recherche dans le protocole SIP. Au niveau d'IMS, SIP est utilisé par les équipements du réseau IMS pour le contrôle de l'appel (établissement, modification, fin) lors de toute session multimédia. SIP sait gérer des appels multidestinataires, par groupe ou automatique [24].

- SIP est un protocole client /serveur.
- Tout opérateur SIP se compose une série de message requête/réponse.
- SIP est un protocole TCP/IP de couche application.
- SIP fonctionne bien avec IPv4 qu'avec IPv6.
- SIP n'est pas un système de communication intégré verticalement, c'est un composant qui est utilisé avec d'autres protocoles de l'IETF.

### II.6.1.2 Architecture de protocole SIP :

L'architecture SIP basé sur des relations client /serveur.



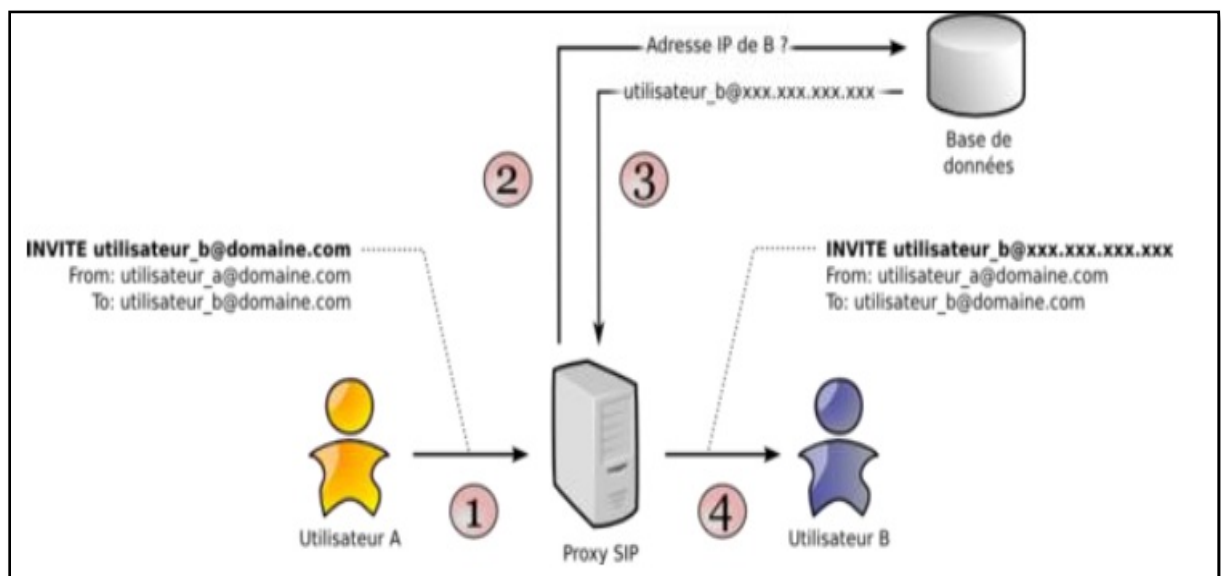
**Figure II.5 : Architecture de SIP**

#### ❖ Rôle des composants d'architecture :

On trouve deux types de composant :

- Les agents utilisateurs (UAC, UAS) .
- Réseau de serveurs (Proxy, Registrar) .

- **User agent** : sont les agents que l'on retrouve dans les téléphones SIP, les soft phones (logiciels de téléphonie sur IP) des ordinateurs et PDA ou les passerelles SIP et aussi caractérisé les points d'extrémités de la communication. Dans l'UA on a :
  - ✚ **UAC (User Agent Client)** : Un Agent Utilisateur Client est tout élément de réseau qui envoie une requête SIP et reçoit des réponses SIP. Les clients peuvent ou non interagir directement avec un utilisateur humain [32]. UAC représente l'agent de la partie appelante.
  - ✚ **UAS (User Agent Server)** : est une entité logique qui génère une réponse à une requête SIP. La réponse accepte, rejette, ou redirige la requête [32] représente l'agent de la partie appelée.
  - ✚ **Proxy server** : Entité intermédiaire entre deux User Agents serveur et client qui ne connaissent pas leurs emplacements respectifs (adresse IP)[33]. En effet, l'association URI-Adresse IP a été stockée préalablement dans une base de données par un Registrer. Le Proxy peut donc interroger cette base de données pour diriger les messages vers le destinataire.
- La Figure II.6 montre les étapes de l'interrogation du proxy la base de données.



**Figure II.6 : Principe de Protocole SIP**

- 1- envoi d'une requête INVITE au proxy.
- 2- Le Proxy interroge la base de donnée.
- 3- la base de donnée renvoie l'adresse IP du destinataire.
- 4- le proxy relaie le message au destinataire

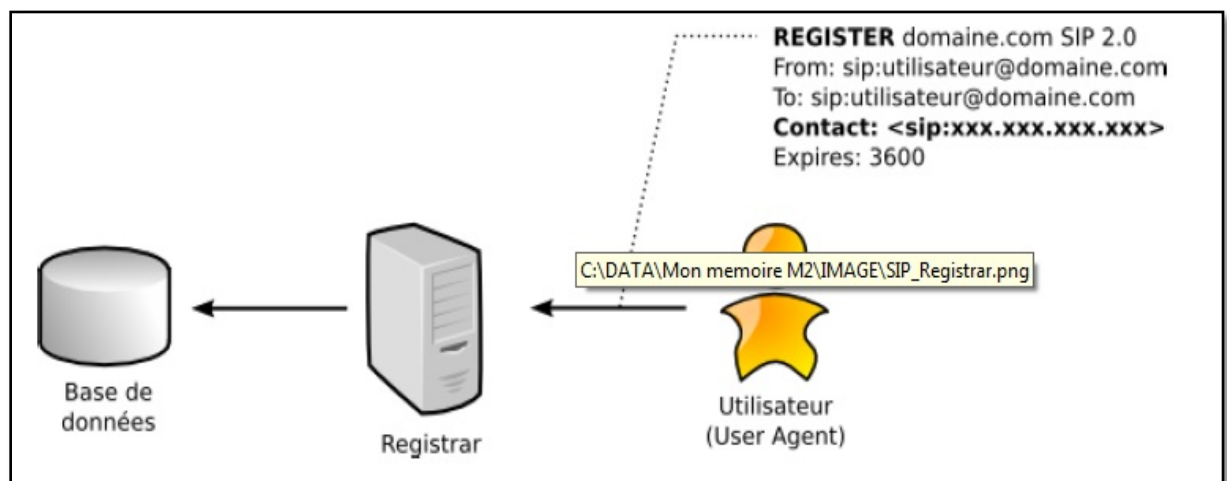
- Proxy joue principalement un rôle d'acheminement.
- Remplit la même fonctionnalité qu'un serveur de redirection, mais pas de la même manière.
- N'annonce pas au client la localisation actuelle de l'utilisateur.

Le Proxy se contente de relayer uniquement les messages SIP pour établir, contrôler et terminer la session (voir la figure 5). Une fois la session établie, les données, par exemple un flux RTP pour la VoIP, ne transitent pas par le serveur Proxy. Elles sont échangées directement entre les User Agents [33].

- **Serveur d'enregistrement(le Registrar) :**Le Registrar est un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données.

Les URI SIP sont très similaires dans leur forme à des adresses email : sip:utilisateur@domaine.com.

Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI [33].



**Figure II.7 : Enregistrement d'un utilisateur.**

- **Serveur de localisation :** Il peut être basé sur une base de données ou un simple fichier texte permettant la mémorisation des différents utilisateurs, leurs droits, leur mot de passe, etc.... ainsi que leurs positions actuelles .Il faut se rappeler que le serveur de localisation est en réalité un «programme »installé sur une machine reliée au réseau. (C'est pourquoi il ne faut pas oublier de la protéger par un mot de passe et un firewall)[34].aussi offre des services pour obtenir et mettre à jour des informations sur le destinataire .Il est utilisé par les serveurs proxy et de redirection.
- **Serveur de redirection :** Permet de rediriger les appels vers la position actuelle d'un utilisateur, en effet le protocole SIP introduit la notion de mobilité, l'adresse utilisée pour appeler un utilisateur ne donne donc aucune indication sur la position actuelle de l'utilisateur, il se peut même qu'il ait simultanément plusieurs positions enregistrées [34]. Un serveur de redirection est un agent d'utilisateur serveur (UAS) qui reçoit les requêtes et renvoie à l'émetteur une ou plusieurs adresses pour contacter le destinataire.
- **Gateway– Passerelle :** Les **Gateway (passerelles)** sont des entités logiques qui sont capables d'établir des liaisons vers des destinations non-IP notamment les réseaux PSTN [34].Actuellement la grande majorité des téléphones sont encore raccordés au réseau Téléphonique commuté.

### II.6.1.3 Responsabilités du SIP :

SIP a la responsabilité de cinq actions :

- Déterminer la localisation de l'utilisateur ; il s'agit de son réseau mère (home) et non pas de sa localisation géographique. Avant tout établissement de session, la localisation des terminaux de bout en bout doit être faite.
- Définir les possibilités de l'appareil de l'utilisateur. L'appareil devant supporter par exemple les codecs multimédia appropriés pour pouvoir espérer une réussite dans l'établissement de la session. En conséquence, SIP doit trouver les types de média utilisés ainsi que leurs paramètres.
- Définir les capacités de l'utilisateur. Ce à quoi l'utilisateur a droit (média, temps de session,...).
- Établir la connexion et définir les paramètres d'appel de l'appelant et de l'appelé.
- Gérer la session. Cela implique la modification des paramètres des sessions en cours, mettre fin à une session, activer les applications [24].

### II.6.1.4 Les différentes requêtes (méthodes) de protocole SIP :

SIP est un protocole de type texte comme HTTP. Le message envoyé comprend une Partie contenant le nom de méthode en première ligne et d'en-têtes pour le passage de paramètres (capacités dont la machine dispose, etc...) sur les lignes suivantes [34].

Le client envoie des requêtes au serveur, qui lui renvoie une réponse.

Les méthodes de base du SIP sont résumées dans le tableau qui suit :

**Tableau II. 2: Méthode de base**

Méthodes	Rôles
INVITE	Elle est utilisée afin d'établir une session entre les clients SIP (User Agent)
ACK	Elle permet de confirmer la réception d'une méthode
BYE	Elle permet la libération d'une session préalablement établie(Demande la fin d'une session).
REGISTER	Elle est utilisée par un UA afin d'indiquer au serveur Registrar la correspondance entre son adresse SIP et son adresse de contact
CANCEL	Elle est utilisée pour demander l'abandon d'un appel en cours mais n'a aucun effet sur un appel déjà accepté. En effet, seule la méthode BYE peut terminer un appel établi.( Annulation d'une requête en attente, cette requête est envoyée par un terminal ou un proxy server)
OPTIONS	Elle est utilisée afin d'interroger les capacités et l'état d'un User agent ou d'un serveur (demande d'information sur les capacités d'un serveur)

Dans IMS, le protocole SIP est utilisé avec ses extensions et ceci de manière intensive. Pour des exigences d'IMS, il y a aussi l'ajout de nouveaux champs d'entête (Path, Service Route et les P-Headers) aux messages SIP. Le tableau ci dessous présente quelques extensions SIP utilisées par IMS.

**Tableau II. 3: Méthodes SIP utilisées par IMS**

Méthodes	Rôles
SUBSCRIBE	Demande de souscription (Demande d'enregistrement à un service de notification).
NOTIFY	Notification d'évènement à un client SIP.
UPDATE	Mise à jour des paramètres de session (Modification des caractéristiques d'une session en cours).
REFER	Renvoi du récepteur vers une ressource identifiée dans la méthode (Demande à un serveur).
PUBLISH	Publier l'état d'une entité
MESSAGE	Transfert pour la messagerie instantanée
PRACK	Acquitter la réception des messages provisoires à un message INVITE.
INFO	Message contenant de la signalisation téléphonique (PSTN).

Cependant la gestion de l'authentification des abonnés et de la sécurité est assurée par le protocole diameter sur les interfaces sh, cx et Dx.

#### **II.6.1.5 Les statuts de réponses :**

Il existe 6 classes de réponses SIP identifiées par la valeur du premier numéro du code de réponse :

- 1xx = "Information" : Requête reçue et traitement de la requête.
- 2xx = Succès : L'action a été reçue avec succès, comprise et acceptée.
- 3xx = Redirection : Une autre action doit être menée afin de valider la requête.
- 4xx = Erreur client : La requête contient une mauvaise syntaxe ou ne peut pas être traitée par ce serveur.
- 5xx = Erreur serveur : Le serveur n'a pas réussi à traiter une requête apparemment correcte.
- 6xx = Echec général : La requête ne peut être traitée par aucun serveur.

#### **II.6.2 Protocole DIAMETER :**

##### **II.6.2.1 Introduction :**

L'évolution progressive du monde des télécommunications vers des réseaux et des services de nouvelle génération est aujourd'hui une tendance forte qui suscite l'intérêt d'une majorité d'acteurs. Avec l'avènement des nouvelles technologies et applications, de nouveaux besoins d'autorisation et d'authentification ont été créés. Des protocoles traditionnels tels que RADIUS ne permettent pas de satisfaire certains détails. Pour cette raison, nous allons étudier le protocole Diameter et le traitement des scénarios d'appel [35].

##### **II.6.2.2 Description du protocole DIAMETER :**

Le protocole DIAMETER a été conçu comme une version améliorée du protocole RADIUS. D'ailleurs ces deux protocoles sont des protocoles AAA (Authentication, Authorisation,



Accounting) et sont utilisés par des procédures d'authentification, d'autorisation et de taxation (online et offline) dans le monde IP.

Dans un domaine IMS, on utilise Diameter entre le HSS et l'I/S\_CSCF pour la gestion des autorisations des abonnés.

Diameter est un protocole qui fournit une trame de base pour tout type de services nécessitant une prise en charge de l'accès, de l'autorisation et de la comptabilité (AAA) ou de la stratégie sur de nombreux réseaux IP. Ce protocole a été dérivé à l'origine du protocole RADIUS qui est également un protocole fournissant des services AAA aux ordinateurs afin de se connecter et d'utiliser un réseau.

Le protocole Diameter a apporté beaucoup d'améliorations sur le protocole RADIUS sous différents aspects. Il comprend de nombreuses améliorations telles que la gestion des erreurs et la fiabilité de la livraison des messages. Ainsi, il vise à devenir le protocole d'authentification, d'autorisation et de comptabilité (AAA) pour la prochaine génération [35].

### **II.6.2.3 Les responsabilités de Diameter :**

Tel qu'il a été défini par l'IETF, Diameter peut être divisé en deux composants :

- Le protocole Diameter en lui-même (Diameter Base) : fournit les conditions de communication et de format des messages, et utilise les protocoles TCP ou SCTP. Ses fonctions sont essentiellement :
  - Livraison des AVPs (Attribute-Value Pair)
  - Négociation des capacités ;
  - Notification des erreurs ;
  - Gestion de session.
- Diameter Application : placée au-dessus du "Diameter Base", cette partie du protocole hérite des facilités de communication ainsi offertes, fournit des messages spécifiques de requête/réponse pour les services utilisés. Ses fonctions sont :
  - Autorisation de l'utilisateur
  - Assignation d'un serveur (S-CSCF)
  - Récupération des informations de localisation
  - Authentification multimédia
  - Finalisation de l'enregistrement
  - Modifications du profil de l'utilisateur [24].

### **II.6.2.4 Types de nœuds et Agents DIAMETER :**

Un nœud DIAMETER est un hôte qui implante le protocole DIAMETER.

- Un client DIAMETER est un nœud à la frontière du réseau qui réalise un contrôle d'accès. Des exemples de clients DIAMETER sont les Network Access Servers (NAS), MME, S4-SGSN.

- Un serveur DIAMETER prend en charge les demandes d'authentification, d'autorisation et de taxation pour un domaine donné (appelé realm). Un exemple de serveur est le HSS [35].

- **Agent DIAMETER** : c'est un nœud DIAMETER qui fournit des services de relai, de proxy ou de traduction [35].
- **Agent relai** : Un agent relai est un agent DIAMETER qui accepte des requêtes, et les relaie soit à un autre agent, soit au nœud DIAMETER de destination à partir des informations présentes dans les requêtes. Cette décision de routage est réalisée grâce à la table de routage basée sur le Destination Realm (nom de domaine de la destination), qui indique le nœud suivant pour une destination donnée. Les agents Relai ne réalisent aucun traitement de niveau application. Les agents relai modifient les messages DIAMETER en y insérant et en y supprimant des informations de routage, mais ne modifient aucune autre partie des messages. Les agents relai ne maintiennent pas d'état de session mais doivent maintenir un état de transaction. Le maintien de l'état de transaction permet de garantir qu'une requête et une réponse appartenant à une même transaction suivent le même chemin.. [26].
- **Agent proxy** : comme un agent relai route le message DIAMETER en utilisant les tables de routage de realm. Cependant, il diffère puisqu'il peut modifier les messages DIAMETER afin d'implanter des politiques d'opérateur (e.g., topology hiding).. Toutefois un agent Proxy peut modifier les messages afin de réaliser un contrôle d'accès, un contrôle de politiques, etc. Un exemple d'agent proxy est l'entité PCRF dans l'architecture LTE [35].
- **Agent de redirection** : fournit aussi une fonction de routage. Il sert de directory permettant généralement la traduction de Nom de domaine Adresse du serveur. A la différence des autres types d'agent (relai et proxy) qui acheminent les messages DIAMETER, l'agent de redirection retourne un type particulier de réponse à l'émetteur de la requête. La réponse contient l'information de routage afin que l'émetteur puisse retransmettre son message directement au serveur destinataire [35].

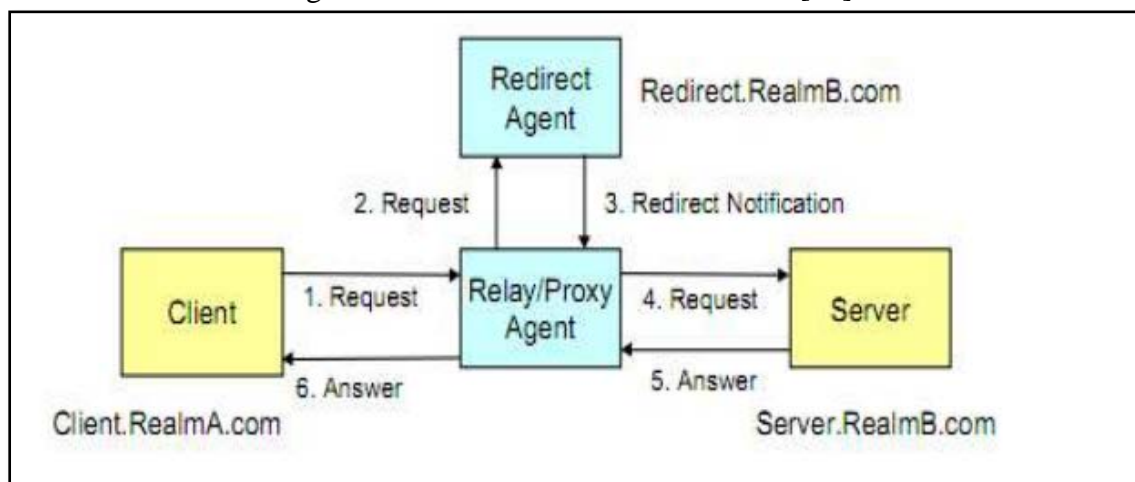
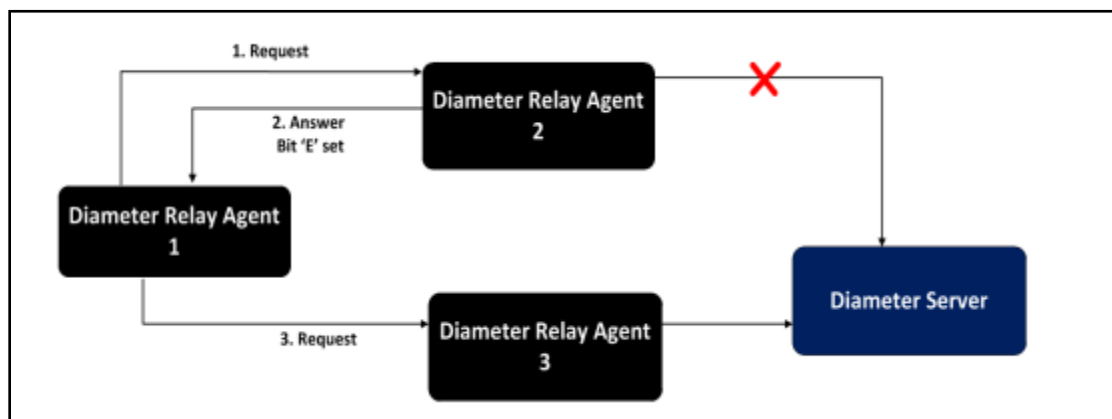


Figure II.8: : les nœuds DIAMETER

- **Un agent de traduction** : traduit les protocoles tels que DIAMETER en RADIUS ou DIAMETER en MAP (Mobile Application Part) pour des aspects d'authentification/autorisation data mobile ou DIAMETER en CAP (CAMEL Application Part) pour des aspects de taxation online ou DIAMETER en SOAP, etc[26].

Les grands fournisseurs d'agent DIAMETER sont ORACLE (DSR, DIAMETER Signaling Router), F5 Networks (SDC, Signaling Delivery Controller) et Ericsson (DIAMETER Signaling Controller). L'agent est appelé DRF (DIAMETER Routing Function) dans les recommandations 3GPP.

- Il est à noter que diameter implémente nativement des mécanismes de gestion d'erreurs. Ainsi, si deux nœuds adjacents ne communiquent pas pendant un certain temps, ils initient périodiquement des requêtes et réponses pour s'assurer de la bonne connectivité. Cela permet de détecter d'éventuelles ruptures de lien. Si un nœud envoie une requête à un voisin sans obtenir de réponse, il retransmet ce message à un nœud alternatif dans la mesure du possible. Le schéma ci-dessous illustre ce scénario [26] :



**Figure II.9 : Mécanisme de gestion des erreurs**

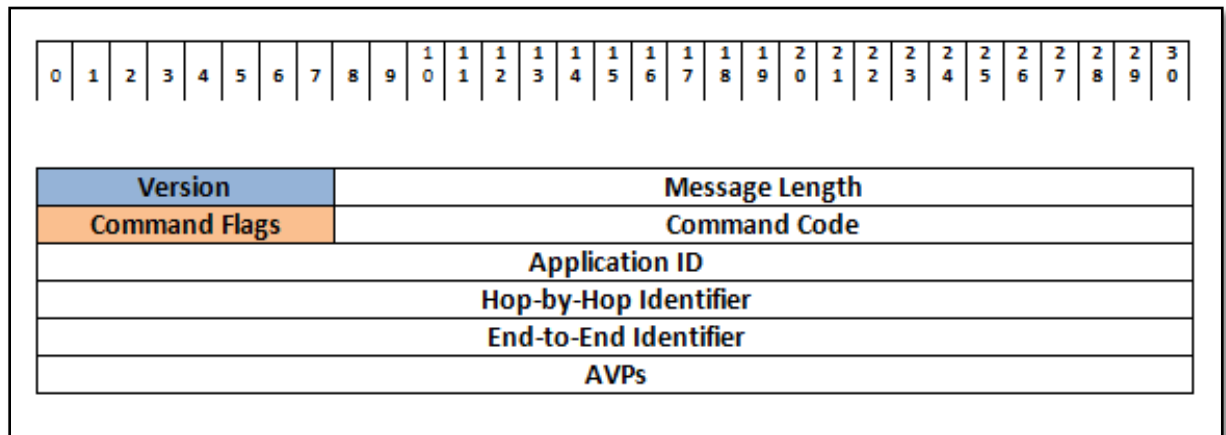
### II.6.2.5 Messages DIAMETER :

Les messages Diameter servent soit à la signalisation du protocole ou bien à délivrer des données propres aux couches applicatives clientes.

Tout message Diameter utilise le schéma montré dans la figure ....

- 1- Version : version du protocole utilisée.
- 2- Message Length : taille du message, incluant l'entête.
- 3- Command Flags : trois bit, le premier indique la nature du message (requête ou réponse), le second indique si le message doit être transféré ou traité localement, le dernier est utilisé seulement pour les réponses importantes (peut spécifier si la réponse contient une erreur).
- 4- Command Code : contient un indicateur d'appartenance du message.
- 5- Application ID : identifie l'application Diameter utilisée.
- 6- Hop-by-Hop ID : permet d'associer la réponse à la requête.
- 7- End-to-End ID : identifiant du message qui doit rester le même tout le long, afin d'éviter les duplications. Cet identifiant doit donc rester unique.

8- AVP : contient les paires attribut-valeur (ou tuple) constituant les paramètres du message [35].



**Figure II.10 : structure du message Diameter**

### II.6.2.6 Son rôle dans les réseaux NGN & IMS :

"Diameter" vise à garantir que les réseaux IMS et les services NGN peuvent compter sur une infrastructure et des solutions éprouvée de vente. Le protocole Diameter joue un rôle crucial dans les réseaux NGN. Il est utilisé comme un AAA pour les applications de gestion, la mobilité, le nomadisme, la sécurité de réseau, l'accès au réseau et les services de tarification. Le résultat, qui vise à tester et démontrer l'interopérabilité de toutes les technologies NGN utilisant des interfaces de Diameter, comprendra IMS, WiMAX et les tests LTE. Certaines normes utilisées pour décrire les interfaces sont les suivantes: IETF, 3GPP, 3GPP2, TISPAN, WiMAX, LTE, et Packet Cable.

Avec la nouvelle architecture de service orienté tout IP, Diameter est largement} utilisé dans IMS et dans les normes développés par le 3GPP et le groupe de travail sur LTE. Comme exemple, nous pouvons regarder les plans de contrôle et de service de IMS comme décrit ci dessous:

- Le Home Subscriber Server (HSS) est une base de données contenant} l'identification des utilisateurs, les informations de contrôle de service et des utilisateurs, l'authentification et l'autorisation des utilisateurs, les informations de localisation, et les profils utilisateur. HSS est également utilisé dans l'architecture LTE.
- Le Service Call Session Control Function (S-CSCF) utilise les interfaces Diameter pour autoriser les utilisateurs (en échangeant des informations avec le HSS en réponse à une demande d'enregistrement SIP) et récupérer les informations relatives aux abonnés.
- Les Serveurs d'applications, qui récupèrent les profils d'abonnés utilisent} également Diameter.
- Les interfaces de charge (Ro et Rf dans l'architecture IMS) sont basées sur) le diameter de l'IETF et sur les extensions du protocole résultant de 3GPP. Diameter joue également un rôle central dans la mise en oeuvre de la Qualité de Service (QoS) dans les réseaux NGN,

permettant ainsi à des services comme la VoIP, la diffusion vidéo, la vidéoconférence et des communications unifiées d'entreprises d'être gérés dans le même réseau convergent [35].

## **II.7 Signalisation dans L'IMS :**

Comme SIP ne décrit pas le flux média, on utilise en plus le protocole SDP (Session Description Protocol) [HaPJ06]. SDP est transporté dans le cœur des messages SIP ; il décrit les sessions multimédia en termes de codeur audio, vidéo, informations de session (bande requise, type de flux...) et adressage multicast ... Ces informations seront exploitées pour faire la réservation de ressource dans le plan transport. Notons toutefois que certaines interfaces internes du réseau IMS utilisent la signalisation "Diameter" et non pas SIP. C'est une application standardisé par le 3GPP qui permet d'interfacer différentes entité du réseau IMS. Les échanges Diameter sont toujours du type : un message requête et une réponse associé. Les informations échangées dans ces messages sont mis dans des attributs appelés AVP (Attribute Value Pairs). Chaque interface Diameter a ces AVPs et ces commandes [24].

### **II.7.1 Type de signalisation en IMS :**

Dans tout type de réseau il y a toujours quatre types de signalisations ; dans IMS la signalisation est réaliser essentiellement par SIP :

- Signalisation d'enregistrement : c'est la signalisation par la qu'elle un terminal s'enregistre dans le réseau. Elle contient les procédures de téléchargement du profile et la gestion de la localisation. Cette signalisation est effectuée par la procédure d'enregistrement SIP (SIP REGISTER).
- Signalisation d'appel : c'est la signalisation par la qu'elle on établit une association de bout en bout entre les points d'extrémité désirant communiquer, c'est caractérisé par l'échange de référence. Ceci est réalisé en IMS grâce à la procédure d'établissement de session (SIP INVITE)
- Signalisation de connexion : c'est l'affectation d'un service support à un appel. De proche en proche on va réserver des ressources dans le réseau selon la QoS requise pour le service. Au niveau SIP cette signalisation est effectuée grâce aux entêtes SDP qui permettent de décrire le trafic et le ressources requis. Au niveau transport on utilise les mécanismes RSVP, DiffServ, MPLS pour faire la qualité de service dans le réseau IP.
- Signalisation d'intelligence : c'est la signalisation qui nous permet de faire un traitement substitutif par rapport au traitement d'appel normal. D'une façon similaire aux réseaux intelligent de type RI (INAP) ou CAMEL, les services sont exécuter par l'équivalent aux plateformes de service qui sont des serveurs d'applications (AS). Un autre type de signalisation SIP est utilisé sur l'interface ISC entre les AS et les S-CSCF [30].

## **II.8 Etude comparative des solutions IMS sur le marché : [26]**

Dans un réseau IMS, on peut utiliser plusieurs solutions. Ces solutions peuvent être propriétaires ou open source.

## II.8.1 Solutions :

Les solutions IMS sont le plus souvent proposées par des équipementiers et permettent généralement d'insérer l'IMS dans une architecture NGN (NextGeneration Network) déjà implémentée ou un réseau 3G/4G. Il existe plusieurs solutions, mais nous allons présenter 3 solutions :

- IMS AAA JUNIPER.
- IMS par Ericsson.
- OpenIMSCore.

### II.8.1.1 IMS AAA JUNIPER :

JUNIPER propose cette solution. JUNIPER est une société américaine proposant des solutions d'interconnexion et de sécurité.

Le serveur IMS AAA de Juniper permet aux opérateurs mobiles (2G, 3G ou 4G) de supporter les technologies 3GPP WLAN afin d'assurer en collaboration avec la base de données (HSS ou HLR) l'authentification des abonnés.

Cette solution implémente les protocoles du type AAA (Authentication, Accounting, Authorization). Ces protocoles permettent généralement de gérer l'authentification, la facturation et l'autorisation des abonnés aux services. La figure 11 montre architecture de la solution IMS AAA de JUNIPER :

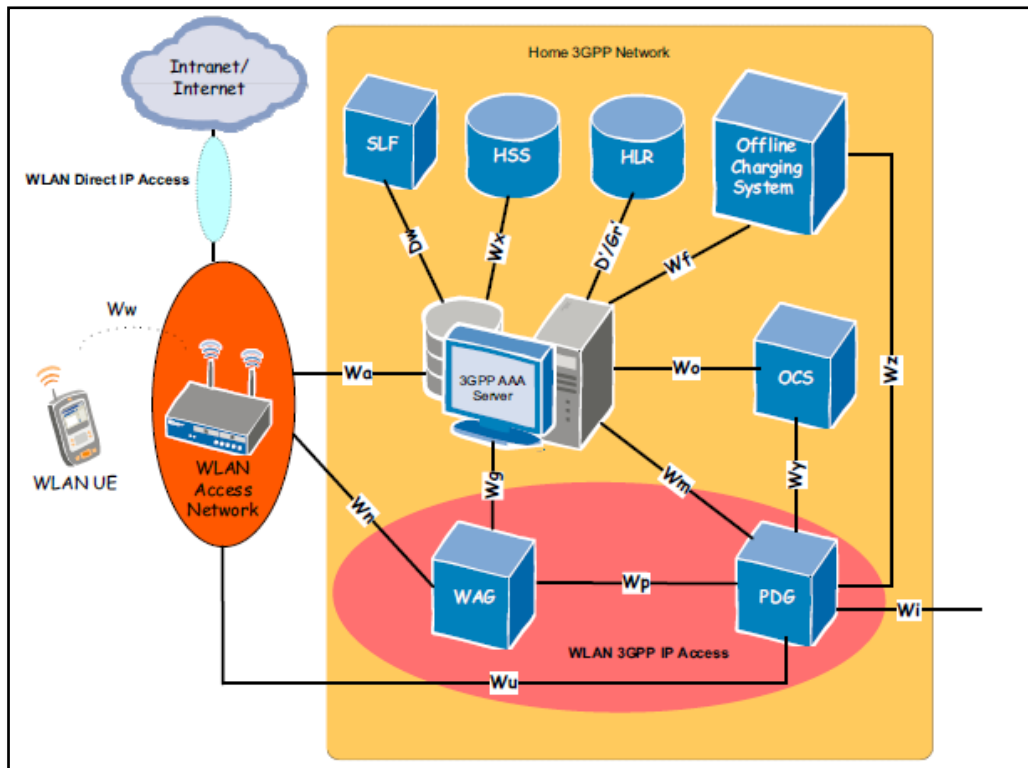


Figure II.11 : Architecture de la solution IMS AAA de JUNIPER

L'avantage de cette solution est qu'elle supporte plusieurs protocoles dont radius, diameter, IP (IPV4 et IPV6), ipsec, TLS et TCP/UDP.

IMS AAA JUNIPER (3GPP AAA Server sur la figure) s'interconnecte aux différents blocs (HSS, HLR, SLF, OCS ....) via des interfaces spécifiques qui supportent soit le protocole diameter ou le protocole raduis.

### II.8.1.2 IMS par Ericsson:

Ericsson est l'un des leaders du marché en termes de fourniture d'équipement des réseaux de télécommunication. Ainsi il propose plusieurs solutions permettant la migration vers l'IMS et l'une de ces solutions est : Ericsson Call Session Control Function (Ericsson CSCF).

La solution Ericsson CSCF permet d'introduire un coeur de réseau IMS. Ces blocs CSCF se chargeront des opérations de signalisation et permettront aussi d'authentifier ensemble avec le HSS les abonnés et leur position. Mise sur le marché depuis 2015, cette solution favorise la convergence et dispose d'une bonne interopérabilité. Elle offre également une grande flexibilité, prend en charge une grande variété de procédure d'authentification, et fournit une haute disponibilité. Elle offre également des possibilités de tarification souples pour soutenir de nombreux modèles de trafic, y compris post-payé, prépayé, basé sur le volume, l'heure, par événement, etc.

### II.8.1.3 OpenIMSCore:

La plateforme OPENIMSCORE contient les fonctionnalités de base d'un serveur SIP. Elle a été conçue de façon modulaire et est composée d'un noyau fortement efficace responsable de la réception, de l'analyse SIP et des routages des messages. L'OpenIMSCore est une implémentation des Call Session Control Functions (CSCFs) et du HSS (Home Subscriber Server), qui forment ensemble le réseau coeur des architectures IMS comme spécifié par le 3GPP, le 3GPP2, l'ETSI et TISPAN. Les CSCF sont essentiellement le P-CSCF, l'I-CSCF, et le S-CSCF. La figure 12 présentée l'architecture d'OpenIMSCore:

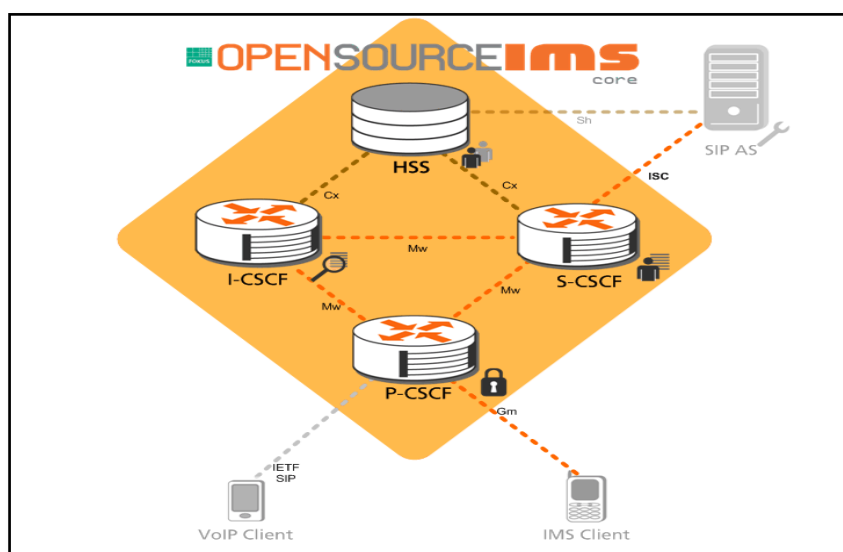


Figure II.12: Architecture OpenIMSCore

## II.8.2 Etude comparative des solutions :

Les solutions présentées ci-haut ne sont pas les seules permettant la migration vers IMS mais sont les plus utilisées. On va faire un tableau qui fait une étude comparative de ses différentes solutions :

**Tableau II. 4: Etude comparative des solutions.**

Solutions	Protocoles supportés	Accessibilité	Niveau de Sécurité	Flexibilité
<b>IMS-AAA-JUNIPER</b>	TCP, UDP, Diameter, Raduis, IP, SSL/TLS, IPSec.	Requiert une Licence car c'est un produit propriétaire.	Elevé grâce à l'utilisation de l'AAA (Authentification, Authorization, Accounting).	Bonne
<b>Ericsson CSCF</b>	TCP, UDP, Diameter, IP, SIP, SSL/TLS, IPSec .	Requiert une Licence car c'est un produit propriétaire.	sécurité standard de l'IMS. Procédure AKA pour l'authentification.	Bonne
<b>OpenIMSCore</b>	TCP, UDP, Diameter, IP, SIP, SSL/TLS, IPSec, RTP, RTSP.	Produit Open Source (Libre).	sécurité standard de l'IMS. Procédure AKA pour l'authentification.	Bonne



## II.9 Conclusion

L'objectif de ce chapitre est de fournir un point de départ pour comprendre les normes entourant IMS, un sujet immense et très compliqué. Nous avons présenté les concepts de l'architecture IMS, sa motivation ainsi que les bases des différents protocoles utilisés (SIP, Diameter).

Grâce à l'IMS, les réseaux fixes et mobiles ne se contentent plus d'être un « réseau téléphonique » classique. L'IMS permet d'établir des communications entre multiples terminaux / utilisateurs, et il permet d'intégrer des services temps-réel et non temps-réel dans une même session. De plus, il est possible de créer de nouveaux usages en utilisant des interactions entre ces services.

les éléments nécessaires à l'élaboration de stratégies de déploiement de business de services sur IP basée sur IMS :

- Mise en œuvre des nouveaux services supportés par l'IMS et les principes de leur facturation ;
- Scénarii de migration vers une architecture IMS en particulier scénarii de migration du réseau intelligent téléphonique,
- Niveau des investissements nécessaires,
- Taxation et facturation des services de l'IMS
- Exploitation des réseaux et des services IMS

## **Chapitre III**

# ***Mise en service d'une solution IMS OPENIMSCORE***

### III.1 Introduction :

L'Open IMS Core est une implémentation open source des fonctions de contrôle de session d'un cœur de réseau IMS (CSCFs) et d'une version légère d'un Home Subscriber Server (HSS), qui forment ensemble les éléments de cœur de toutes architectures IMS/NGN. Tous les composants sont basés sur des logiciels opensource, tels que SER(SIP Express Router)ou MySQL... Cette implémentation est avant tout conçue pour la recherche et le développement (fournisseurs de matériel de télécommunications, opérateurs de réseaux, projets de recherche universitaire)[20]. Open source IMS Core est formé par l'ensemble des éléments de base d'une architecture IMS définie dans les réseaux de nouvelle génération et telle qu'indiquée dans 3GPP, 3GPP2, ETSI TISPAN[28].

IMS est aujourd'hui en phase de test au sein de plus en plus d'opérateurs à travers le monde, les efforts de R&D respectant NGNs ont des chances de trouver le soutien d'une audience plus large dans un avenir proche – Plus particulièrement pour le développement de services [36].

Alors qu'il ya déjà de nombreux projets opensource dans le domaine de la VoIP pour les clients SIP, les proxys, les différentes couches réseaux liée à la VoIP, il n'y a pour le moment presque pas de projets opensource qui se concentre particulièrement sur IMS [36].

Le projet d'Opensource IMS (Open IMSCore) a été lancé en 2006, développé par l'institut Franhofer FOKUS (Fraunhofer Institute for Open Communication System) a pour objectif de remplir le vide actuel qui existe pour IMS dans le paysage des logiciels opensource avec une solution flexible et extensible qui a déjà montré ses performances dans différents projets de R&D[36].

Cette solution a été adoptée par plusieurs opérateurs et fournisseurs de télécommunications dans le monde comme un banc d'essais pour tester les fonctionnalités de système IMS avec l'intégration des nouveaux services sur IP comme la télévision sur IP (IPTV)[28].

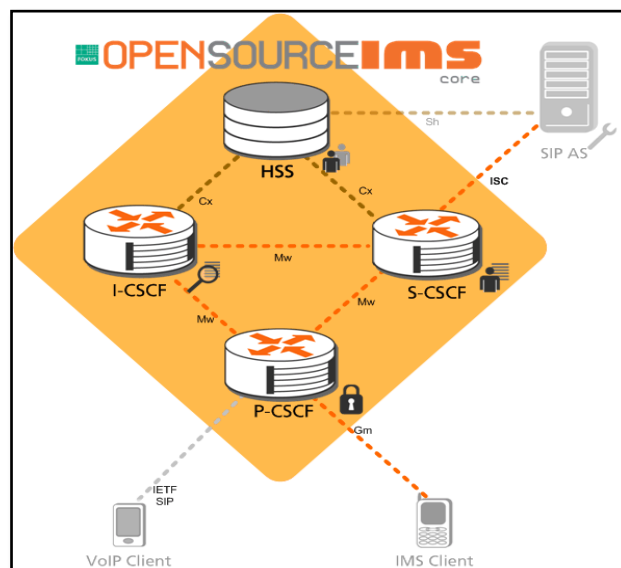


Figure III.1: Opensource IMS

La base des données d'OpenIMSCore, FHoSS (FOKUS Home Subscriber Server) est basé sur MySQL. La logique du FHoSS d'application est entièrement écrite avec Java. La composante principale de cette base de données est l'utilisateur maître (Master) à base de MySQL, supportant des entités de réseaux qui gèrent les communications sur IMS. Plus précisément, le FHoSS offre les fonctions suivantes :

- stocke et gère les informations relatives au profil d'abonnés ;
- génère des données pour l'authentification et l'autorisation des utilisateurs ; - maintenir les tables de routage sous forme de répertoires de localisation de l'abonné ;
- fournir des informations sur les points de service de l'abonné ;
- gestion de déclencheur des services;

FHoSS est configuré pour supporter plusieurs millions d'abonnés et peut servir de multiples centaines d'utilisateurs enregistrés par seconde[28].

### III.2 Architecture de la solution :

OpenIMSCore est une plate-forme libre constitué des entités principale de l'IMS (le bloc de contrôle CSCF et la base de donnée HSS) conformément aux normes définie par la 3GPP[28], on a inséré dans l'architecture un serveur DNS.

- Le serveur DNS nous permet de faire de la résolution des noms. Pour des raisons de performance liées à nos équipements, nous avons implémenté ce service sur le même serveur où est implémenté OpenIMCore.

La plate-forme d'architecture est présentée comme ça:

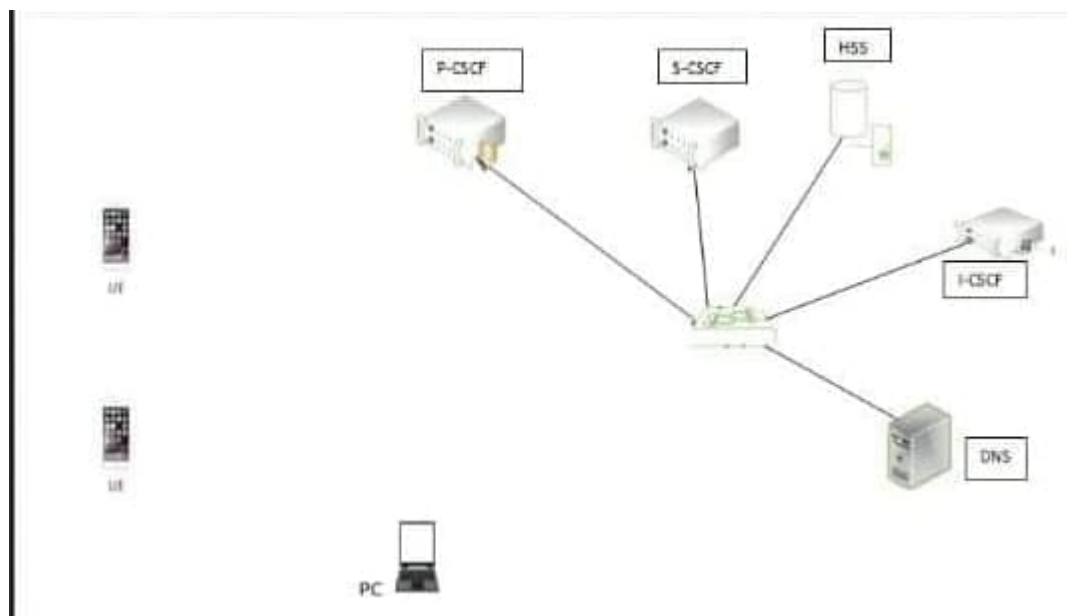


Figure III.2: la plate-forme d'architecture

### III.3 Installation et configuration d'OpenIMSCore :

L'installation d'openIMSCore requiert quelques logiciels et ressources matérielles comme dépendances.

#### III.3.1 Les pré-requis :

Pour installer OpenIMSCore, certaines dépendances sont requises.

La configuration matérielle doit au moins respecter les exigences suivantes :

- Une machine Linux Opérationnelle ( Avec un système Ubuntu dans notre Cas) ;
- Environ 100 à 150 Mo d'espace libre sur le disque de la machine (pour être sur le côté sécuritaire);
- De préférence 1Go de RAM ;
- Un serveur DNS configurable préinstallé ;
- Un accès internet est requis pour l'installation des paquets (pour ceux utilisant une machine virtuelle)

En ce qui concerne les pré-requis logiciels, nous aurons besoin des paquets suivants :

- SVN pour la récupération des packages sources d'openIMSCore ;
- GCC3/4, faire (make), ant pour la compilation ;
- Flex, bison comme analyseur lexical et syntaxique ;
- JDK 1.7 (default-jdk ou openjdk) pour simuler une machine virtuelle java ;
- Les paquets : libmysql, libmysql-dev, libxml2, curl, libcurl4-gnutls-dev et libxml2-dev sont aussi nécessaires ;
- Le paquet `ipsec-tools`, `openssl` sont utiles pour la sécurité (pour le chiffrement de clés) ;
- MySQL-server configurés pour un lancement à chaque démarrage de la machine, pour plus de simplicité – normalement par défaut lors de l'installation;

Vu que nous avons utilisé un système ubuntu (version 15), tous les paquets précités vont s'installer en utilisant la commande `apt-get install` « nom du paquet »[26].

Une fois toutes les dépendances satisfaites, nous pourrons passer à l'installation d'openIMSCore.

- **L'installation des pré-requis pour OpenIMSCore** : [37]

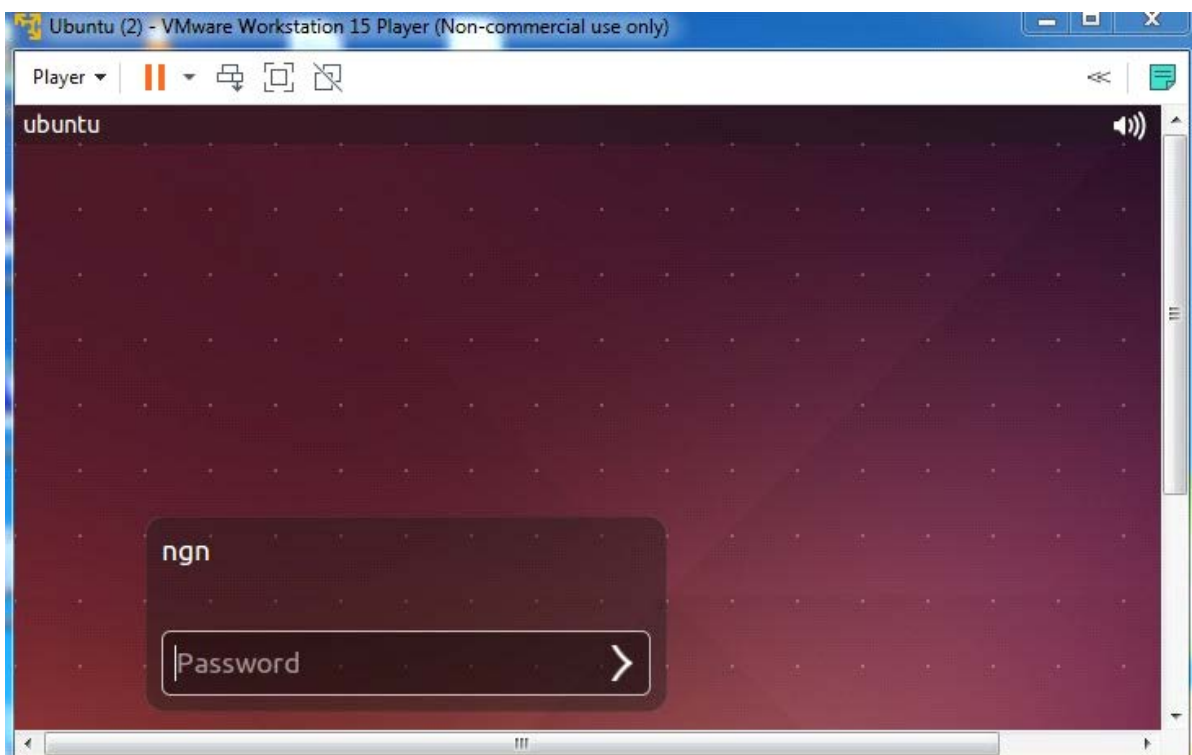
Et pour les prérequis logiciels, nous aurons besoin des paquets suivants :

```
sudo apt-get install subversion
sudo apt-get install gcc
sudo apt-get install make
sudo apt-get install openjdk-7-jdk
sudo apt-get install openjdk-7-jre-headless
sudo apt-get install openjdk-7-jre-lib
sudo apt-get install ant
```

```
sudo apt-get install bison
sudo apt-get install flex
sudo apt-get install libxml2 libxml2-dev
sudo apt-get install ipsec-tools
sudo apt-get install curl
sudo apt-get install libcurl4-gnutls-dev
sudo apt-get install bind9
```

➤ Installation MySQL :

```
sudo apt-get install mysql-server-5.5
sudo apt-get install mysql-client-5.5
sudo apt-get install libmysqlclient-dev
```



**Figure III.3:VMware Workstation 15 Player**

### III.3.2 Récupération du code source d'OpenIMSCore (Via SVN) : [26]

Pour installer OpenIMSCore, nous allons d'abord récupérer les codes sources. Le code source est préconfiguré pour fonctionner selon un chemin de fichier standard

Ainsi avant de récupérer les paquets, nous devons dans un premier temps créer un répertoire dans lequel nous allons mettre les paquets. Ceci se fait en utilisant la commande :

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

Après la création, on va créer les dossiers `ser-ims`, `FHoSS` et y placer respectivement les serveurs CSCFs (P-CSCF, I-CSCF, S-CSCF) et HSS :

```
cd /opt/OpenIMSCore
```

```
mkdir ser_ims
```

```
mkdir FHoSS
```

Pour récupérer les codes sources des paquets qui concernent les blocs CSCFs, on se rend dans le répertoire `/opt/OpenIMSCore` et on exécute en utilisant la commande :

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

Dans le même répertoire `/opt/OpenIMSCore`, nous allons récupérer les paquets responsable de la mise en place de la base de données HSS. En utilisant la commande suivante :

```
svn checkout https://svn.code.sf.net/p/openimscore/code/FHoSS/trunk/FHoSS/
```

Après la récupération des codes sources, nous devons passer à la compilation de ces codes.

### III.3.3 Compilation d'OpenIMSCore :

- **Compilation des serveurs .csf (ser\_ims) ;** [20]

Nous allons nous rendre dans le répertoire `/opt/OpenIMSCore/ser_ims` et taper la commande suivante :

```
cd ser_ims
```

```
make install-libs all
```

Cette dernière commande permet de mettre en place les différents blocs CSCF à savoir P-CSCF, I-CSCF, S-CSCF. Il ne reste plus qu'à les configurer.

On passe à la configuration de JAVA:[37]

```
echo $JAVA_HOME
```

```
echo $CLASSPATH
```

```
echo $PATH
```

```
which java
```

```
whereis java
```

Ensuite, on utilise le paquet suivant : `apt-get update`

```
export JAVA_HOME=/usr/lib/jvm/java-7-openjdk-i386
```

- **Compilation du serveur FHoSS ;** [38]

D'abord le JDK doit être installé sur la machine. Ensuite, il faut se rendre dans le répertoire `/opt/OpenIMSCore/FHoSS` et exécuter les commandes suivantes :

```
cd FHoSS
ant compile
ant deploy
cd ..
```

- **Fichiers de configuration adaptall** :[37]

modifier le nom de domaine en utilisant configurator.sh (appliquer le script dans trois répertoires) :

- Pour modifier le nom de domaine et l'adresse IP, nous avons utiliser un script(configurator.sh) dans ser\_ims/cfg/.

-Copiez tous les fichiers \*.sql \*.cfg \*.xml que nous avons modifié dans le même répertoire que configurator.sh et exécutez-le.

- Répertoire : `cd /opt/OpenIMSCore/FHoSS/deploy`

```
cd /opt/OpenIMSCore/ser_ims/cfg/
```

```
root@lab:/opt/OpenIMSCore/ser_ims/cfg#./configurator.sh
/opt/OpenIMSCore/FHoSS/deploy/c3p0.properties
/opt/OpenIMSCore/FHoSS/deploy/DiameterPeerHSS.xml
/opt/OpenIMSCore/FHoSS/deploy/hibernate.properties
/opt/OpenIMSCore/FHoSS/deploy/hss.properties
/opt/OpenIMSCore/FHoSS/deploy/log4j.properties
```

Dominio: imscuba.test

IP : 192.168.0.254

- Répertoire : `/opt/OpenIMSCore/FHoSS/scripts`

```
root@lab:/opt/OpenIMSCore/ser_ims/cfg#./configurator.sh
/opt/OpenIMSCore/FHoSS/scripts/hss_db_migrate_dsai.sql
/opt/OpenIMSCore/FHoSS/scripts/hss_db.sql /opt/OpenIMSCore/FHoSS/scripts/userdata.sql
```

Dominio: imscuba.test

IP:192.168.0.254

### **III.3.4 Paramétrage de la configuration d'IMS :**

La configuration initiale d'openIMSCore permet uniquement un fonctionnement en local host .

Par ailleurs, le domaine par défaut est « open-ims.test ».

On remplace 127.0.0.1 le cas échéant avec notre adresse IP 192.168.0.254

- On change les mots de passe de base de données



Pour cette opération, les `ser_ims / cfg / configurator.sh` pourrait nous aider.

#### - Configuration de MySQL:

On se rend dans le répertoire `/opt/OpenIMSCore` et on effectue les 3 dumps suivants :

```
cd /opt/OpenIMSCore/  
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 »

On doit vérifier que la base est accessible et chargée.

```
mysql -u root -p -h localhost  
show databases
```

#### - Configuration de DNS:[20]

La configuration d'OpenIMSCore consistera essentiellement à configurer les serveurs DNS. Un échantillon de la zone DNS du fichier peut être trouvé dans `ser_ims/cfg/open-ims.dnszone`.

On doit modifier le fichier `/etc/bind/named.conf` en ajoutant la zone suivante :

```
zone "open-ims.test" {  
    type master;  
    file "/etc/bind/open-ims.dnszone";  
};
```

Ensuite, on doit copier le fichier `"open-ims.dnszone"` sous `/etc/bind/`

```
sudo cp ser_ims/cfg/open-ims.dnszone etc/bind/
```

On doit éditer le fichier `/etc/resolv.conf` [37]

```
root@lab:~# nano etc/resolv.conf
```

```
search open-ims.test  
domain open-ims.test  
nameserver 192.168.0.254
```

#### Remarque

A chaque redémarrage du système, ce fichier va être écrasé par le Network Manager.

Ainsi, nous avons fait un backup de ce fichier (nous l'utiliserons dans notre script automatique de lancement des serveurs, que nous verrons à la fin de ce tutoriel) :

```
cp /etc/resolv.conf /etc/resolv.conf.ims
```

On doit éditer le fichier `/etc/hosts` et ajouter les lignes suivantes :

```
root@lab:/# nano etc/hosts
```

```
192.186.0.254 localhost
```

```
192.168.0.254 imscore
```

```
192.168.0.254 imscore
```

```
192.168.0.254 pcscf
```

```
192.168.0.254 scscf
```

```
192.168.0.254 trcf
```

```
192.168.0.254 bgcf
```

```
192.168.0.254 mgcf
```

```
192.168.0.254 hss
```

```
192.168.0.254 ue
```

```
192.168.0.254 presence
```

```
192.168.0.254 pcrf
```

```
192.168.0.254 clf
```

Comme précédemment, faites un backup de ce fichier :

```
cp /etc/hosts /etc/hosts.ims.
```

Enfin, on va redémarrer Bind Server :

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

Pour vérifier que le changement de configuration a bien été pris en compte (via dig) :

```
dig open-ims.test.
```

### III.3.5 Lancement des serveurs d'OpenIMS: [20]

Nous avons copier les fichiers de configuration `.cfg` et `.xml`, ainsi que les scripts de lancement `.sh` des serveurs `x.cscf` dans le répertoire de notre choix (nous avons choisis de les placer dans le répertoire d'OpenIMS pour plus de simplicité et d'organisation :

```
cd /opt/OpenIMSCore/
```

```
cp ser_ims/cfg/*.cfg /opt/OpenIMSCore/
```

```
cp ser_ims/cfg/*.xml /opt/OpenIMSCore/
```

```
cp ser_ims/cfg/*.sh /opt/OpenIMSCore/
```

- **Lancement d'Open OpenIMS :**

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

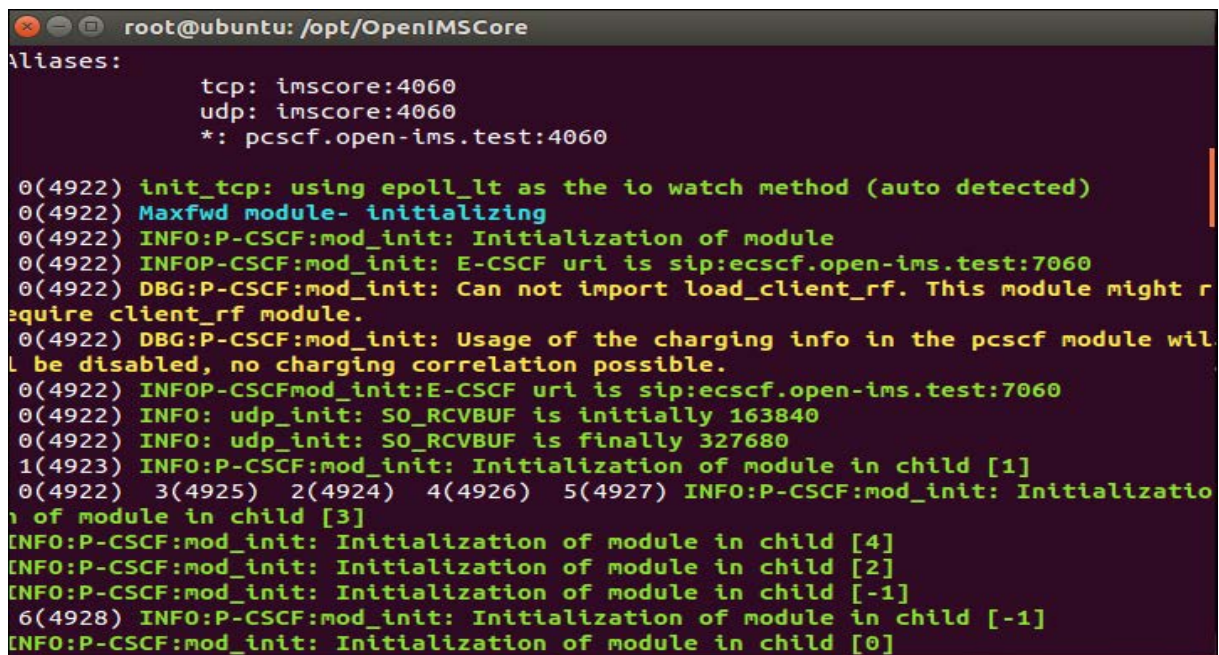
- Ces trois serveurs doivent fonctionner en parallèles; on peut lancer ces trois serveurs sur une même VM, cela ne pose aucun problème technique (en revanche, pas top au niveau des performances)

Ceci se fait en utilisant les commandes :

## 1- P-CSCF

```
cd opt/OpenIMSCore
```

```
./pcscf.sh
```



```
root@ubuntu: /opt/OpenIMSCore
Aliases:
    tcp: imscore:4060
    udp: imscore:4060
    *: pcscf.open-ims.test:4060

0(4922) init_tcp: using epoll_lt as the io watch method (auto detected)
0(4922) Maxfwd module- initializing
0(4922) INFO:P-CSCF:mod_init: Initialization of module
0(4922) INFO:P-CSCF:mod_init: E-CSCF uri is sip:ecscf.open-ims.test:7060
0(4922) DBG:P-CSCF:mod_init: Can not import load_client_rf. This module might require client_rf module.
0(4922) DBG:P-CSCF:mod_init: Usage of the charging info in the pcscf module will be disabled, no charging correlation possible.
0(4922) INFO:P-CSCF:mod_init:E-CSCF uri is sip:ecscf.open-ims.test:7060
0(4922) INFO: udp_init: SO_RCVBUF is initially 163840
0(4922) INFO: udp_init: SO_RCVBUF is finally 327680
1(4923) INFO:P-CSCF:mod_init: Initialization of module in child [1]
0(4922) 3(4925) 2(4924) 4(4926) 5(4927) INFO:P-CSCF:mod_init: Initialization of module in child [3]
INFO:P-CSCF:mod_init: Initialization of module in child [4]
INFO:P-CSCF:mod_init: Initialization of module in child [2]
INFO:P-CSCF:mod_init: Initialization of module in child [-1]
6(4928) INFO:P-CSCF:mod_init: Initialization of module in child [-1]
INFO:P-CSCF:mod_init: Initialization of module in child [0]
```

Figure III.4: Démarrage de P-CSCF

## 2- S-CSCF

```
cd opt/OpenIMSCore
```

```
./scscf.sh
```

```

root@ubuntu: /opt/OpenIMSCore
4(4985) [16777216,10415]
4(4985) [16777216,4491]
4(4985) [16777216,13019]
4(4985) [16777216,0]
4(4985) [16777217,10415]
4(4985) [16777221,10415]
4(4985) -----
5(4976) INF:S-CSCF:----- Registrar Contents begin -----
5(4976) INF:S-CSCF:----- Registrar Contents end -----
4(4985) --- Peer List: ---
4(4985) S[I_Open] hss.open-ims.test:3868 D[ ]
4(4985) [16777216,10415]
4(4985) [16777216,4491]
4(4985) [16777216,13019]
4(4985) [16777216,0]
4(4985) [16777217,10415]
4(4985) [16777221,10415]
4(4985) -----
5(4976) INF:S-CSCF:----- S-CSCF Dialog List begin -----
5(4976) INF:S-CSCF:----- S-CSCF Dialog List end -----
5(4976) INF:S-CSCF:----- Registrar Contents begin -----
5(4976) INF:S-CSCF:----- Registrar Contents end -----
4(4985) DBG:peer_timer(): Peer hss.open-ims.test State 6
4(4985) --- Peer List: ---

```

Figure III.5: Démarrage de S-CSCF

### 3- I-CSCF

```
cd opt/OpenIMSCore
```

```
./icscf.sh
```

```

root@ubuntu: /opt/OpenIMSCore
17(5069) INFO:I-CSCF:mod_init: Initialization of module in child [7] tcp receiver child=2
19(5071) 18(5070) INFO:I-CSCF:mod_init: Initialization of module in child [8] tcp receiver child=3
INFO:I-CSCF:mod_init: Initialization of module in child [-4] tcp main process
9(5061) INFO:I-CSCF:mod_init: Initialization of module in child [1003] cdp_worker
9(5061) INFO:[2] Worker process started...
14(5066) DBG:peer_timer(): Peer hss.open-ims.test State 0
14(5066) DBG:I_Snd_Conn_Req(): Peer hss.open-ims.test
14(5066) INFO:peer_connect(): Trying to connect to 192.168.0.254 port 3868
14(5066) INFO:peer_connect(): Peer hss.open-ims.test:3868 connected
14(5066) --- Peer List: ---
14(5066) S[Wait_Conn_Ack] hss.open-ims.test:3868 D[ ]
14(5066) -----
12(5064) --- Peer List: ---
12(5064) S[I_Open] hss.open-ims.test:3868 D[ ]
12(5064) [16777216,10415]
12(5064) [16777216,4491]
12(5064) [16777216,13019]
12(5064) [16777216,0]
12(5064) [16777217,10415]
12(5064) [16777221,10415]
12(5064) -----

```

Figure III.6: Démarrage d'I-CSCF

## Serveur FHoSS:

On va lancer le serveur via `FHoSS/deploy/startup.sh`.

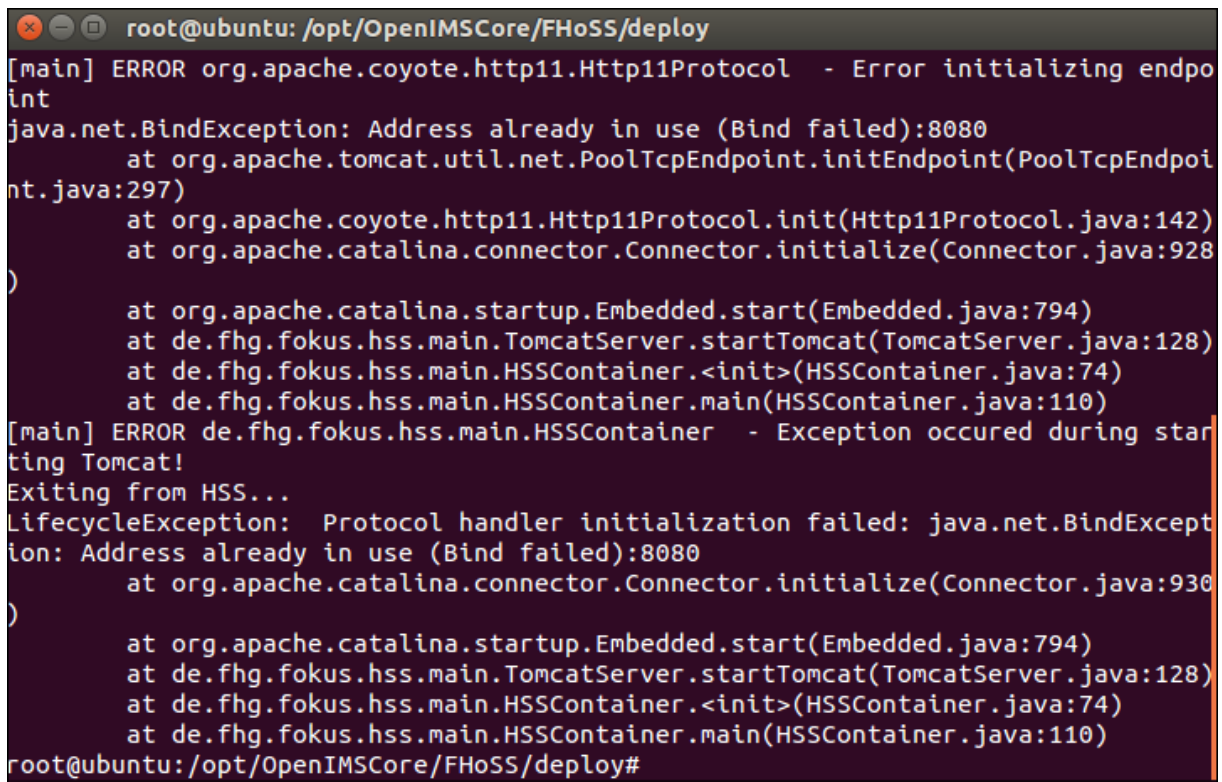
```
cd opt/OpenIMSCore
```

```
cd FHoSS/deploy
```

```
sh startup.sh
```

**Remarque :** Il est possible que nous obtenions une erreur lors du lancement du script; dans ce cas, il est fort probable que celle-ci soit liée à la variable d'environnement `JAVA_HOME`. On va vérifier que cette variable a été correctement exportée. Si ce n'est pas le cas, on doit lancer la commande suivante dans un terminal :[20]

```
> export JAVA_HOME= »/usr/lib/jvm/java-1.7.0-openjdk/ »
```



```
root@ubuntu: /opt/OpenIMSCore/FHoSS/deploy
[main] ERROR org.apache.coyote.http11.Http11Protocol - Error initializing endpoint
java.net.BindException: Address already in use (Bind failed):8080
    at org.apache.tomcat.util.net.PoolTcpEndpoint.initEndpoint(PoolTcpEndpoint.java:297)
    at org.apache.coyote.http11.Http11Protocol.init(Http11Protocol.java:142)
    at org.apache.catalina.connector.Connector.initialize(Connector.java:928)
    at org.apache.catalina.startup.Embedded.start(Embedded.java:794)
    at de.fhg.fokus.hss.main.TomcatServer.startTomcat(TomcatServer.java:128)
    at de.fhg.fokus.hss.main.HSSContainer.<init>(HSSContainer.java:74)
    at de.fhg.fokus.hss.main.HSSContainer.main(HSSContainer.java:110)
[main] ERROR de.fhg.fokus.hss.main.HSSContainer - Exception occurred during starting Tomcat!
Exiting from HSS...
LifecycleException: Protocol handler initialization failed: java.net.BindException: Address already in use (Bind failed):8080
    at org.apache.catalina.connector.Connector.initialize(Connector.java:930)
    at org.apache.catalina.startup.Embedded.start(Embedded.java:794)
    at de.fhg.fokus.hss.main.TomcatServer.startTomcat(TomcatServer.java:128)
    at de.fhg.fokus.hss.main.HSSContainer.<init>(HSSContainer.java:74)
    at de.fhg.fokus.hss.main.HSSContainer.main(HSSContainer.java:110)
root@ubuntu: /opt/OpenIMSCore/FHoSS/deploy#
```

**Figure III.7: Démarrage de FHoSS**

Pour vérifier que le FHoSS est correctement lancée en accédant à l'interface :

<http://192.168.0.254:8080/hss.web.console/>

Maintenant la plateforme est prête pour l'exploitation et tests ce que nous allons le détailler dans le chapitre suivant.

# **Chapitre IV**

## **Test et exploitation de la plateforme OpensourceIMSCore**

## IV.1 Scénario :

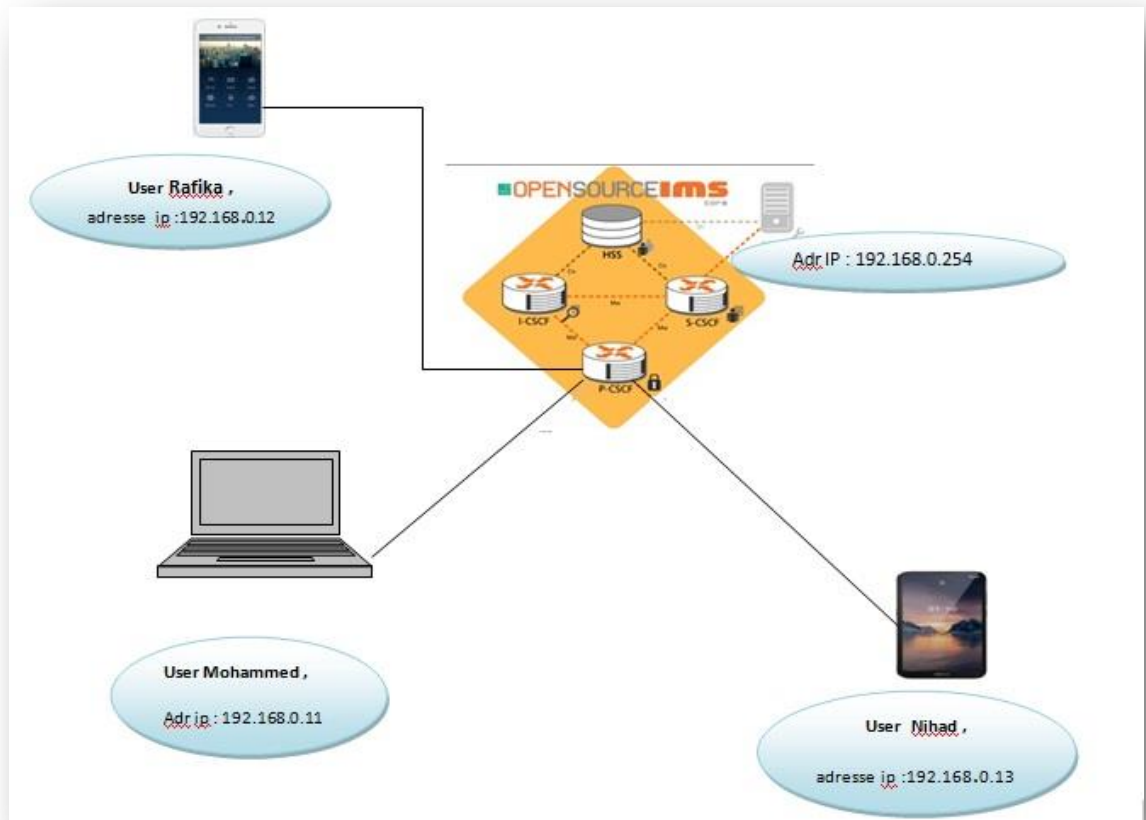


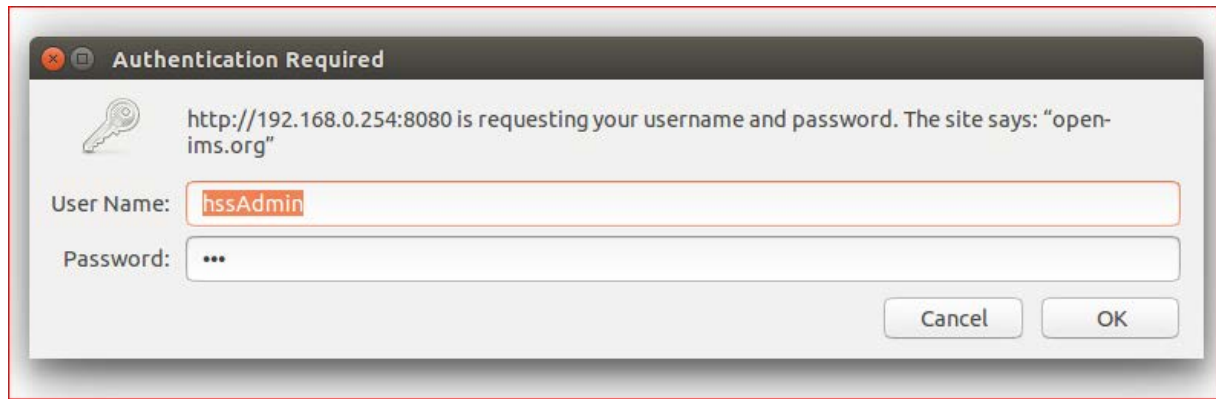
Figure IV.1: Le scénario

## IV.2 Configuration des abonnés IMS:

Après l'installation de l'implémentation open source « Open IMS Core » (de Fraunhofer FOKUS), deux abonnés sont configurés par défauts : Alice & Bob. Ces deux abonnés sont suffisante pour la réalisation de tests.

Nous allons créer 3 utilisateurs : Rafika et Nihad et Mohamed .

- ❖ Accéder à l'interface de contrôle du FHoSS :  
<http://192.168.0.254:8080/hss.web.console/>
- ❖ Login: hssAdmin (pour l'interface d'administration)
- ❖ Mot de passe: hss



**Figure IV.2: interface de connexion au HSS**

Et après aller à l'onglet User Profiles.



**Figure IV.3: page d'accueil de HSS**

Par défaut, FHoSS vient approvisionner avec un couple d'utilisateurs de l'échantillon :

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

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

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

Nous allons commencer par créer une identité publique (IMPU) pour les nouveaux utilisateurs.

- 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 Rafika et NIHAD et Mohamed :

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

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

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

- Sélectionner le service profile par défaut (default\_sp).

Note : Le service profile permet de lier un utilisateur à une liste d'IFC (Initial Filter Criteria).



Grossièrement, ce service profile va donner à un utilisateur les droits d'utiliser un ensemble de services (résolus via des serveurs d'application)[20].

- Cocher la case "Can Register" pour autoriser l'enregistrement d'un abonné (utile avec un serveur de présence).
- Modifier les autres informations comme sur la capture suivante et sauvegarder :

### Public User Identity -IMPU-

ID	12			
Identity*	sip:rafika@open-ims.test			
Barring	<input type="checkbox"/>			
Service Profile*	default_sp			
Implicit Set	12			
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	<input type="text"/>	Add
---------------	----------------------	-----

#### List IMPUs from Implicit-Set

ID	IMPU Identity	Delete
12	sip:rafika@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	<input type="text"/>	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
14	rafika@open-ims.test	<input type="checkbox"/>

#### Push Cx Operation

Apply for	User-Data
Execute	PPR

**Figure IV.4: Public User Identity-IMPU-rafika**

Une fois sauvegardé, nous allons ajouter le réseau open-ims.test à la liste des "Visited-Networks" comme sur la figure précédente.

Note : on remarque sur la capture que l'IMPU est liée à une IMPI; Nous ne pouvons pas faire cette association tout de suite, l'IMPI n'étant pas encore créée. Nous allons donc créer l'IMPI dès à présent et nous reviendrons plus tard sur cette page pour vérifier l'association IMPU/IMPI [20].

○ **Etape 2 : Création d'une IMPI [Private User Identity]:**

Ensuite, nous allons créer une identité privée (IMPI) pour les 3 utilisateurs rafika et nihad et Mohamed.

- Comme précédemment, une syntaxe est à respecté pour l'IMPI: **utilisateur@domaine**. Donc, dans notre cas,

[rafika@open-ims.test](mailto:rafika@open-ims.test) ; [nihad@open-ims.test](mailto:nihad@open-ims.test); [mohamed@open-ims.test](mailto:mohamed@open-ims.test)

- Nous avons choisi une clé secrète pour notre utilisateur (équivalent d'un mot de passe);
- Pour les autres paramètres, on doit réfère à la capture (figure) ci-dessous (laisser par défaut les cases AMF, OP et SQN):

The screenshot shows a web-based configuration interface for a Private User Identity (IMPI) named 'rafika'. The interface is organized into several functional areas:

- Authentication Schemes:** A list of authentication methods with checkboxes. 'All' is selected, and 'Digest-AKAv1-MD5' is set as the default.
- Associate an IMSU:** A section with an 'Add/Change' button for linking an IMSU to the identity.
- Associated IMSU:** A table showing the current association:
 

ID	IMSU Identity	Delete
12	rafika	<input type="checkbox"/>
- Associate IMPU(s):** A section with an 'Add' button and a warning: "Warning: The current IMPU will be associated with all the corresponding IMPUs (within the same implicit-set)".
- List of associated IMPUs:** A table showing the current IMPU association:
 

ID	IMPU Identity	Delete
12	sip:rafika@open-ims.test	<input type="checkbox"/>
- Push Cx Operation:** A section with a dropdown set to 'User-Data' and an 'Execute' button labeled 'PPR'.
- RTR Operation:** A section with a dropdown set to 'IMPU(s) of crt IMPU', a text field containing 'sip:rafika@open-ims.test', and an 'Execute' button with 'RTR-All' and 'RTR-Selected' options.

At the bottom, there are 'Save', 'Refresh', and 'Delete' buttons, along with a note: "Mandatory fields were marked with \*\*".

**Figure IV.5: Private User Identity –IMPI-rafika**

- Une fois sauvegardé, nous allons dans la zone "Associate IMPU(s)" : c'est ici que nous allons pouvoir faire l'association entre l'IMPU et l'IMPI. Saisissez l'IMPU créée à l'étape 1 (pour rappel, dans notre cas "**sip:rafika@open-ims.test**"), puis faite "Add".

Note : Pour revenir sur la note précédente, nous pouvons à présent vérifier l'attachement de l'IMPU créée à l'étape 1 et l'IMPI nouvellement créée.

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

Il est nécessaire à présent de créer une souscription utilisateur, ou IMSU (pour IMS Subscription).

- On choisi un nom pour la souscription ("rafika ;nihad ;mohamed" pour rester cohérent)
- On réfère à la capture d'écran ci-dessous pour les paramètres à renseigner puis sauvegarder:

## IMS Subscription -IMSU-

ID	12	Create & Bind new IMPI +						
Name*	rafika	Associate IMPI(s)						
Capabilities Set	cap_set1	IMPI Identity <input type="text"/> <input type="button" value="Add"/>						
Preferred S-CSCF	scscf1	List of associated IMPIs						
S-CSCF Name		<table border="1"><thead><tr><th>ID</th><th>IMPI Identity</th><th>Delete</th></tr></thead><tbody><tr><td>14</td><td>rafika@open-ims.test</td><td><input type="checkbox"/></td></tr></tbody></table>	ID	IMPI Identity	Delete	14	rafika@open-ims.test	<input type="checkbox"/>
ID	IMPI Identity	Delete						
14	rafika@open-ims.test	<input type="checkbox"/>						
Diameter Name								

Mandatory fields were marked with "\*"

Figure IV.6: IMS Subscription-IMSU-rafika

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

Note : Pour pouvoir sélectionner le "Preferred S-CSCF", il faut d'abord que celui-ci soit créé dans l'onglet "Network Configuration" du FHoSS, ce qui est le cas par défaut lors de l'installation d'openIMSCore [20].

### IV.3 Configuration et Utilisation d'un client IMS:

#### Configuration d'un client IMS sur Windows :

Nous avons utilisé un client BogheIMS pour faire les tests.

Etape 1 : téléchargement de l'application :

- Nous avons télécharger cette application sur le pc :



Etape 2 : Paramétrage

Nous avons lancé le client Boghe IMS client et créer l'utilisateur Mohamed :

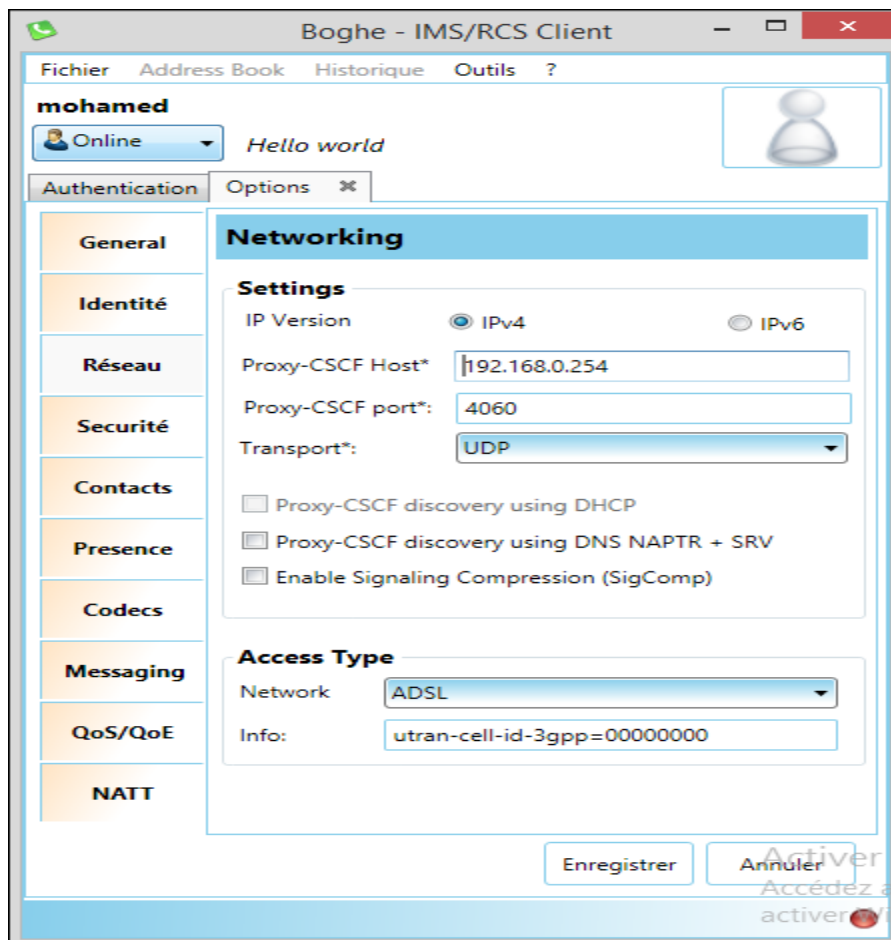
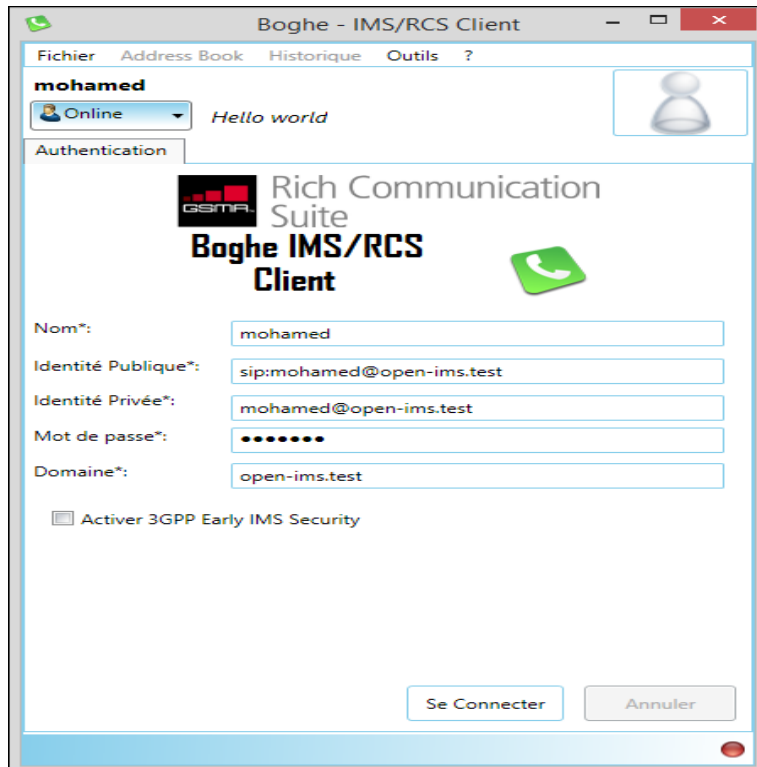
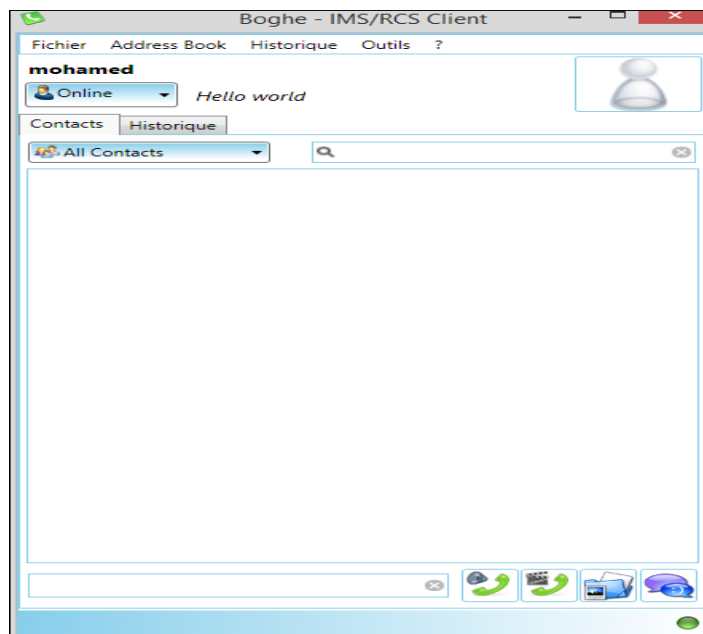


Figure IV.7: config networking IP P-CSCF et le port

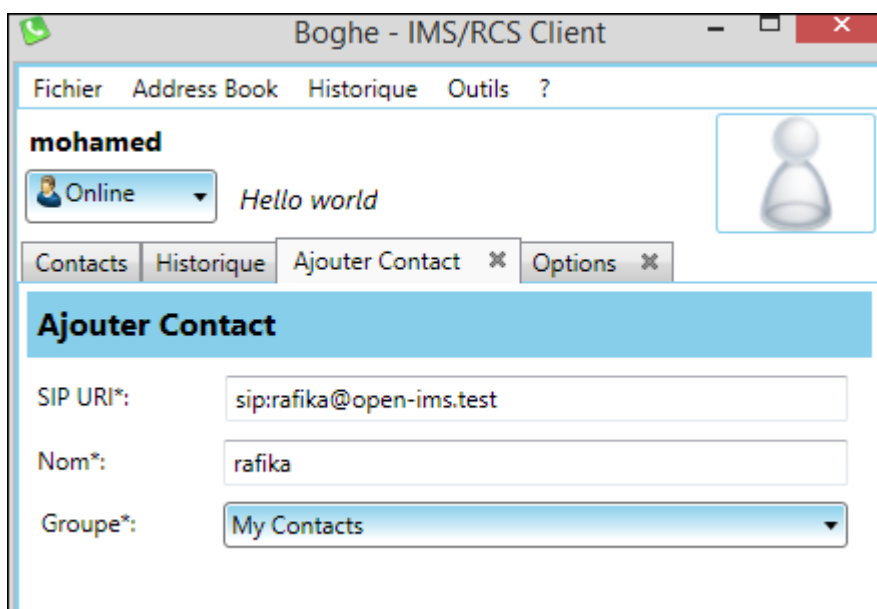


**Figure IV.8: Boghe-IMS client .**

Sur la capture, le point vert signifie que l'utilisateur est enregistré dans l'IMS core et il joignable par contre et le point rouge signifie qu'il n'est pas connecté.

Etape 3 : ajouter de contact :

Nous avons ajouté Rafika et Nihad dans les contacts de Mohamed, pour cela, allez dans le menu contact puis cliquez sur add contact et saisissez les informations sur l'identité de Rafika et Nihad, voir la capture (figure) ci-dessous :



**Figure IV.9: ajouter un contact –rafika**

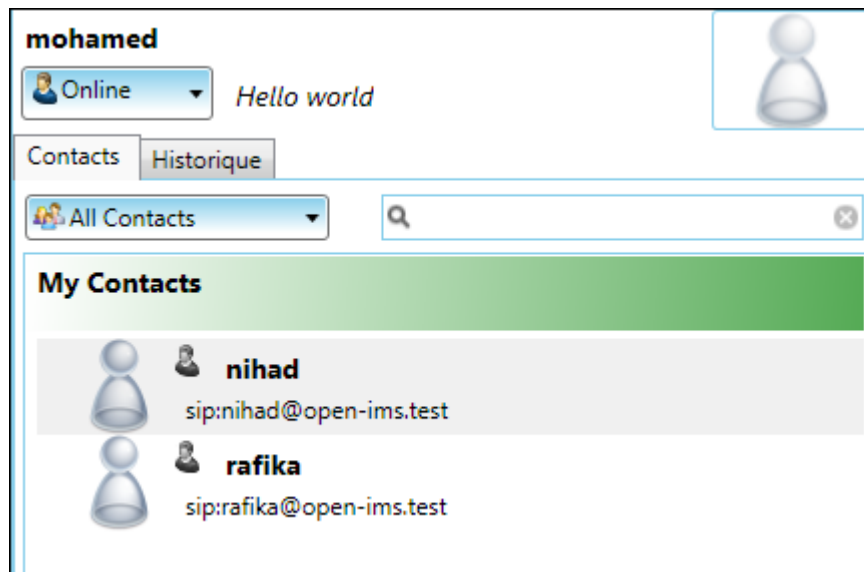


Figure IV.10: Contact de Mohamed

### Configuration d'un client IMS sur smartphone Android :

Nous avons utilisé l'application IMSDroid pour faire les tests.

#### Etape 1 : téléchargement

- Nous avons téléchargé cette application sur le mobile :

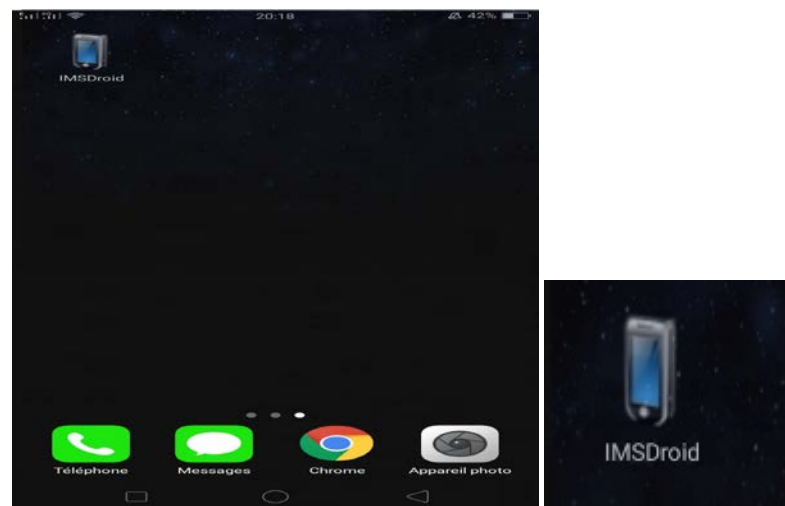
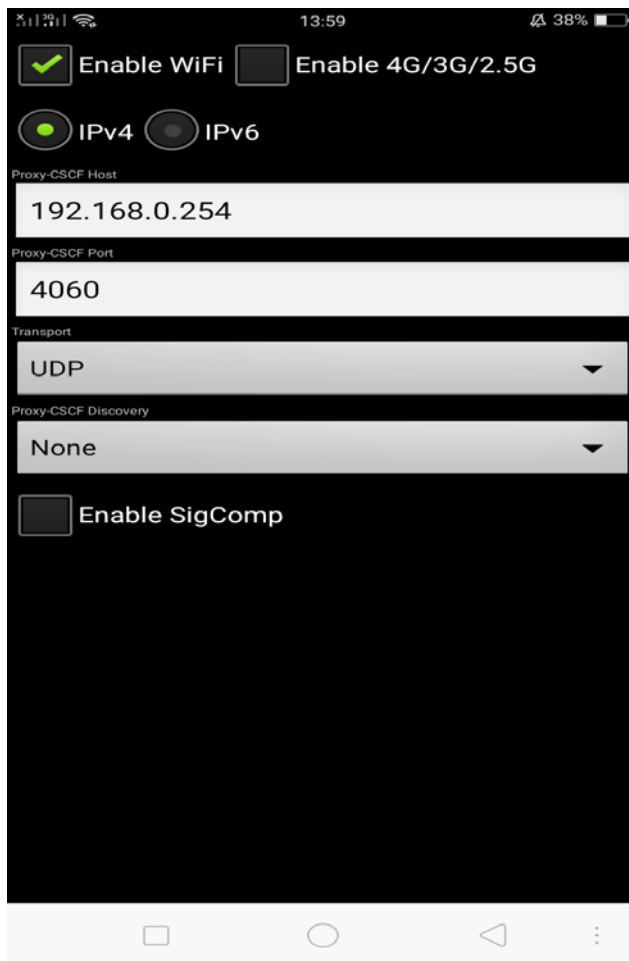
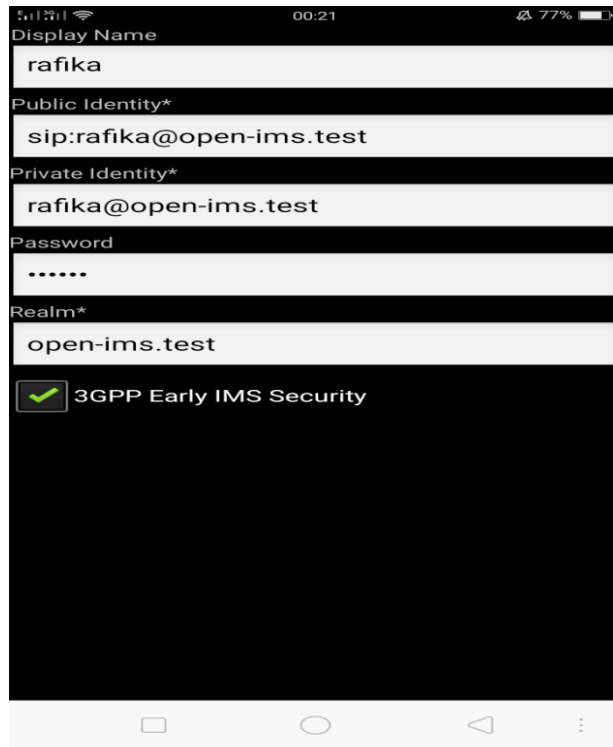


Figure IV.11: IMSDroid

#### Etape 2 : Paramétrage :

Nous avons lancé IMSDroid et créer deux utilisateurs Rafika et Nihad voir les captures :



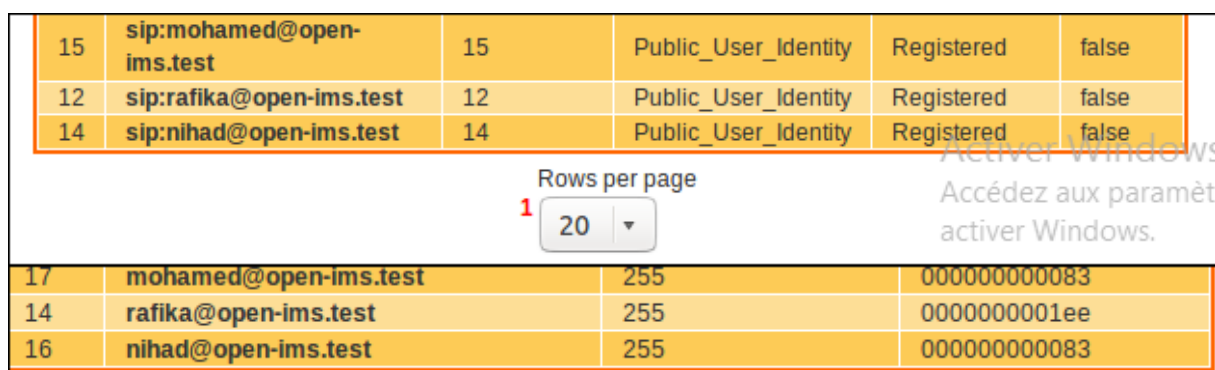
Etape 3 : ajouter de contacts

Nous avons ajouté Nihad et Mohamed dans les contacts de Rafika et c'est pareil pour Nihad.

## IV.4 Test et Fonctionnement :

### IV.4.1 Test d'enregistrement :

Une fois nous avons configuré les users dans les terminaux à savoir Mohamed dans l'application Boghe IMS sous windows et Nihad et Rafika chacune dans des smartphone via l'application IMSdroid , nous remarquons en accédant à l'interface du HSS que ces utilisateurs sont enregistrés dans notre plateforme IMS .



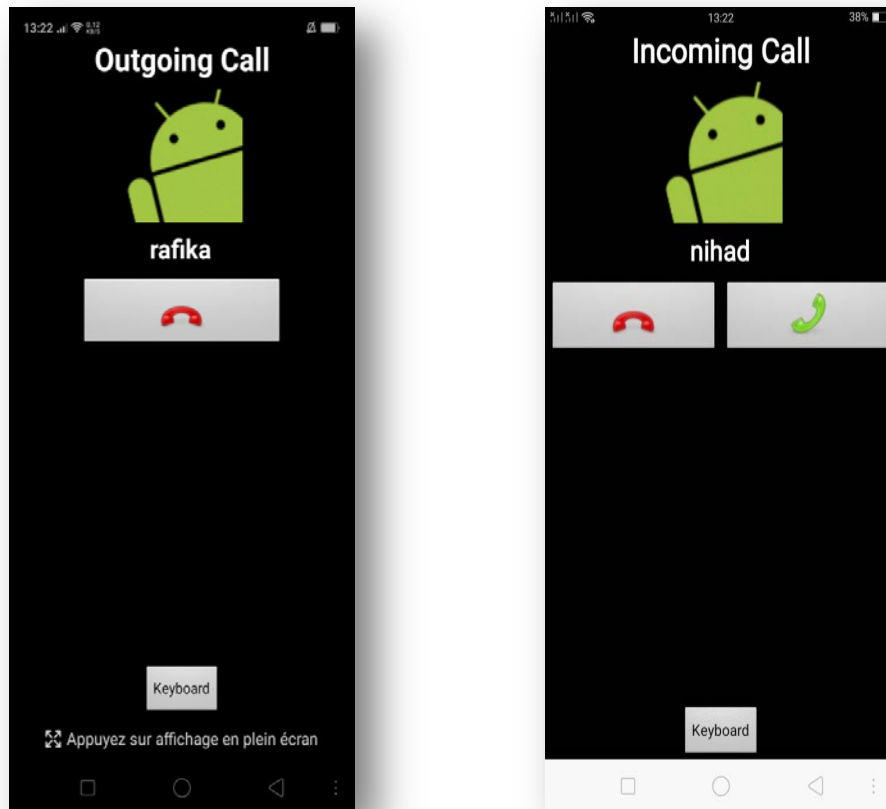
15	sip:mohamed@open-ims.test	15	Public_User_Identity	Registered	false
12	sip:rafika@open-ims.test	12	Public_User_Identity	Registered	false
14	sip:nihad@open-ims.test	14	Public_User_Identity	Registered	false
Rows per page 1 20 ▾					
17	mohamed@open-ims.test	255		000000000083	
14	rafika@open-ims.test	255		0000000001ee	
16	nihad@open-ims.test	255		000000000083	

Figure IV.12: Test d'enregistrement

### IV.4.2 Test d'appel :

On a fait le test d'appel entre les deux utilisateurs Rafika et Nihad. Les captures ci-dessous montrent que les appels (voaux ou vidéo) marchent bien.

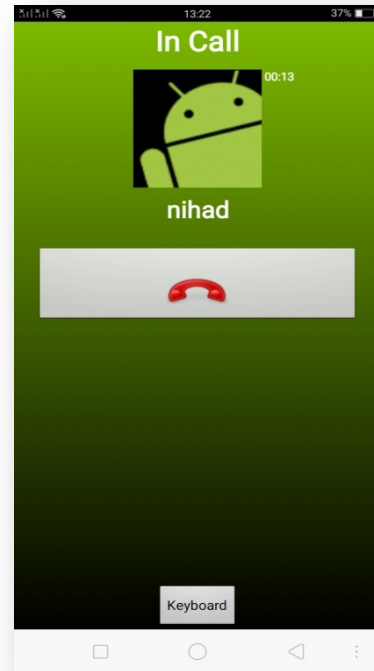
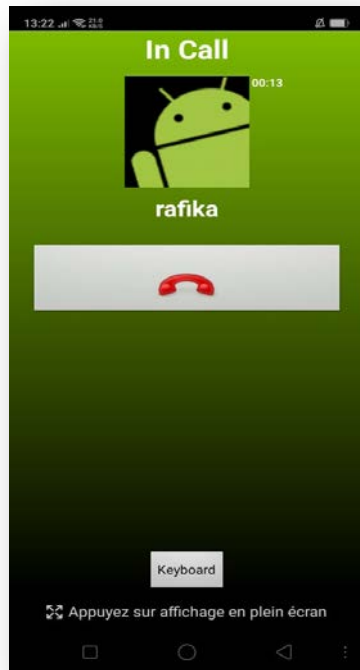




**Figure IV.13: Test d'appel**

Nihad appelle Rafika .

Les captures ci-dessous montrent la communication entre les deux utilisateurs :



Les captures ci-dessous montrent les messages échangés dans la plateforme lors d'une communication audio entre des abonnés (entre les serveurs xCSCF aussi entre les terminaux des users et les serveurs).

Serveur P-CSCF : les clients communiquent avec ce serveur par :

L'adresse du P-CSCF : 192.168.0.254

Le port : 4060

```

root@ubuntu: /opt/OpenIMSCore
<sip:nihad@192.168.0.13:38025;transport=udp>
5(2945) INF:P-CSCF: SR: <sip:orig@scscf.open-ims.test:6060;lr>
5(2945) INF:P-CSCF: NAT:<1://192.168.0.13:38025>
5(2945) INF:P-CSCF: P: D[X] <sip:nihad@open-ims.test>
5(2945) INF:P-CSCF:[ 95] C: <1://192.168.0.12:51807> Exp:[1422] R:[ 1] SOS:[ ]
<sip:rafika@192.168.0.12:51807;transport=udp>
5(2945) INF:P-CSCF: SR: <sip:orig@scscf.open-ims.test:6060;lr>
5(2945) INF:P-CSCF: NAT:<1://192.168.0.12:51807>
5(2945) INF:P-CSCF: P: D[X] <sip:rafika@open-ims.test>
5(2945) INF:P-CSCF:[ 147] C: <1://192.168.0.12:45866> Exp:[ 781] R:[ 1] SOS:[ ]
<sip:rafika@192.168.0.12:45866;transport=udp>
5(2945) INF:P-CSCF: SR: <sip:orig@scscf.open-ims.test:6060;lr>
5(2945) INF:P-CSCF: NAT:<1://192.168.0.12:45866>
5(2945) INF:P-CSCF: P: D[X] <sip:rafika@open-ims.test>
5(2945) INF:P-CSCF:[ 159] C: <1://192.168.0.13:52021> Exp:[1421] R:[ 1] SOS:[ ]
<sip:nihad@192.168.0.13:52021;transport=udp>
5(2945) INF:P-CSCF: SR: <sip:orig@scscf.open-ims.test:6060;lr>
5(2945) INF:P-CSCF: NAT:<1://192.168.0.13:52021>
5(2945) INF:P-CSCF: P: D[X] <sip:nihad@open-ims.test>
5(2945) INF:P-CSCF:----- Registrar Contents end -----
5(2945) INF:P-CSCF:----- Subscription list begin -----
5(2945) INF:P-CSCF:[ 22] P: <sip:rafika@open-ims.test> D:[ 1089] E:[ 1452]
Att:[-1]
5(2945) INF:P-CSCF:[ 106] P: <sip:nihad@open-ims.test> D:[ 1142] E:[ 1451]

```

Serveur S-CSCF : les clients communiquent avec se serveur par :

L'adresse du S-CSCF : 192.168.0.254

Le port : 6060

```
root@ubuntu: /opt/OpenIMSCore
red: [ ]
5(2995) INF:S-CSCF: CCF1: <pri_ccf_address> CCF2: <>
5(2995) INF:S-CSCF: C: <sip:rafika@192.168.0.12:37726;transport=udp> Ex
p:[1633] SOS:[ ]
5(2995) INF:S-CSCF: Path:<sip:term@pcscf.open-ims.test:4060;lr>
5(2995) INF:S-CSCF: UA: <IM-client/OMA1.0 android-ngn-stack/v2.0.481
(doubango r685)>
5(2995) INF:S-CSCF: Param: <+g.3gpp.cs-voice=>
5(2995) INF:S-CSCF: Param: <+g.3gpp.icsi-ref=urn%3Aurn-7%3A3gpp-appli
cation.ims.1ari.gsma-vs>
5(2995) INF:S-CSCF: Param: <audio=>
5(2995) INF:S-CSCF: Param: <+g.oma.sip-im.large-message=>
5(2995) INF:S-CSCF: Param: <+g.3gpp.smsip=>
5(2995) INF:S-CSCF: Param: <language=en,fr>
5(2995) INF:S-CSCF: Param: <+g.oma.sip-im=>
5(2995) INF:S-CSCF: Param: <expires=1700>
5(2995) INF:S-CSCF: S: Event[0] Exp:[1672] <sip:pcscf.open-ims.test:406
0>
5(2995) INF:S-CSCF:[ 106] P: <sip:nihad@open-ims.test> R[ 1] Early-IMS: <> Barr
ed: [ ]
5(2995) INF:S-CSCF: CCF1: <pri_ccf_address> CCF2: <>
5(2995) INF:S-CSCF: C: <sip:nihad@192.168.0.13:44314;transport=udp> Exp
:[1633] SOS:[ ]
5(2995) INF:S-CSCF: Path:<sip:term@pcscf.open-ims.test:4060;lr>
```

Serveur I-CSCF : les clients communiquent avec se serveur par :

L'adresse de l'I-CSCF : 192.168.0.254

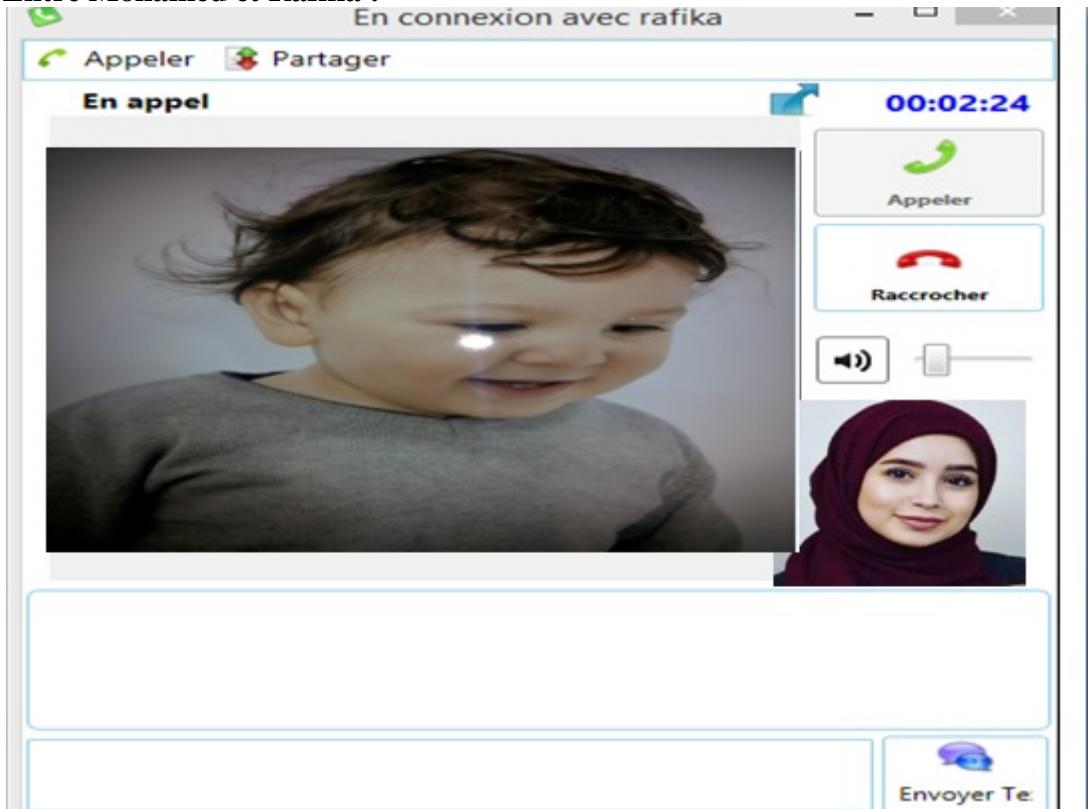
Le port : 5060

```
root@ubuntu: /opt/OpenIMSCore
1(3050) INFO:I-CSCF:Cx_get_server_name: Failed finding avp
1(3050) INFO:I-CSCF:new_scscf_entry: <sip:scscf.open-ims.test:6060>
2(3051) INFO:I-CSCF:Cx_get_result_code: Failed finding avp
2(3051) INFO:I-CSCF:Cx_get_server_name: Failed finding avp
2(3051) INFO:I-CSCF:new_scscf_entry: <sip:scscf.open-ims.test:6060>
3(3052) INFO:I-CSCF:Cx_get_result_code: Failed finding avp
3(3052) INFO:I-CSCF:Cx_get_capabilities: Failed finding avp
3(3052) INFO:I-CSCF:new_scscf_entry: <sip:scscf.open-ims.test:6060>
4(3053) INFO:I-CSCF:Cx_get_result_code: Failed finding avp
4(3053) INFO:I-CSCF:Cx_get_capabilities: Failed finding avp
4(3053) INFO:I-CSCF:new_scscf_entry: <sip:scscf.open-ims.test:6060>
L4(3063) --- Peer List: ---
L4(3063) S[R_Open] hss.open-ims.test:3868 D[ ]
L4(3063) [16777216,10415]
L4(3063) [16777216,4491]
L4(3063) [16777216,13019]
L4(3063) [16777216,0]
L4(3063) [16777217,10415]
L4(3063) [16777221,10415]
L4(3063) -----
4(3053) INFO:I-CSCF:new_scscf_entry: <sip:scscf.open-ims.test:6060>
2(3051) INFO:I-CSCF:new_scscf_entry: <sip:scscf.open-ims.test:6060>
L4(3063) --- Peer List: ---
L4(3063) S[R_Open] hss.open-ims.test:3868 D[ ]
```

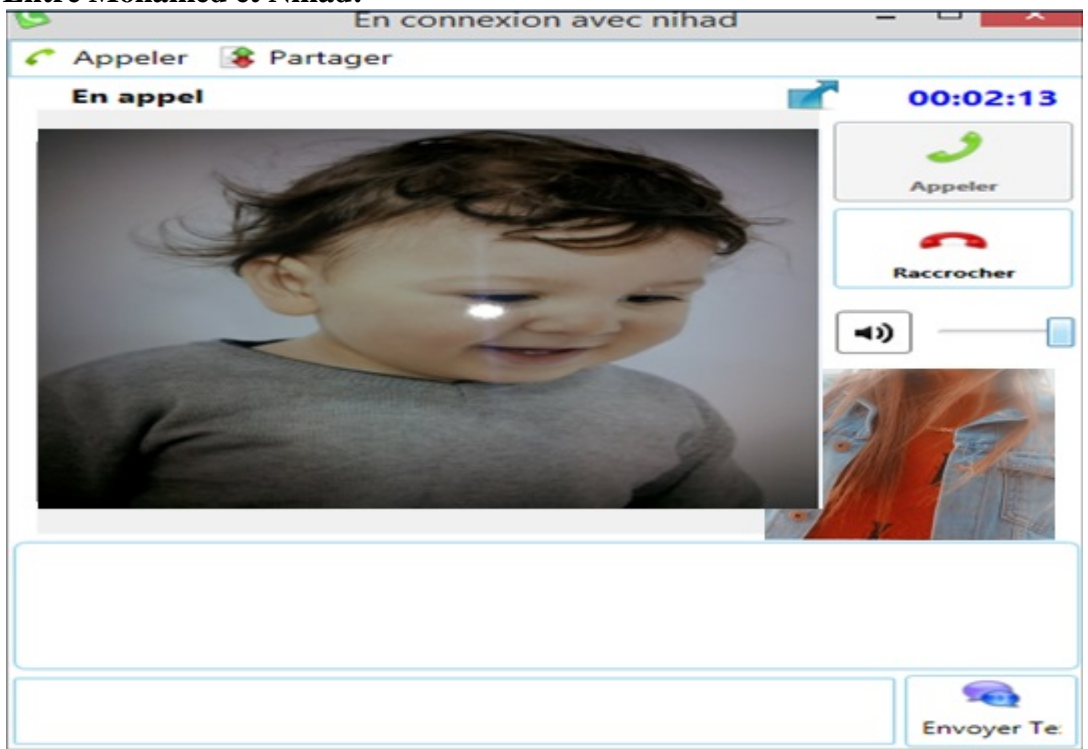
### Appel vidéo :

Le test concernant l'appel vidéo est illustré par les captures suivantes :

- **Entre Mohamed et Rafika :**



- **Entre Mohamed et Nihad:**



### IV.4.3 Test de la messagerie instantanée:

Voici un test de messagerie entre Nihad et Rafika :

1



Figure IV.14: Message de Nihad



**Figure IV.15: Message de Rafika**

## Conclusion générale :

Les experts en télécommunication et informatique considèrent que l'IMS est l'une des clés vers la convergence des réseaux fixes et mobiles, informatiques et télécoms. De ce fait, il a une valeur capitale pour les opérateurs afin de profiter de ces valeurs ajoutées et offrir les services.

La réalisation de ce travail nous a permis de mettre en exergue nos connaissances théoriques dans ce domaine, et aussi comprendre l'architecture de l'IMS et leur couches et les protocoles utilisés (SIP, DAEMON). En plus la compréhension de l'outil OpenIMSCore, l'installation et la configuration d'un cœur de réseau IMS. En exploitant cette plateforme nous avons bien assimilé le principe de fonctionnement d'une plateforme IMS en faisant des tests réels d'appels audio/vidéo et messagerie instantanée entre des abonnés, en même temps nous a permis de voir la traçabilité et le comportement des différents serveurs xCSCF lors de toutes les phases de communications (Enregistrement, signalisation, communication et fin de la communication).

Dans ce travail nous avons réussi à mettre en œuvre une plateforme IMSCore et en même temps comprendre le principe de fonctionnement des autres services AS qui peuvent ajouter tel que IPTV, Serveur de Présence, VOD ...etc

Espérons par ce modeste travail avoir présenté les aspects clés de cette technologie qui est un sujet d'actualité et être utile pour d'autres personnes abordant des sujets pareils.

## **Références :**

- [1]: E. Bertin, N. Crespi, I. Grida Ben Yahia. Next Generation Networks[en ligne].(6 avr. 2018).Disponible sur :<<<<[https://www.researchgate.net/publication/260287419\\_Next\\_Generation\\_Networks](https://www.researchgate.net/publication/260287419_Next_Generation_Networks)>>>> (consulté le 01/03/2020).
- [2]:Med Zakaria ELQASMI.Ingénierie des MSANs (Multi Service Access Node). Ecole marocaine des sciences de l'ingénieur (EMSI) - Ingénieur 2010. Memoire Online > Informatique et Télécommunications.2009/2010.Format PDF :<[https://www.memoireonline.com/05/12/5835/m\\_Ingenierie-des-MSANs-Multi-Service-Access-Node5.html](https://www.memoireonline.com/05/12/5835/m_Ingenierie-des-MSANs-Multi-Service-Access-Node5.html)>.(consulté le 02/03/2020).
- [3]:file:///C:/Users/admin/Desktop/ngn/net\_implementation\_white\_paper0900aec806a7df1.pdf [4]:CISCO IP NGN Carrier Ethernet Design.[en ligne](le 21 août 2017).Disponible sur :<<https://wireless365.wordpress.com/2017/08/21/ip-ngn-carrier-ethernet-design/>>.( consulté le 0 2/03/2020).
- [4]:CISCO IP NGN Carrier Ethernet Design.[en ligne](le 21 août 2017).Disponible sur :<<https://wireless365.wordpress.com/2017/08/21/ip-ngn-carrier-ethernet-design/>>.( consulté le 04/03/2020).
- [5]:Quelles différences entre la fibre jusqu'à l'abonné (FTTH), la fibre à terminaison coaxiale (FTTLA) et la fibre à terminaison cuivre (FTTdp) ?[en ligne](le 16 juin 2020).Disponible sur :<<https://www.echosdunet.net/dossiers/quelles-differences-entre-fibre-ftth-fttla-fttdp>> (consulté le 04/03/2020)
- [6]:FTTH – Fiber To The Home - Fibre jusqu'à l'abonné [en ligne].Disponible sur :<<https://fibre.guide/deploiement/technologies/ftth>>(consulté le 07/03/2020)
- [7]:La quatrième génération des téléphones mobiles 4G (LTE).disponible sur :<<https://sites.google.com/site/bhsidali/home/la-quatrieme-generation-des-telephones-mobiles-4g-lte>> (consulté le 07/03/2020)
- [8]:VU DINH Dau Promotion 13, IFI.Utilisation de la compression des entêtes dans les réseaux cellulaires de type 4G (LTE/SAE) .Mémoire de fin d'études Intégration de RoHC dans l'architecture de LTE Master Informatique, option Systèmes et Réseaux.FRANCE .September, 2009 .disponible sur :<<<<<https://wikimemoires.net/2013/07/la-compression-des-entetes-dans-les-reseaux-cellulaires-de-type-4g;Mémoire>>>>>. nous avons pris de ce partie :Évolution LTE, Architecture de LTE et Interface radio[en ligne].(le19 juil. 2013).Disponible sur :<<<<<https://wikimemoires.net/2013/07/evolution-lte-architecture-de-lte-et-interface>>>>>.(consulté le 08/03/2020)
- [9]:Yazid KARKAB.Les Réseaux IP/MPLS .l'UFR Ingénieurs 2000 de l'Université Paris Est-Marne la vallée.Disponible sur :<<<<[http://igm.univ-mlv.fr/~dr/XPOSE2007/karkab MPLS/glossary.html](http://igm.univ-mlv.fr/~dr/XPOSE2007/karkab/MPLS/glossary.html)>>>> (consulté le 10/03/2020)



- [10]: Alasdair Gilchrist .What is IP/MPLS?[en ligne].(le 10 Mars 2019) .Disponible sur :<<https://www.virtualhostedpbx.net/what-is-ipmpls/>>.(consulté le 11/03/2020)
- [11]: Mattieu Baptiste et Fabien Vincent.Définition d'un réseau VPN BGP / MPLS et des entités collaboratrices.2008. Disponible sur :<<https://www.brimbelle.org/mattieu/projects/bgpmpls/etat-art.htm>>(consulté le 11/03/2020)
- [12]: Définition /VPN/Futura Tech -Futura-Sciences.Disponible sur :<<https://www.futura-sciences.com/tech/definitions/connection-vpn-1819/>> .(consulté le 12/03/2020)
- [13]: Ivan Pepeljak .Tutoriel BGP : Comprendre le protocole de routage qui fait fonctionner Internet (1/2).(le 11 déc 2017).Disponible sur :<<https://www.lemagit.fr/conseil/Tutoriel-BGP-Comprendre-le-protocole-de-routage-qui-fait-fonctionner-Internet-1-2.>>.(consulté le 15/03/2020)
- [14]: Simon ZNATY et Louis DAUPHIN.Architecture NGN: Du NGN Téléphone au NGN Multimédia .2005 Disponible sur :<[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwji49avn9zqAhUnx4UKHUO3CqgQFjAMegQIBBAB&url=http%3A%2F%2Fwww.efort.com%2Ffr\\_tutoriels%2FNGN\\_EFORT.pdf&usq=AOvVaw1nj9I5A-HVBAX8yG2yclpk](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwji49avn9zqAhUnx4UKHUO3CqgQFjAMegQIBBAB&url=http%3A%2F%2Fwww.efort.com%2Ffr_tutoriels%2FNGN_EFORT.pdf&usq=AOvVaw1nj9I5A-HVBAX8yG2yclpk)> (consulté le 15/03/2020)
- [15]: La convergence fixe-mobile A Way To IMS. 2008.Disponible sur : <<<<<https://www.ims-way.com/about/convergence-fixe-mobile/>>>>>.(consulté le 20/07/2020 )
- [16]: L'IMS, l'avenir de la téléphonie .Christophe Ravelingien Technology Manager chez Telenet.[en ligne].Disponible sur :<<https://www2.telenet.be/fr/business/inspiration/ims-l-avenir-de-la-telephonie/>> .(consulté le 15/03/2020)
- [17] : Cuiting Huang, N. Crespi, Enriched SCIM for Service Composition within IMS Environment, in: Management and Service Science, September 2009.(consulté le 19/03/2020).
- [18] : M. Tadault, S. Soormally, and L. Thiebault, Network evolution towards IP multimedia subsystem, Alcatel, 2003.(consulté le 19/03/2020).
- [19] : 3GPP, Overview of 3GPP Release 5 – Summary of all Release 5 Features, in: ETSI Mobile Competence Centre, June 2003.(consulté le 19/03/2020).
- [20]: IMS-Way -Au sujet d'IMS /AWay To IMS [en ligne ].(mise à jour le 10 Avril 2011) .Disponible sur : <[https://www.ims-way.com/about/what-is-ims/#:~:text=IMS%20est%20une%20architecture%20fonctionnelle,les%20r%C3%A9seaux%20fixes%20et%20mobiles.&text=Il%20est%20%C3%A9galement%20%C3%A0%20noter,Engineering%20Task%20Force%20\(IETF\).](https://www.ims-way.com/about/what-is-ims/#:~:text=IMS%20est%20une%20architecture%20fonctionnelle,les%20r%C3%A9seaux%20fixes%20et%20mobiles.&text=Il%20est%20%C3%A9galement%20%C3%A0%20noter,Engineering%20Task%20Force%20(IETF).>)> .(consulté le 22/03/2020).

[21]: L'IMS, Architecture et Protocoles ... Ainsi, originellement conçu pour les réseaux cellulaires, L'IMS, considéré par British Telecom comme le réseau du 21ème [en ligne].(mise à jour le 10/07/2020) Disponible sur :<<<<<<<<<<http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2007-ttnfa2008/Caffier-Delamare/Objectifs.html>>>>>>>>>> (consulté le 22/03/2020).

[22]: Camarillo, Gonzalo; García-Martín, Miguel A. (2007). Le sous - système multimédia IP 3G (IMS): Internet et fusion des mondes cellulaires (2 ed.). Chichester [ua]: Wiley [en ligne].In : IP Multimedia Subsystem - IP Multimedia Subsystem.Disponible sur : <[https://fr.qwe.wiki/wiki/IP\\_Multimedia\\_Subsystem](https://fr.qwe.wiki/wiki/IP_Multimedia_Subsystem)> . (consulté le 22/073/2020) .

[23]: Gaëtan BOIVIN .exposé sur la technologie IMS effectué en 3e année d'école d'ingénieur : Ingénieurs 2000. Disponible sur : <<<<<<<<<<<http://igm.univ-mlv.fr/~dr/XPOSE2010/IMS/definition.html#:~:text=IMS%20est%20une%20architecture%20de,filaires%20qu'aux%20r%C3%A9seaux%20mobiles>>>>>>>>>>>. (Consulté le 22/03/2020).

[24] : M.MOHAMED MAACHAOUI .Securite et performances pour les reseaux de nouvelle generation (NGN) .Thèse de Doctorat de L'université de TOULOUSE .Institut National polytechnique de Toulouse (INP) .le Vendredi 12 juin 2015 .183p (Consulté le 22/03/2020).

[25] : YUAN ZHANG .Network Framework of IMS.China Telecom Beijing Research Institute. Department: Chinatelecom Beijing Research Institute. 33 page .Format Power Point sur :

<file:///C:/Users/admin/Desktop/ngn/chapitre%203%20ngn/Session%203-2%20Framework%20of%20IMS%E5%BC%A0%E5%9B%AD.pdf> . (consulté le 24/03/2020) .

[26]:M. Hermann Orly GBILIMAKO ,Etude et mise en place d'une plateforme IMS sécurisée.Mémoire de fin de cycle pour l'obtention du master professionnel,Option : Réseaux Télécommunication .Institut Supérieur d'Informatique .SENEGAL .2014-2015.93 page .Format PDF sur :<<https://fr.slideshare.net/orly-hermann/etude-et-mise-en-place-dun-plateforme-ims-scurise>>.(Consulté le 24/03/2020).

[27]:Réseaux cellulaires et téléphonie.Réf .Internet:42288/2ème édition :Denis MISCHLER, Bastien LAMER.ETSI TISPAN - Standardisation du NGN IMS pour les réseaux fixes.In:Techniques de L'ingénieur .10 mai 2010.Réf : TE7602 v1.Disponible sur :<<https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/reseaux-cellulaires-et-telephonie-42288210/etsi-tispan-te7602/>>.(consulté le 27/03/2020)

[28]:NAOUI KHALED ,BENAHMED SIDALI .Etude et mise en place de la solution VOIP over LTE, dimensionnement et mesure de la QoS .Mémoire de master :Sciences et Technologie,Filière :Télécommunication.université des Sciences et de la Technologie Houari Boumediene .2014-2015.62 p (Consulté le 28/04/2020).

- [29]: Architecture IMS/ A Way To IMS -A Way To IMS [en ligne].(mise à jour le 14 juil 2020).Disponible sur <<https://www.ims-way.com/about/what-is-ims/architecture-ims/>>. (consulté le 29/04/2020 ).
- [30] : MROUEH Lina et LABAKY Elie. Etude des procédures d'enregistrement et d'établissement de session en IMS. Télécom Paris école nationale supérieurs des télécommunications .15 Avril 2006. 39 pages. Disponible sur : <http://perso.isep.fr/mroueh/docs/IMS.pdf>.( consulté le 15/06/2020 ).
- [31] : [https://www.memoireonline.com/01/17/9512/m\\_Deploiement-dun-serveur-streaming-m-learning-dans-un-reseau-UMTS16.html](https://www.memoireonline.com/01/17/9512/m_Deploiement-dun-serveur-streaming-m-learning-dans-un-reseau-UMTS16.html) (consulté le 19/06/2020)
- [32]:Le protocole SIP :contexte,protocole,analyse et mise en oeuvre .[en ligne](mise à jour le 16 juil 2020) .Disponible sur :<<<<<<<<https://sip.goffinet.org/sip-01-architecture/>>>>>>>>. (consulté le 10/07/2020)
- [33]:Julien Barisoux et Jordan Gourong .Le protocole SIP ,De H.323, SIP ou H325, quel protocole s'imposera ?.[en ligne].Disponible sur :< <https://wapiti.imt-lille-douai.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesser2010-ttnfa2011/barisoux-gourong/SIP.html> >. (consulté le14/07/2020 )
- [34]:ADDA Zahia,BELGAID Hanane .Etude et Configuration du protocole(SIPTG) dans la téléphonie IP.Mémoire de fin d'étudesDe MASTER ACADEMIQUE Domaine: Sciences et TechnologiesFilière: Génie électriqueSpécialité: Réseaux et Télécommunication. 2014/2015.85 p . Format PDF sur : <<<<<<<[https://dl.ummtto.dz/bitstream/handle/ummtto/6545/AddaZahia\\_BelgaidH.pdf?sequence=1](https://dl.ummtto.dz/bitstream/handle/ummtto/6545/AddaZahia_BelgaidH.pdf?sequence=1)>>>>>>>. (consulté le 19/07/2020 ).
- [35]Mame Gracé SECK ,Djibril SAMBE ,Emeric KAMLEU .Projet SIgnalisation NGN/IMS : Protocole Diameter et Scenario de Traitement D'appel .Ecole Supérieur Multinationale des Télécommunication .le 2009/2011 .Disponible sur :<<<<<<<<https://fr.slideshare.net/kml29/protocole-diameter>>>>>>>>. (Consulté le 19/07/2020)
- [36]:Open IMS Core - IMS Project - [en ligne].Disponible sur :<<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjIg-vnrpHrAhWBxIUKHT46DHIQFjAAegQIBRAB&url=https%3A%2F%2Fsites.google.com%2Fsite%2Fimssagemst%2Fopen-ims-core&usg=AOvVaw2ojVWmQ6w-Kv0ourjG5ns7>>. (consulté le 01/08/2020)
- [37]:Yanko Antonio Marín Muro.OPENIMSCORE PRACTICE GUIDE.Universidad Central "Marta Abreu" de las Villas · Faculty of Electrical Engineering.Presentation · January 2017.Disponible Format PDF sur :< <https://www.researchgate.net/publication/325931179> >. (consulté le 10/08/2020).
- [38]:Installation de O.I.C- IMS Project - .[en ligne](mise à jour le 04/08/2020).Disponible sur :< <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiDy4nR3ZHrAhWR3oUKHbqUD2cQFjADegQIBhAB&url=https%3A%2F%2Fsites.google.com%2Fsite%2Fimssagemst%2Finstallation&usg=AOvVaw0Y9VETrnKt2tedVVbLVFrp> >. (consulté le 10/08/2020)