الجـمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et publique

وزارة التعليم الـعـالي و البحـث العـلمـي
Ministère de l'enseignement supérieur et de la recherche scientifique

جـامعة سعد دحلب البليدة 1
Université SAAD DAHLAB BLIDA 1

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Projet de Fin d'études

Filière Télécommunication
Spécialité Systèmes de Télécommunication

Présenté par

ADDA ABBOU ABDELKADER

La Voix sur LTE

Encadré par: **Dr. Hocine AIT SAADI**.
&
Co-encadré par**: Mr. Khalil LAIREDJ.**

Année Universitaire 2019-2020

Résumé

Le système de communication mobile 4G LTE est la norme retenue ces dernières années par l'association 3GPP pour les communications radio mobiles, il utilise une infrastructure IP complète (de bout en bout) en substitution à l'ancienne technologie à base de commutation de circuits CS (Circuit Switched) par le recours au routage de paquets IP (Packet Switch) dans son réseau cœur EPC (Evolved Packet Core).

Cette évolution a posé un problème aux opérateurs pour prendre en charge le service vocal en 4G LTE sans dépendre de leurs anciens réseaux 2G et 3G.

3GPP et GSMA (GSM Association) ont remédié à ce problème en adoptant une solution intéressante qui permet la prise en charge de la voix sur IP (VoIP) et la mise en œuvre d'une infrastructure IMS (IP Multimedia Subsystem) qui offre un service vocal tout en se connectant au réseau LTE, nous appelons cela "VoLTE ".

Par conséquent, la VoLTE est clairement l'avenir des communications vocales du fait qu'elle soit à base d'IP et compatible avec les réseaux NGN (fixe et mobile), comme elle peut également assurer une très bonne QoS (Quality of Service) car le paquet IP a été conçu pour prendre en charge un débit de données élevé.

Notre contribution dans ce mémoire a consisté à simuler un réseau IMS avec ses composants de base à travers le déploiement d'une plateforme "OpenIMSCore" basée sur des solutions Opensource.

Cette plateforme a servi comme banc d'essai pour la simulation de certaines fonctionnalités nécessaires à l'établissement de toute session multimédia à savoir la configuration et l'enregistrement des utilisateur IMS.

Elle a aussi servi au lancement de tests d'échange de flux de signalisations SIP et d'établissement de sessions multimédia (service voix et message SMS) entre deux utilisateurs IMS .

Abstract

4G Mobile communication system LTE adopted by 3gpp (3d generation partnership project) standard for Radio communications, uses a full IP infrastructure and replace the older CS (Circuit Switched) systems by using only PS (Packet switched) in its EPC (Evolved Packet Core).

This evolution posed a problem for operators to support Voice service in 4G LTE without depending on their 2G and 3G networks. 3GPP and GSMA (GSM Association) have remedied this problem by adopting an interesting solution that allows support for voice over IP (VoIP) and the implementation of an IMS infrastructure (IP Multimedia Subsystem) that offers a service voice while connecting to the LTE network, we call this "VoLTE".

Therefore, VoLTE is clearly the future of voice communications since it is over IP and it is compatible with NGN networks (fixed and mobile), also it can ensure a very good QoS (Quality of Service) because IP packet was designed to support high data throughput.

Our contribution in this thesis consisted in simulating an IMS network with its basic components through the deployment of an "OpenIMSCore" platform based on Opensource solutions.

This platform served as a testing ground for the simulation of certain functionalities necessary for the establishment of any multimedia session, namely the configuration and registration of IMS users.

It was also used to launch tests for exchanging SIP signaling flows and establishing multimedia sessions (voice and SMS message services) between two IMS users.

ملـــخَّـــص

نظام اتِّصالات الجيل الرَّابع للهاتف المحمول هو أحدَث معيار للاتِّصالات اللَّاسلكيَّة عبر ذبذبات الرَّاديو، إذ أنَّه يستخدم بروتوكول الأنترنت بصفة كاملة في البنية الأساسية و يمحي كلَّ استعمال لتحويل الدَّوائر الكهربائيَّة التقليديَّة باستعمال تحويل الحزمات فقط في لبِّ شبكته المتطوِّر.

هذا التطوُّر طرح مشكلة بالنِّسبة للمتعاملين لدعم خدمة الصَّوت في الجيل الرَّابع دون الاعتماد على شبكات الجيل الثَّاني و الثَّالث الخاصَّة بهم، 3GPP و GSMA قاموا بعرض حلٍّ رائع لدعم خدمة الصَّوت عبر بروتوكول الأنترنت و هذا عبر وضع بنية نظام بروتوكول الأنترنت، التي تمنح خدمة الصَّوت و تصل شبكة الجيل الرَّابع بها، نسمِّي هذه التِّقنية بـــ" الصَّوت عبر تقنيَّة الجيل الرَّابع".

و بالتَّالي يبدو واضحا أنَّها مستقبل الاتِّصالات الصَّوتية بما أنَّها عبر بروتوكول الأنترنت و متوافقة مع شبكات الجيل القادم في الهاتف الثابت، أيضا هذه التِّقنية باستطاعتها ضمان جودة خدمة جيِّدة لأنَّ في الأساس حزمات بروتوكول الأنترنت صمِّمت لدعم تدفُّق عالي للبيانات.

تتمثل مساهمتنا في هذه المذكرة في محاكاة شبكة IMS بمكوناتها الأساسية من خلال نشر منصة "OpenIMSCore" على أساس حلول مفتوحة المصدر. عملت هذه المنصة كمنصة اختبار لمحاكاة بعض الوظائف اللازمة لإنشاء أي جلسة وسائط متعددة، و هي تهيئة و تسجيل مستخدمي IMS.

كما تم استخدامه لإطلاق اختبارات لتبادل تدفقات إشارات SIP و إنشاء جلسات الوسائط المتعددة (خدمة الرسائل الصوتية و الرسائل النصية القصيرة) بين اثنين من مستخدمي IMS.

Table des matières

Liste des Figures

Liste des Tableaux

Listes des acronymes et abréviations

3GPP	Third Generation Partnership Project
BGCF	Breakout Gateway Control Function
CS	Circuit Switched
CSFB	Circuit Switched Fall Back
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
ETSI	European Telecommunications Standards Institute
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
I-CSCF	Interrogating Call Session Control Function
IMS	IP Multimedia Subsystem
LTE	Long Term Evolution
MGCF	Media Gateway Control Function
MME	Mobility Management Entity
MIMO	Multiple Input Multiple Output
MRF	Media Resource Function
MSC	Mobile-Switching Centre
OFDMA	Orthogonal Frequency-Division Multiple Access
PCRF	Policy Control and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDN	Packet Data Network
PS	Packet Switched
QCI	QoS Class Identifier
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
QAM	Quadrature Amplitude Modulation
RRC	Radio Resource Control
RTP	Real-time Transport Protocol
S-CSCF	Serving Call Session Control Function
SGW	Serving Gateway
SIP	Session initial protocol
SDP	Session Description Protocol
UA	User Agent
UAA	User-Authorization-Answer
UAC	User Agent Client
UAR	User-Authorization-Request
UAS	User Agent Server
URI	Uniform Resource Identifier
VoLGA	Voice over LTE via Generic Access
VANC	VoLGA Access Network Controller
VoLTE	Voice over LTE

Remerciements

Je voudrais tout d'abord adresser toute ma gratitude à mon encadreur **Dr. Hocine AIT SAADI,** pour m'avoir soutenu et encouragé par sa disponibilité et surtout ses conseils, qui ont contribué à alimenter et enrichir ma réflexion.

Mes remerciements vont aussi à tous mes enseignants du département électronique pour le niveau et la qualité de la formation qu'ils m'ont prodigué durant tout le semestre.

Je remercie également Messieurs le président et les membres de jury pour l'honneur qu'ils m'ont fait d'examiner et évaluer mon travail et d'assister à ma soutenance.

Je tiens à remercier chaleureusement **Mr. Khalil LAIREDJ**, pour son soutien et ces précieux conseils.

Ma reconnaissance à Madame Hind Mesbah, Sous directrice à l'ANF pour toute l'aide et le soutien apportés durant toute l'année.

Je ne termine sans exprimer toute ma reconnaissance à Mr. le DG de l'ANF pour m'avoir autorisé et aidé à mener à bien ce travail modeste soit-il.

En dernier mais pas le moindre, je remercie ma précieuse famille pour leurs véritables soutiens sans lesquels je ne serais à ce niveau.

Introduction Générale

Les télécommunications radio-mobiles n'ont cessé de se développer, de la première génération, qui a utilisé des systèmes analogiques à la quatrième génération (et bientôt la cinquième), qui utilisent bien entendu des systèmes numériques.

En Algérie, les opérateurs mobiles ont commencé à installer la 4G LTE, ce qui constitue une nouveauté, car il offre de multiples nouveaux services, un débit de données plus élevé comparé au 3G UMTS et une capacité de réseau plus élevée. Cette amélioration de la capacité provient de l'utilisation de nouvelles techniques et de nouveaux algorithmes de planification permettant aux utilisateurs de se partager des ressources fréquentielles sur un spectre plus large, en limitant les interférences par l'utilisation sur la liaison descendante, de la technique de multiplexage fréquentiel OFDMA.

La mise en œuvre de la communication radio sans fil mobile et la standardisation du GSM par 3GPP devaient soutenir la communication vocale entre les utilisateurs du monde entier et assurer la compatibilité.

Le service vocal à côté du SMS n'a pas connu de développement lorsque 3GPP a lancé la 3G UMTS en 1999, car il utilisait toujours des systèmes à commutation de circuits CS pour la prise en charge de la voix, et cela pour des raisons de rentabilité économique pour les opérateurs car ils n'ont pas abandonné la structure CS de leur réseau central 2G, et également pour des raisons de compatibilité technique avec les réseaux fixes qui continuaient à être à commutation de circuits.

Contrairement aux générations précédentes, la 4G LTE n'inclut pas de domaine à commutation de circuits car son réseau cœur ne prend en charge que les paquets commutés avec une architecture IP complète, il continue néanmoins à compter sur des réseaux 3G ou 2G pour prendre en charge le service vocal, ce qui constitue un paradoxe du fait que chaque réseau doit prendre en charge ses services par lui-même.

D'autre part, les réseaux fixes par leur migration vers l'architecture NGN (réseaux de prochaine génération) n'utilisent plus de CS dans 80% des pays du monde. La voix est désormais intégrée dans leurs services basés sur IPv4 puis IPv6 récemment, c'est ce que

nous appelons dans la suite de notre projet la VoIP ou voix sur IP. En Algérie, le projet MSAN (Multiple Service Access Node) s'inscrit dans ce cadre.

C'est justement cette convergence des réseaux aussi bien fixes que mobiles vers le tout IP qui motive le choix de notre sujet pour étudier le service vocal sur LTE (VoLTE) en utilisant l'infrastructure IP.

Notre projet est structuré en quatre (4) chapitres comme suit:

Le premier chapitre est consacré aux technologies mobiles apparues avant la 4G LTE, des technologies 1G les plus connues à la 2G GSM standard et enfin la 3G UMTS standard.

Le deuxième chapitre porte sur le fonctionnement de la 4G LTE, de son architecture et de sa solution de prise en charge de la voix à côté du GSM et de l'UMTS.

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

Le quatrième chapitre est relatif à la simulation d'une plate-forme IMS avec analyse de ses fonctionnalités.

Chapitre I:

Avant la 4G LTE

Chapitre I: Avant la 4G-LTE

I-1) Introduction

Chaque année, la communication radio mobile devient de plus en plus importante dans notre vie, ce qui explique son développement rapide et l'intérêt qu'elle suscite. Elle est aussi à l'origine de la succession de ce que nous appelions les générations mobiles (1G, 2G, 3G, 4G et maintenant la 5G).

En raison de la demande du marché, la bande passante et la capacité étaient les principales parties à développer d'où le recours à d'autres méthodes d'accès et de moyens pour une plus grande efficacité spectrale.

La première génération a connu plusieurs normes, la nécessité d'unifier une norme internationale apparaît très rapidement et conclut avec GSM comme la norme internationale de 2e génération.

Après cela, l'UMTS a été normalisé en 3G et évolué par la suite en 4G LTE. Notre objectif dans ce chapitre est de décrire l'évolution des réseaux mobiles d'une génération à une autre et de comprendre comment le service vocal a été géré et développé dans chaque génération, car cela sera très utile pour comprendre la voix sur LTE ou VoLTE dans les chapitres à venir.

I-2) Réseaux radio-mobiles de première génération

Comme mentionné dans l'introduction, la 1ère génération a eu plusieurs normes partout dans le monde, l'incompatibilité et le prix élevé des communications induit ont donc constitué le principal handicap. le tableau ci-dessous décrit les normes de 1ère génération les plus connues dans le monde.

Le principal développement technologique qui a distingué les téléphones mobiles de première génération de la génération précédente a été l'utilisation de plusieurs sites cellulaires et la possibilité de transférer des appels d'un site à un autre pendant que l'utilisateur voyageait entre les cellules pendant une conversation.

Standard	Utilisation	Technologie
Advanced Mobile Phone System (AMPS)	Amérique du Nord, 1980	Cellulaire, analogique, FDMA.
Total Access Communication System (TACS)	UK, 1983	Cellulaire, analogique, FDMA.
Nordic Mobile Telephone (NMT)	Suède, Russie,1 octobre 1981	Cellulaire, analogique, FDMA.
The Radio Telephone Network C	Allemagne, 1985	Cellulaire, analogique, FDMA, Roaming.

Tableau I-1: Les normes de première génération.

I-3) Le réseau radio mobile de deuxième génération

Au début des années 90, le GSM Système mondial de communications mobiles a déclenché un changement sans précédent dans la façon dont les gens communiquent entre eux. Alors que seules quelques personnes utilisaient des systèmes sans fil analogiques antérieurs, plus de 5 milliards d'abonnés dans le monde en 2014 utilisent le GSM.

Cela a été principalement réalisé par les améliorations constantes dans tous les domaines de la technologie des télécommunications et les réductions de prix qui en résultent pour les équipements d'infrastructure et les appareils mobiles **[1]**.

La désignation GSM (Global System for Mobile Communications) combine deux types de réseaux de télécommunications cellulaires numériques pour les abonnés mobiles:

• Le réseau GSM900: il utilise des fréquences porteuses dans la gamme 900 MHz et a été le premier type de réseau mobile cellulaire européen mobile.

• Le DCS1800 (Digital Cellular Telecommunications System): qui utilise des fréquences porteuses dans la gamme 1800 MHz.

Les réseaux GSM/DCS fournissent des services de télécommunications au public avec une couverture continue sur une large zone.

Cette disponibilité du service est obtenue par la localisation automatique de la station mobile et par des accords d'itinérance entre opérateurs **[2]**.

I-3-1) L'Architecture GSM:

Le réseau mobile GSM comprend deux composants principaux, l'infrastructure fixe installée (réseau) et les abonnés mobiles qui utilisent les services de ce réseau.

Le réseau fixe installé peut à nouveau être subdivisé en trois sous-réseaux: réseaux d'accès radio, réseau de commutation mobile et réseau de gestion. Ces sous-réseaux sont appelés sous-systèmes. Les trois sous-systèmes respectifs sont:

-Sous-système de station de base (BSS);

-Sous-système NSS (Network Switching Subsystem);

-Sous-systèmes d'exploitation et de maintenance OMSS (Operation and Maintenance Subsytem) **[3]**.

I-3-1-1) Le Sous-système de station de base (BSS)

Il comprend le contrôleur de station de base (BSC) et la station émettrice-réceptrice de base/station de base (BTS/BS).

La station mobile (MS) est en permanence au contact de la station émettrice-réceptrice de base, qui est l'interface du mobile avec le réseau cellulaire. Une BTS est généralement située au centre d'une cellule. Elle fournit les canaux radio pour la signalisation et le trafic de données utilisateur dans les cellules.

Les principales tâches du BSC comprennent :

-Administration des fréquences;

-Contrôle du BTS;

-Gestion de la mobilité du MS **[3]**.

I-3-1-2) Le Sous-système NSS (Network Switching Subsystem)

Le sous-système (NSS) se compose de centres de commutation mobiles et de bases de données qui stockent les données requises pour le routage et les services. Le centre de commutation d'un réseau mobile appelé Mobile Switching Center (MSC), exécute toutes les fonctions de commutation similaires d'un nœud de commutation de réseau fixe. Les BSC d'un sous-système de base sont subordonnés à un seul MSC **[3]**.

Passerelle dédiée MSC (GMSC)

Elle sert à transférer le trafic vocal entre les réseaux fixes et les réseaux mobiles. Le réseau fixe n'est pas en mesure de connecter directement un appel entrant au MSC local

sans passer via le GMSC. Ce GMSC demande les informations de routage au Home Location Register (HLR) et achemine la connexion au MSC local dans la zone où se trouve actuellement la station mobile. Les connexions à d'autres réseaux internationaux mobiles sont principalement acheminées via le centre de commutation international (ISC) du pays respectif.

Registres des localisations de domicile et des visiteurs (HLR et VLR)

Un réseau mobile donné possède plusieurs bases de données. Deux unités fonctionnelles sont définies pour la synchronisation de l'enregistrement des abonnés et de leur emplacement actuel: un registre de localisation de domicile (HLR) et le registre de localisation de visiteur (VLR). En général, il existe un HLR central par réseau mobile terrestre public (PLMN) et un VLR pour chaque MSC.

I-3-1-3) Le Sous-système d'exploitation et de maintenance (OMSS)

L'exploitation du réseau est contrôlée et maintenue par le sous-système d'exploitation et de maintenance OMSS. Les fonctions de contrôle du réseau sont surveillées et lancées à partir du centre OMC (opération et maintenance Centre).

L'OMC a accès à la fois au GMSC et au BSC. Certaines de ses fonctions sont:

- Administration et exécution des opérations commerciales (abonnés, terminaux, tarification, statistiques);
- Gestion de la sécurité;
- Configuration du réseau, fonctionnement, gestion des performances;
- Tâches de maintenance.

L'OMC configure le BTS via le BSC et permet à l'opérateur de vérifier les composants connectés du système **[3]**.

I-3-1-4) Authentification de l'utilisateur et enregistrement de l'équipement

Deux bases de données supplémentaires sont responsables des différents aspects de la sécurité du système. Elles servent à l'authentification, l'identification et l'enregistrement des utilisateurs. Les données et clés confidentielles sont stockées ou générées dans le centre d'authentification (AUC). Le registre d'identification d'équipement (EIR) stocke les numéros de série (fournis par le fabricant) des terminaux (IMEI), ce qui

permet de bloquer l'accès au service pour les stations mobiles signalées comme volées **[3]**.

I-3-1-5) Adresses et identificateurs

Station mobile (MS)

Ce sont des équipements utilisés par les abonnés mobiles pour accéder aux services. Ils se composent de deux composants principaux: l'équipement mobile (ME) et le module d'identité d'abonné (SIM). En plus de l'identifiant d'équipement, l'IMEI (International Mobile Equipment Identity), la station mobile a une identification d'abonné (IMSI et MSISDN, ou le numéro RNIS d'abonné mobile) en tant que données dépendantes de l'abonné **[3]**.

Module d'identité d'abonné (SIM)

Le module d'identité d'abonné (SIM) fournit aux équipements mobiles une identité. Certains paramètres d'abonné sont stockés sur la carte SIM, ainsi que les données personnelles utilisées par l'abonné. La carte SIM identifie l'abonné au réseau. Pour protéger la carte SIM contre une utilisation inappropriée, les abonnés doivent entrer un numéro d'identification personnel (PIN) 4 bits avant d'utiliser le mobile. Le code PIN est enregistré sur la carte. Si le mauvais code PIN est entré trois fois de suite, la carte se bloque et ne peut être débloquée qu'avec une clé de blocage personnelle (PUK) 8 bits, également stockée dans la carte **[3]**.

Identité internationale d'équipement de station mobile (IMEI)

Ce numéro de série identifie de manière unique les stations mobiles au niveau international. Il est attribué par le fabricant de l'équipement et enregistré par les opérateurs de réseau qui les stockent dans le registre d'identité de l'équipement (EIR). IMEI est une adresse hiérarchique, contenant les parties suivantes:

- Code d'approbation de type (TAC): 6 décimales, attribuées de manière centrale;
- Le code d'assemblage (FAC): 2 décimales, attribuées par le fabricant;
- Numéro de série (SNR): 6 décimales, attribuées par le fabricant;
- Rechange (SP): 1 décimale **[3]**.

I-3-2) Evolutions du GSM

I-3-2-1) GPRS (General Packet Radio Service)

Le GPRS est un service non vocal, c'est-à-dire de données, à valeur ajoutée pour le réseau GSM. Cela se fait en superposant une interface radio basée sur les paquets sur le réseau GSM à commutation de circuits existant. En termes d'infrastructure, l'opérateur n'a qu'à ajouter quelques nœuds et quelques modifications logicielles pour mettre à niveau le système GSM vocal existant vers le système GPRS voix plus données. Le trafic vocal est commuté par circuit tandis que le trafic de données est commuté par paquets. La commutation de paquets permet d'utiliser les ressources uniquement lorsque l'abonné envoie et reçoit réellement les données. Cela permet aux ressources radio d'être utilisées simultanément tout en étant partagées entre plusieurs utilisateurs. La quantité de données qui peut être transférée dépend du nombre d'utilisateurs. Des vitesses maximales théoriques allant jusqu'à 171,2 kilobits par seconde (kbps) sont réalisables avec le GPRS en utilisant simultanément les huit intervalles de temps. Le GPRS permet l'interconnexion entre le réseau et Internet. Comme il utilise les mêmes protocoles, le réseau GPRS peut être considéré comme un sous-réseau d'internet, les téléphones mobiles compatibles GPRS étant considérés comme des hôtes mobiles **[3]**.

Cependant, il existe certaines limitations dans le réseau GPRS, telles que la faible vitesse (la vitesse pratique est bien inférieure aux vitesses théoriques).

I-3-2-2) EDGE (Enhanced Data Rate for GSM Evolution)

La limitation du réseau GPRS a été dépassée dans une certaine mesure par l'introduction de la technologie EDGE.

Le réseau EDGE est considéré comme une extension du GPRS car il peut être installé sur n'importe quel système sur lequel GPRS est déployé. Ce n'est pas une alternative à l'UMTS mais une technologie complémentaire. Dans EDGE, les services 3G peuvent être fournis à un débit de données inférieur mais similaire à l'UMTS, avec des débits allant jusqu'à 384 kbps (théoriquement). Cela se fait en introduisant un nouveau schéma de modulation 8-PSK (modulation par changement de phase) et coexistera avec le GMSK utilisé dans le GPRS.

L'avantage majeur est que les réseaux GSM existants peuvent être mis à niveau (peu de changements dans le matériel sont requis par EDGE, à l'exception de certaines mises à niveau matérielles dans le BTS et de certains logiciels mis à niveau dans le réseau), évitant ainsi les coûts énormes nécessaires pour déployer les réseaux 3G tout en fournissant des services similaires à la 3G.

Les caractéristiques générales d'EDGE incluent un débit amélioré par intervalle de temps (8,8–59,2 kbps / intervalle de temps), des changements de modulation de GMSK à 8-PSK, une sensibilité réduite du signal 8-PSK et une capacité et une couverture plus élevées.

Cependant, le système de deuxième génération manquait de capacité, d'itinérance mondiale et de qualité, sans parler de la quantité de données pouvant être envoyées. Tout cela a conduit l'industrie à travailler sur un système qui avait une portée plus globale (par exemple, l'utilisateur n'avait pas besoin de changer de téléphone pour se rendre au Japon ou aux États-Unis depuis l'Asie du Sud-Est ou l'Europe). Ce fut le début de l'évolution des systèmes de troisième génération **[3]**.

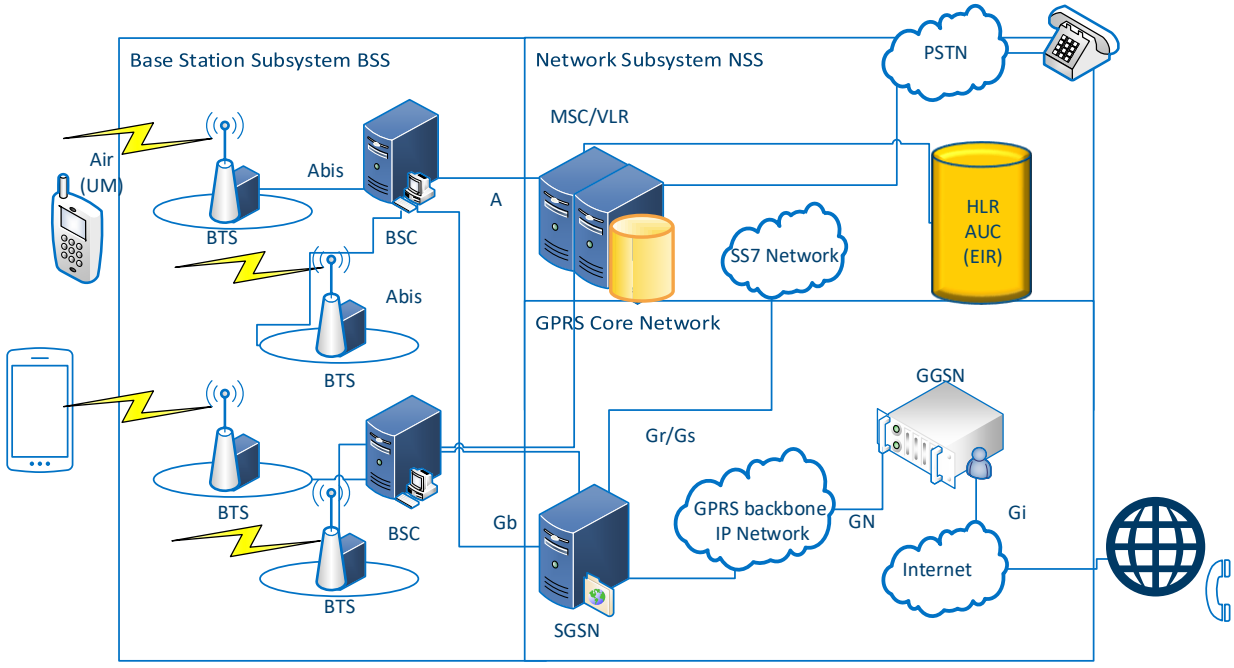


Figure I-1: Architecture du réseau GSM/ GPRS.

I-3-3) Commutation de circuit classique

Le réseau de télécommunications mobiles GSM a été conçu comme un réseau à commutation de circuits de la même manière que les réseaux de téléphonie fixe. Au début d'un appel, le réseau établit une connexion directe entre deux interlocuteurs, qui est alors utilisée exclusivement pour cette conversation. Le centre de commutation utilise une matrice de commutation pour connecter toute partie d'origine à toute partie de destination. Une fois la connexion établie, la conversation est ensuite transmise de manière transparente via la matrice de commutation entre les deux parties. Le centre de commutation ne redevient actif que pour terminer la connexion dans la matrice de commutation si l'un des correspondants souhaite mettre fin à l'appel. Cette approche est identique dans les réseaux mobiles et fixes. Les premiers réseaux de télécommunications fixes ont été conçus uniquement pour les communications vocales, pour lesquelles une connexion analogique entre les parties a été établie.

Au milieu des années 80, la technologie analogique a été remplacée par la technologie numérique dans le centre de commutation. Cela signifiait que les appels n'étaient plus envoyés sur une ligne analogique de l'expéditeur au terminateur. Au lieu de cela, le centre de commutation numérise le signal analogique qu'il reçoit des abonnés, qui lui sont directement rattachés, et transmet le signal numérisé au centre de commutation de terminaison. Là, le signal numérique est de nouveau converti en un signal analogique, qui est ensuite envoyé sur le câble en cuivre à la partie terminale.

Dans certains pays, les lignes ISDN (Integrated Services Digital Network) étaient très populaires. Avec ce système, la transmission est devenue entièrement numérique et la conversion en un signal audio analogique est effectuée directement dans le téléphone.

Par contre, un réseau mobile étant composé de nombreux centres de commutation, chacun couvrant une certaine zone géographique, il n'est même pas possible de prédire à l'avance vers quel centre de commutation un appel doit être renvoyé pour un certain abonné. Cela signifie que le logiciel de gestion des abonnés et de routage des appels des réseaux fixes ne peut pas être utilisé pour le GSM. Au lieu d'un mécanisme statique d'acheminement des appels, une architecture de gestion de la mobilité flexible est devenue nécessaire dans le réseau central, qui devrait être au courant de l'emplacement

actuel de l'abonné et est ainsi en mesure d'acheminer les appels vers l'abonné en tout lieu et à tout moment.

I-3-4) Le système de signalisation numéro 7 -SS7

Pour établir, maintenir et terminer une connexion, les informations de signalisation doivent être échangées entre l'utilisateur final et les périphériques réseau. Dans le réseau fixe, les téléphones analogiques signalent leur demande de connexion lorsque le récepteur est décroché et en composant un numéro de téléphone qui est envoyé au réseau soit par impulsions (numérotation par impulsions), soit par numérotation par tonalité, appelée double tonalité numérotation multifréquence (DTMF). Avec les téléphones RNIS fixes et les téléphones mobiles GSM, la signalisation est effectuée via un canal de signalisation dédié distinct, et des informations telles que le numéro de téléphone de destination sont envoyées sous forme de messages.

Quand plusieurs nœuds du réseau sont impliqués dans l'établissement d'un appel (par exemple les parties d'origine et de destination ne sont pas connectées au même centre de commutation), il est nécessaire qu'ils échangent des informations entre eux. Cette signalisation est transparente pour l'utilisateur, et un protocole appelé SS-7 est utilisé à cet effet. SS-7 est également utilisé dans les réseaux GSM et la norme a été améliorée par ETSI pour répondre aux exigences particulières des réseaux mobiles, par exemple, la gestion de la mobilité des abonnés.

I-4) Le Réseau radio mobile de troisième génération

La troisième génération UMTS ou Universal Mobile Télécommunication System fait partie de la famille IMT-2000 (International Mobile Telecommunications for the year 2000), le réseau UMTS combine et complète simplement les réseaux existants (GSM et GPRS) qui fournissent des fonctionnalités pour la voix et les données.

Les réseaux UMTS ont apporté de nouvelles avancées, notamment une large gamme de services à haute vitesse, des services audiovisuels et l'utilisation d'une seule station mobile sous différents environnements radio.

I-4-1) Architecture de réseau UMTS

Afin de réutiliser les investissements du GSM et de minimiser le coût de déploiement de l'UMTS, il a été décidé que le réseau central GSM et GPRS existant soit légèrement modifié mais les mêmes nœuds seront utilisés pour donner accès aux deux réseaux d'accès radios. Il y a eu quelques modifications mineures définies pour 3G MSC et 3G SGSN.

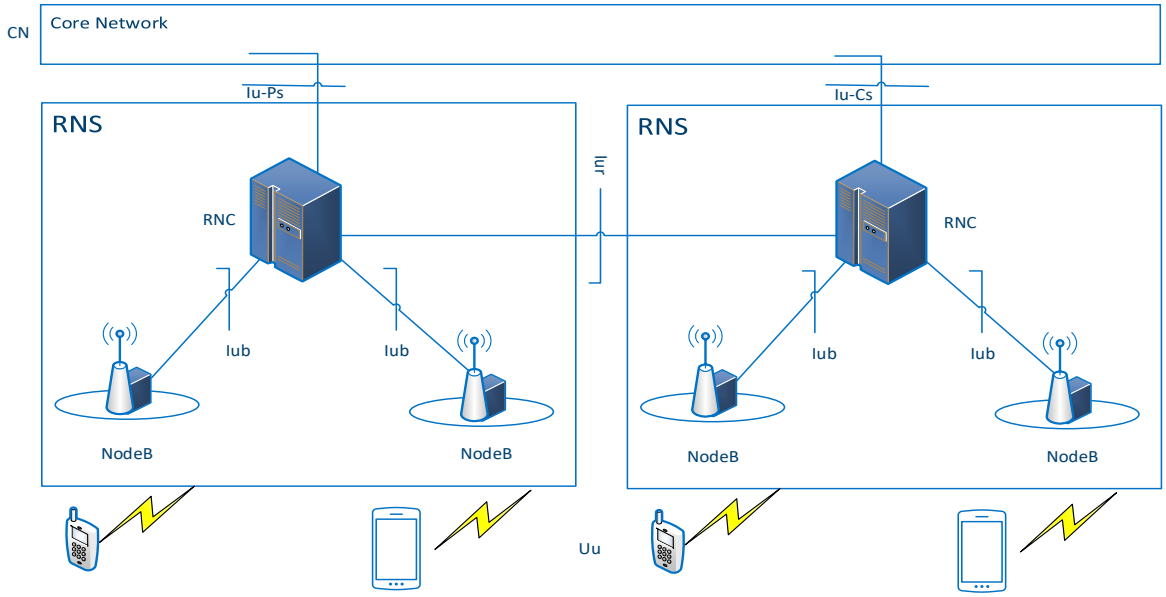


Figure I-2: Architecture UMTS UTRAN.

I-4-1-1) Équipement Utilisateur (UE)

L'équipement utilisateur UE est composé de l'équipement mobile ME et de la carte USIM (module d'identité d'abonné UMTS);

• ME (Mobile Equipment): est l'équipement électronique (émetteur-récepteur) et l'interface homme-machine.

• USIM: USIM assure l'identification des abonnés, la sécurité et la confidentialité des communications.

I-4-1-2) UTRAN

Le réseau universel d'accès radio terrestre UMTS (UTRAN) est le tout nouveau réseau d'accès basé sur CDMA à large bande défini pour les réseaux 3G UMTS. L'UTRAN est divisé en plusieurs sous-systèmes de réseau radio où chaque RNS est géré par un RNC. Un RNS se compose généralement de centaines de stations de base appelées NodeB.

Le Radio Network System (RNS) est le système d'équipements de station de base (émetteurs-récepteurs, contrôleurs, etc ...) qui est perçu par le MSC à travers une seule interface **Iu-CS** comme étant l'entité chargée de communiquer avec les stations mobiles dans une certaine zone. De même, dans les PLMN prenant en charge le GPRS, le RNS est vu par le SGSN via une seule interface **Iu-PS**. En bref, le RNS se compose d'un contrôleur de réseau radio (RNC) et d'un ou plusieurs Node B **[4]**.

NodeB

Le Node B peut être simplement considéré comme le «BTS de la 3G». La fonction principale du Node B est d'établir la mise en œuvre physique de l'interface **Uu** et de l'interface **Iub**. La réalisation de l'interface **Uu** signifie que le Node B implémente les canaux physiques WCDMA et convertit les informations provenant des canaux de transport vers les canaux physiques sous le contrôle du RNC. Pour l'interface **Iub**, le Node B effectue la fonctionnalité inverse. Il convient de noter ici que le NodeB ne possède que les ressources des canaux physiques alors que les canaux de transport sont entièrement gérés par RNC **[4]**.

RNC

Le Contrôleur de réseau radio (RNC) est le principal élément de contrôle de l'UTRAN, car il possède toutes les ressources logiques du RNS. Il est chargé de contrôler l'utilisation et l'intégrité de toutes les ressources radio 3G au moyen de procédures de gestion des ressources radio (RRM). Cela comprend des fonctions telles que le transfert et le contrôle d'admission, le contrôle de puissance et l'allocation de code, le contrôle des ressources radio (RRC) **[4]**.

I-4-1-3) Réseau central (CN)

Le réseau central (CN) est divisé en trois groupes. Le premier est le domaine CS. Le second est le domaine PS, le troisième groupe de regroupement d'entités commun aux domaines PS et CS, à savoir HLR, AuC et EIR.

Il permet à l'utilisateur de communiquer au sein du même réseau mobile et de l'interconnecter avec les réseaux internes et externes, fixes ou mobiles, numériques ou analogiques. Sa principale caractéristique dans la plupart est l'emplacement de la gestion,

le contrôle des paramètres du réseau, la commutation, le routage des données, la signalisation entre les réseaux mobile et distant via l'interface radio **[4]**.

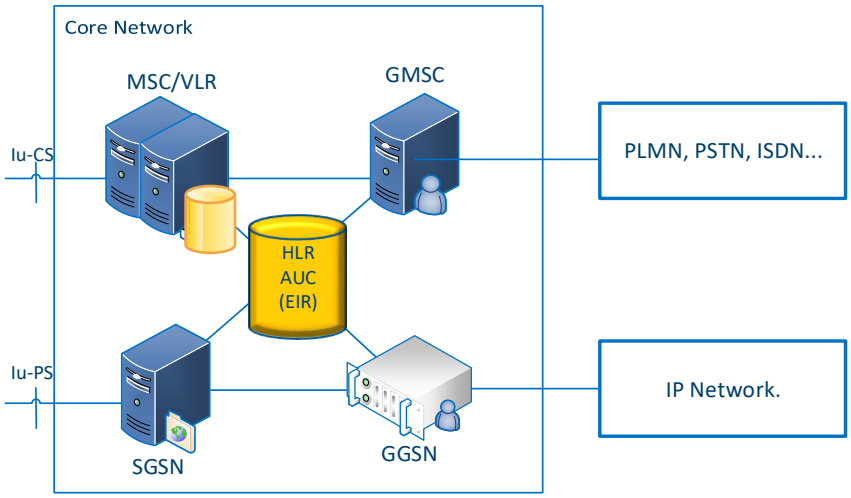


Figure I-3: Architecture du réseau central UMTS.

Domaine à commutation de circuits (domaine CS)

Le domaine à commutation de circuits (CS) comprend les entités MSC, VLR et GMSC. Il est le mieux adapté pour la transmission vocale, la transmission de messages SMS, de fax et pour les services de type temps réel dédiés aux conversations (téléphone, visiophone).

• MSC (Mobile Switching Center): il assure la communication vers un mobile et la commutation des données pour l'accès aux services à commutation de circuits.

• VLR (Visitor Location Register): il s'agit d'une base de données attachée à un ou plusieurs MSC. Son rôle est d'enregistrer les utilisateurs dans une zone géographique LA (Location Area) qui nous donne les informations sur la position de l'abonné et ses identifiants temporaires.

• GMSC (Gateway MSC): Il s'agit d'une passerelle entre le réseau UMTS et les réseaux externes venus PSTN, PLMN, ISDN ... etc **[4]**.

Domaine à commutation de paquets (PS)

Le domaine à commutation de paquets composé d'entités similaires à celles du GPRS (SGSN et GGSN) est basé sur une transmission de données par paquets utilisant le

protocole IP, ce qui garantit une compatibilité maximale avec l'internet. Il permet de gérer des services non temps réel (navigation sur Internet, gestion des jeux en ligne et e-mails ...). Le débit du domaine des paquets est sept fois plus rapide que le circuit de champ.

• SGSN (Serving GPRS Support Node): son rôle est similaire au MSC / VLR. Il achemine les paquets de données, effectue les procédures de routage, la gestion de la mobilité et l'authentification.

• GGSN (Gateway GPRS Support Node): son rôle est similaire au GMSC, mais il est utilisé pour la commutation de paquets. Il permet à l'utilisateur de se connecter à Internet via des réseaux externes **[4]**.

Éléments communs des domaines CS et PS

• HLR (Home Location Register) est une base de données contenant les informations sur les abonnés appartenant à la zone desservie par le centre de commutation de services mobiles (MSC).

• AuC (Authentication Center): il s'agit du centre d'authentification réseau contenant des paramètres secrets sur la gestion de la sécurité du système.

• EIR (Equipment Identity Register): contient une liste d'équipements, appelée liste noire, dont l'accès doit être refusé (équipements volés ou non autorisés) **[4]**.

I-4-2) Prise en charge vocale en 2G/ 3G

L'évolution majeure du GSM à l'UMTS a été dans l'interface d'accès radio, en améliorant l'utilisation des ressources, le spectre radio et la réduction de la consommation d'énergie en particulier, et cela devait prendre en charge un débit de données beaucoup plus élevé de la station de base vers l'utilisateur et de l'utilisateur vers la station de base. L'évolution a également consisté à prendre en charge une grande partie du trafic de données dans le réseau principal lui-même, de sorte qu'en tant que solution intelligente, l'architecture n'a pas été entièrement modifiée, en particulier dans le réseau principal, car l'ajout de composants était suffisant pour fournir la solution recherchée.

Le service vocal dans les deux technologies était basé sur la technologie à commutation de circuits comme mentionné ci-dessus, mais certains opérateurs, qui ont

installé 3G sur la version HSPA, ont préconisé une solution, qui comprend des paquets voix sur IP en cas de saturation dans les circuits commutés GSM et UMTS.

C'est assez proche de la Voix sur LTE qui est basée sur IMS, et qui sera détaillée dans les prochains chapitres.

I-5) Conclusion

Dans ce premier chapitre, ont été présenté les technologies radio-mobiles antérieures à la 4G LTE: de la prise en charge de la voix analogique dans les standards de première génération, à la première norme unifiée mobile internationale qui est GSM et son évolution vers GPRS et EDGE, juste avant l'émergence de l'UMTS 3G.

Ces technologies radio-mobiles prennent en charge la voix sur circuit commuté comme le font les réseaux fixes commutés RTPC.

Cependant, la 3G UMTS est plus intéressante tant sur le plan de la prise en charge des débits de données élevés, que sur le plan de l'offre en termes de nouveaux services et applications, et c'était un défi, pour prendre en charge et le trafic voix du réseau commute CS de la 2G et les paquets de données commutés également.

Dans le chapitre suivant , nous verrons ce que la 4G LTE apporte comme nouveautés.

Chapitre II:

4G LTE & Solution VoLTE

Chapitre II: 4G LTE & Solution VoLTE

II-1) Introduction

La principale fonctionnalité utilisée dans un réseau mobile est la communication vocale; on fait généralement usage des téléphones portables pour la transmission de la voix en premier lieu, pour les opérateurs les services vocaux et SMS représentent la majorité de leur activité. Si comme vu précédemment, que la 2G et la 3G utilisent des systèmes à commutation de circuits pour assurer la communication vocale entre deux utilisateurs du réseau central, la 4G est exclusivement à base de systèmes à commutation de paquets IP.

Dans ce chapitre, on va essayer d'expliquer l'architecture et le fonctionnement du réseau mobile de 4e génération, puis on verra ce qu'est la voix sur LTE, comment cela se fait, en répondant à la fameuse question «est-ce la même chose que la 2G et la 3G?».

II-2) Réseaux radio-mobiles de quatrième génération

Le terme LTE est en fait un nom de projet du 3GPP. L'objectif du projet, qui a débuté en novembre 2004, était de déterminer l'évolution à long terme du système de téléphonie mobile universel UMTS qui était à l'origine, également un projet 3GPP.

L'UMTS également un projet 3GPP à l'origine, qui a étudié plusieurs technologies candidates avant d'opter pour l'accès multiple à division de code à large bande (W-CDMA) pour le réseau d'accès radio UTRAN.

Parce que LTE est l'évolution de l'UMTS dans sa partie radio, les composants équivalents de LTE sont donc appelés Evolved UTRAN (E-UTRAN). Cependant, le système dans sa globalité, est plus qu'un réseau d'accès mobile, ce qui a donné également naissance à un autre projet 3GPP parallèle appelé System Architecture Evolution (SAE), qui définit un nouveau réseau central (CN) en paquets uniquement IP appelé Evolved Packet Core (EPC). La combinaison de l'EPC et du réseau d'accès radio évolué (E-UTRAN) est le système Evolved Packet (EPS).

Selon le contexte, l'un des termes LTE, E-UTRAN, SAE, EPC et EPS peut être utilisé pour décrire une partie ou la totalité du système, bien que EPS soit le seul terme correct

pour le système global, le nom du système sera souvent écrit en LTE / SAE ou même simplement LTE **[5]**.

II-3) Architecture 4G LTE

Comme les réseaux 2G et 3G, l'architecture générale LTE / EPC est définie d'un point de vue physique et fonctionnel.

D'un point de vue physique, l'architecture LTE / EPC est composée des domaines suivants:

- L'UE;
- Le réseau d'accès, appelé LTE ou E-UTRAN (Evolved-UTRAN);
- Le réseau central, appelé EPC.

L'architecture générale LTE/EPC est illustrée dans la figure suivante.

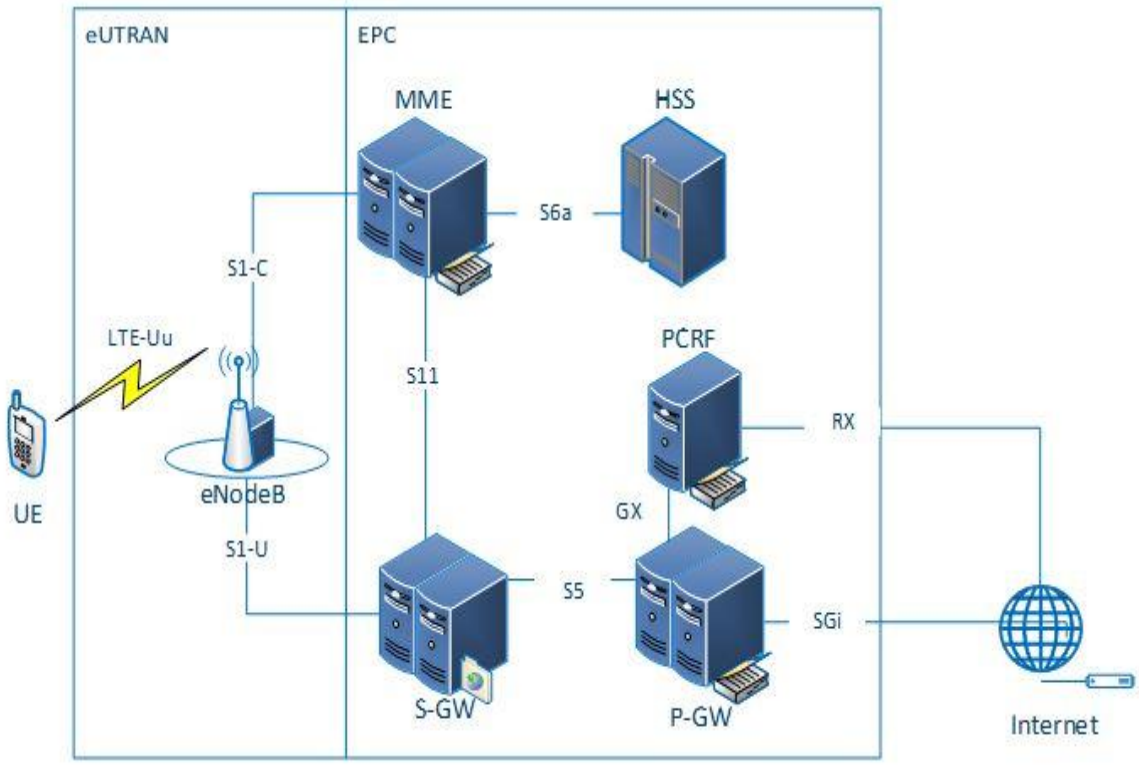


Figure II.1: Architecture LTE.

II-3-1) L'appareil LTE (UE)

L'accès au réseau LTE nécessite l'utilisation d'un appareil compatible avec la technologie LTE (Smartphones, des tablettes, des clés-modems USB), doté de fonctions uniques (améliorées par la vitesse supérieure de la LTE et aux débits maximaux fournis par

le type d'antenne qu'il intègre). Tout terminal doté d'une carte SIM LTE, doit être capable de s'adapter aux 6 largeurs spectrales allant de 1,4 à 20 MHz.

II-3-2) Le réseau d'accès LTE

Contrairement au réseau d'accès de la 3G où sont présentes les entités NodeB et RNC, l'architecture du réseau d'accès LTE (ou E-UTRAN) ne comporte que des eNodeB.

Les fonctions supportées dans la 3G par le RNC sont réparties entre l'eNodeB et les deux entités du réseau cœur à savoir le MME et le SGW.

Il n'y a donc pas de contrôleur centralisé dans E-UTRAN, son architecture est ainsi dite plate.

La eNodeB est responsable de la transmission et de la réception radio avec l'UE, selon le mode MIMO (multiple input multiple output) en recourant à plusieurs antennes en émission et en réception.

En outre, le débit se voit nettement amélioré par d'une part l'utilisation des technologies d'accès basées sur le multiplexage fréquentiel orthogonal du type OFDMA pour les flux descendants et en SC-FDMA pour les flux montants tout en introduisant de modulations du type QPSK et QAM.

La eNodeB dispose de deux types d'interfaces essentielles:

- l'interface **S1** avec le réseau cœur consistant en une interface de signalisation S1-C (S1-Contrôle) entre l'eNodeB et le MME et une autre de session S1-U (S1-Usager) entre l'eNodeB et le SGW.
- l'interface **X2** entre eNodeB adjacents dont le rôle principal est de minimiser la perte de paquets lors de la mobilité intercellulaire de l'usager en mode ACTIF (handover):

Lorsque l'usager se déplace en mode ACTIF d'un eNodeB à un autre eNodeB, de nouvelles ressources sont allouées sur le nouvel eNodeB pour l'UE, tandis que le réseau continue à transférer les paquets entrants vers l'ancien eNodeB qui les fait parvenir via l'interface X2 au nouvel eNodeB tant que celui-ci n'a pas informé le réseau qu'il s'agit de lui relayer directement les paquets entrants.

Les protocoles qui s'exécutent entre les eNodeB et l'UE sont connus sous le nom de «protocoles AS».

L'E-UTRAN est responsable de toutes les fonctions liées à la radio, qui peuvent être résumées brièvement comme suit:

- **Gestion des ressources radio (RRM):** Cela couvre toutes les fonctions liées aux supports radio, telles que le contrôle du support radio, le contrôle d'admission radio, le contrôle de la mobilité radio, la programmation et l'allocation dynamique des ressources aux UE dans les liaisons montantes et descendantes.
- **compression d'en-tête:** Cela permet d'assurer une utilisation efficace de l'interface radio en compressant les en-têtes de paquets IP qui pourraient autrement représenter une surcharge importante, en particulier pour les petits paquets tels que la VoIP.
- **Sécurité:** Toutes les données envoyées via l'interface radio sont cryptées.
- **Connectivité à l'EPC:** Il s'agit de la signalisation vers le MME et du chemin support vers le S-GW.

II-3-3) Le réseau central

Le réseau central (appelé EPC) est responsable du contrôle global de l'UE et de l'établissement des supports. Les principaux nœuds logiques de l'EPC sont:

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

En plus de ces nœuds, EPC comprend également d'autres nœuds et fonctions logiques tels que le Home Subscriber Server (HSS) et l'entité chargée de la fonction de contrôle des politiques (Qos) et des règles de tarification nommée PCRF. Étant donné que l'EPS ne fournit qu'une connectivité d'une certaine QoS, le contrôle des applications multimédias telles que la VoIP est assuré par le sous-système multimédia IP (IMS), qui est considéré comme étant en dehors de l'EPS lui-même, IMS sera discuté dans le 3ème chapitre.

Les nœuds logiques du réseau cœur sont examinés plus en détail ci-dessous:

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

La fonction de contrôle des politiques et des règles de tarification est responsable de la prise de décisions en matière de contrôle des politiques, ainsi que du contrôle des

fonctionnalités de tarification basées sur les flux dans la fonction d'application du contrôle des politiques (PCEF) qui réside dans le P-GW.

L'entité PCRF réalise, à ce titre, deux fonctions :

- La première de "Policy control" liée aux fonctions d'autorisation ou de blocage et de QoS des flux IP qui permet de demander au PDN-GW d'établir, de modifier et de libérer des supports dédiés sur la base de QoS souhaitée par l'usager. Par exemple, Si l'usager demande l'établissement d'une session IMS, un message SIP sera envoyé au P-CSCF qui dialoguera avec le PCRF pour lui indiquer la QoS requise par l'usager pour cette session. Le PCRF dialogue alors avec le PDN-GW pour créer le support dédié correspondant.
- La deuxième de "Charging control" qui fournit au PDN-GW via le PCEF qui y est intégré les règles de taxation lorsqu'un support par défaut ou dédié est activé ou modifié pour l'usager. Ces règles de taxation (sur la base du volume, de la session ou de la durée) permettent au PDN-GW de différencier les flux de données de service.

HSS (Home Subscriber Server)

Il contient les données d'abonnement EPS des utilisateurs telles que le profil QoS souscrit par EPS et toutes les restrictions d'accès pour l'itinérance. Il contient également des informations sur les PDN auxquels l'utilisateur peut se connecter. Il peut s'agir d'un nom de point d'accès (APN) (qui est une étiquette selon les conventions de dénomination DNS décrivant le point d'accès au PDN) ou d'une adresse PDN (indiquant les adresses IP souscrites). De plus, le HSS contient des informations dynamiques telles que l'identité du MME auquel l'utilisateur est actuellement attaché ou enregistré.

Le HSS intègre le centre d'authentification (AUC), qui génère les vecteurs d'authentification et de clés de sécurité **[5,6]**.

Il va sans dire, qu'avec la technologie LTE, l'opérateur réutilise le HLR des réseaux hérités qui est ainsi renommé HSS. Le HSS est donc un HLR évolué qui contient en plus de l'information de souscription pour les réseaux GSM, GPRS, 3G, celle relative aux réseaux LTE et IMS.

À la différence de la 2G et de la 3G où l'interface vers le HLR est supportée par le protocole MAP (protocole du monde SS7), l'interface S6 s'appuie sur le protocole DIAMETER (protocole du monde IP).

Le HSS est une base de données qui est utilisée simultanément par les réseaux 2G, 3G,LTE/SAE et IMS appartenant au même opérateur. Il doit, à cet effet, supporter les protocoles MAP (2G, 3G) et DIAMETER (LTE/SAE, IMS).

P-GW

C'est le routeur passerelle qui permet l'interconnexion du réseau EPS aux réseaux externes de données.

Il est aussi le **seul nœud** du réseau EPS qui assure le routage des paquets IP en ce sens que le réseau EPS transporte le flux des données IP de **manière transparente** de l'UE jusqu'au PGW. En recevant des données du SGW ou d'un réseau externe, le PGW met en place un mécanisme d'ordonnancement des données en se référant à la QoS.

Lors de l'attachement; le PGW alloue l'adresse IP (IPv4 ou IPv6) à l'UE. Il est aussi chargé au moyen de la fonction hébergée PCEF de l'application de la QoS et de la facturation basée sur les flux conformément aux règles de la PCRF. Il est responsable du filtrage des paquets IP d'utilisateur de liaison descendante dans les différents supports basés sur la QoS. Ceci est effectué sur la base des modèles de flux de trafic (TFT).

Il sert également d'ancrage de mobilité pour l'interfonctionnement avec les technologies non 3GPP telles que les réseaux CDMA2000 et WiMAX® **[5,6]**.

S-GW

Il joue le rôle de passerelle de service qui assure le transfert des paquets IP d'utilisateur aussi bien entrants (provenant du PGW vers l'ENB) que sortants (provenant de l'ENB vers le PGW).

Il sert de point d'ancrage pour le handover inter-eNodeB : Lors d'un handover inter-eNodeB, le trafic de l'usager qui s'échangeait entre l'ancien eNodeB et le Serving GW doit désormais être relayé du nouvel eNodeB au Serving GW.

Il sert également de point d'ancrage pour le handover entre LTE et les réseaux 2G/3G: Il relaie les paquets entre les systèmes 2G/3G et le PDN-GW. Lors d'une mobilité

entre LTE et Les réseaux 2G/3G paquet, le SGSN du réseau 2G/3G s'interface avec le Serving GW pour la continuité du service de données.

Il conserve également les informations sur les supports lorsque l'UE est à l'état inactif (connu sous le nom de «EPS Connection Management - IDLE» [ECM-IDLE]) et met temporairement en mémoire tampon les données de liaison descendante pendant que le MME informé par le SGW de l'appel entrant en question; lance la pagination de l'UE pour rétablir les supports.

En outre, le S-GW remplit certaines fonctions administratives dans le réseau visité, telles que la collecte d'informations pour la facturation (par exemple, le volume de données envoyées à ou reçues de l'utilisateur) **[6]**.

MME (Mobility mangement entity)

L'entité de gestion de la mobilité (MME) est responsable de:

- **L'attachement et du détachement de l'UE** : Les terminaux LTE disposent de protocole EMM (EPS Mobility Management) qui leur permettent de gérer leur mobilité (attachement, détachement, mise à jour de localisation). Ce protocole est échangé entre l'UE et le MME **[6]**.
- **La gestion de session**: Les terminaux LTE disposent de protocole ESM (EPS Session Management) qui leur permettent de gérer leur session (établissement/libération de session de données). C'est au MME d'établir pour le compte de l'usager les supports par default nécessaires à la prise en charge de ses communications par la sélection des entités SGW et PGW.
- **L'Authentification** : Le MME est responsable de l'authentification des UEs à partir des informations (profil et données d' authentification) recueillies du HSS.
- **La Joignabilité de l'UE dans l'état IDLE (incluant paging)** : C'est l'entité MME qui est responsable du paging lorsque l'UE est dans l'état IDLE et que des paquets à destination de l'UE sont reçus et mis en mémoire par le Serving GW.
- **La Gestion de la liste de zone de localisation:** L'UE est informé des zones de localisation prises en charge par le MME, appelées Tracking Area TA. L'UE met à jour sa localisation lorsqu'il se retrouve dans une TA qui n'est pas prise en charge par son MME.

- **La Sélection du SGSN lors du handover avec les réseaux d'accès 2G et 3G** : Si l'usager se déplace d'une zone LTE à une zone 2G/3G, c'est le MME qui sélectionnera le SGSN qui sera impliqué dans la mise en place du support par défaut ou (default Bearer).
- **L'Interception légale du trafic de signalisation** : L'entité MME reçoit toute la signalisation émise par le mobile, par exemple l'état du mobile (en veille ou connecté), sa localisation si le mobile est en veille, l'identité de la cellule si le mobile est en session.

II-4) Solutions pour la Voix sur LTE

L'une des principales nouveautés de la LTE est d'être un réseau mobile tout IP c.à.d. de bout en bout. Paradoxalement, il ne permet pas l'acheminement de la voix.

À l'instar de la téléphonie fixe ou la voix sur IP est déployée depuis déjà longtemps, pour que le réseau LTE puisse transporter la voix, il doit être géré par un protocole SIP.

Ce protocole basé sur une plateforme nommée IMS garantit une priorisation des appels temps réels (avec la meilleure qualité de service possible) par rapport aux autres flux IP.

Au niveau de l'opérateur, la gestion de la voix sur IP dans un réseau LTE (ou plus exactement voix sur LTE) est réalisée par un cœur réseau IMS. Cependant son déploiement est compliqué et onéreux, ce qui constitue pour un opérateur un choix pas viable économiquement d'autant plus que les terminaux compatibles VoLTE étaient à l'époque rares faute de maturité technologique.

La VoLTE a été normalisée par l'organisme 3GPP et complétée par un profilage supplémentaire de la part du GSMA qui a requis et identifié pour la voix et les SMS IMS un ensemble minimal obligatoire de fonctionnalités définies dans les spécifications 3GPP qu'un dispositif sans fil (UE) et un réseau doivent mettre en œuvre afin de garantir un service de téléphonie vocale IMS basé sur IMS interopérable et de haute qualité sur LTE.

Depuis, la VoLTE est devenue la principale technologie de transport vocal pour les réseaux mobiles 4G LTE et reste donc **la solution la mieux indiquée à long terme.**

Étant donné que le LTE n'a pas de domaine à commutation de circuits dans le **réseau cœur**, et que dans un premier temps, l'IMS pour offrir la VoLTE via l'accès 4G n'est pas mis

en œuvre, les opérateurs 4G ont du recourir pour la transmission vocale à leurs réseaux existants 2G ou 3G.

A cet effet, l'organisme 3GPP a résolu , **à titre transitoire**, ce problème en proposant aux opérateurs d'utiliser des services vocaux entre différentes technologies radio-mobiles les deux (02) solutions suivantes:

- CSFB (Circuit Switched FallBack);
- VoLGA (Voice over LTE via Generic Access).

II-4-1) CSFB (Circuit Switched FallBack)

La solution de Circuit Switched FallBack fournit un moyen pratique de réutiliser le réseau GSM/UMTS existant pour prendre en charge la voix dans le réseau LTE. Cette solution est normalisée par 3GPP et offre aux opérateurs la flexibilité de déployer le LTE en tant que réseau de superposition de données uniquement et d'utiliser le réseau CS existant pour prendre en charge la fonctionnalité vocale.

L'architecture réseau de CS fallback est illustrée dans la figure suivante:

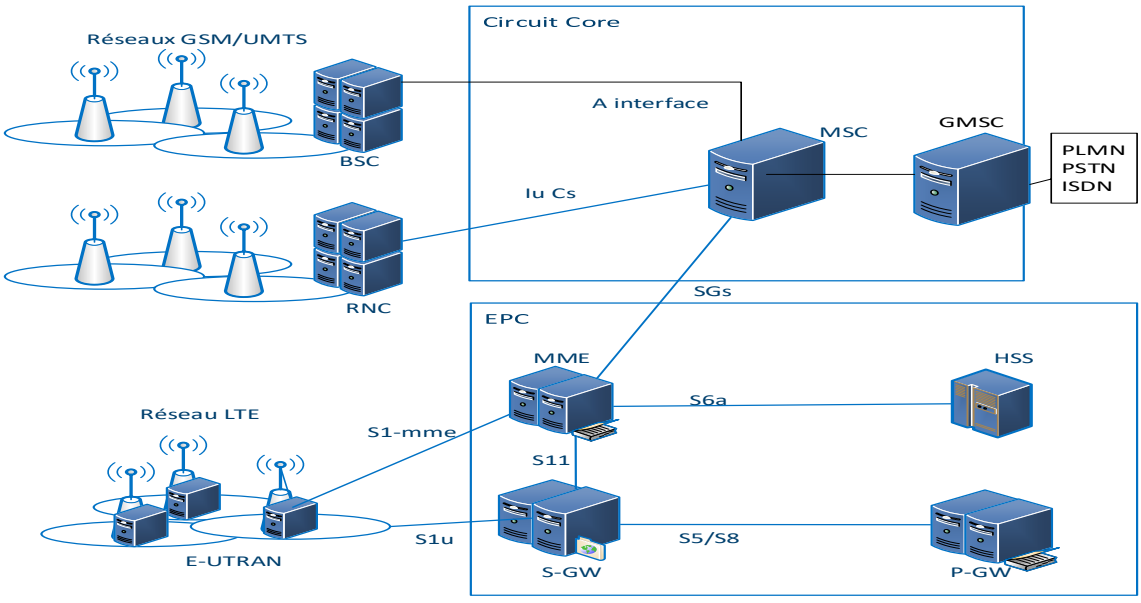


Figure II-2: Architecture CS fallback.

L'utilisateur effectue un enregistrement combiné avec le réseau LTE ainsi qu'avec le réseau GSM / UMTS pendant la procédure d'enregistrement initiale. Cet enregistrement combiné est facilité par l'entité de gestion de la mobilité (MME) du réseau LTE, qui effectue l'enregistrement sur le réseau 2G / 3G pour le compte de l'utilisateur.

Pendant le lancement de l'appel vocal par l'utilisateur, le MME redirige la demande vers le serveur MSC dans le domaine CS. En cas de réservation réussie des ressources dans le domaine CS pour l'appel, le serveur MSC doit répondre au MME sur l'état de la demande. Le MME ordonne alors au eNodeB de demander à l'utilisateur d'effectuer un transfert vers le réseau GSM / UMTS. Dans les deux cas, une seule radio est activée (soit 2G ou 3G) pour éviter un DAS (Débit d'Absorption Spécifique) élevé et économiser batterie.

La session de données en cours pour l'utilisateur dans le réseau LTE est suspendue si le réseau de destination est un réseau GSM. À la fin, le terminal retourne en 4G pour disposer du meilleur débit possible pour ses sessions data qui sont reprises.

Si le réseau de destination est un réseau UMTS, les sessions data sont maintenues avec la même adresse IP et l'appel voix peut être établi en parallèle des sessions data. À la fin, le terminal retourne en 4G pour retrouver son meilleur débit possible pour ses sessions data sans leur interruption **[7]**.

Cette solution présente plusieurs inconvénients comme l'augmentation du temps d'établissement des appels en raison de la procédure de transfert intercellulaire et la perturbation de la transmission des données pendant toute la durée de l'appel vocal lorsque l'utilisateur revient sur un réseau GSM ou UMTS.

Cette solution est utilisée lors du déploiement initial lorsque le LTE (non compatible avec VoLTE) est davantage utilisé pour les données à haut débit et que la voix est entièrement gérée par les réseaux à commutation de circuits des réseaux hérités. Par conséquent, la solution de repli CS fallback n'est considérée que comme une solution temporaire lors du déploiement initial du réseau LTE **[7]**.

Par conséquent, le CSFB offre l'avantage de permettre une réutilisation complète de l'infrastructure existante (réseau, services, systèmes de facturation ...) ne nécessitant que quelques mises à jour mineures. il s'agit d'une solution qui prolonge la durée de vie du réseau 2G/3G existant et le rentabiliser plutôt que de profiter de l'introduction de la 4G, ce qui pourrait considérablement réduire l'intérêt de déployer cette nouvelle technologie **[7]**.

II-4-2) VoLGA (Voice over LTE via Generic Access)

Le concept consiste à connecter les centres de commutation mobiles (MSC) déjà existants au réseau LTE via une passerelle. Comme aucun retour à un réseau hérité n'est requis, les temps d'établissement des appels ne sont pas augmentés et la qualité d'expérience de l'utilisateur est cohérente avec celle de l'environnement vocal 2G ou 3G.

Le seul nouvel élément de réseau introduit est le contrôleur de réseau d'accès VoLGA (VANC), illustré dans la figure ci-dessous. Tous les autres éléments du réseau et les interfaces entre eux existent déjà et sont réutilisés sans aucune modification.

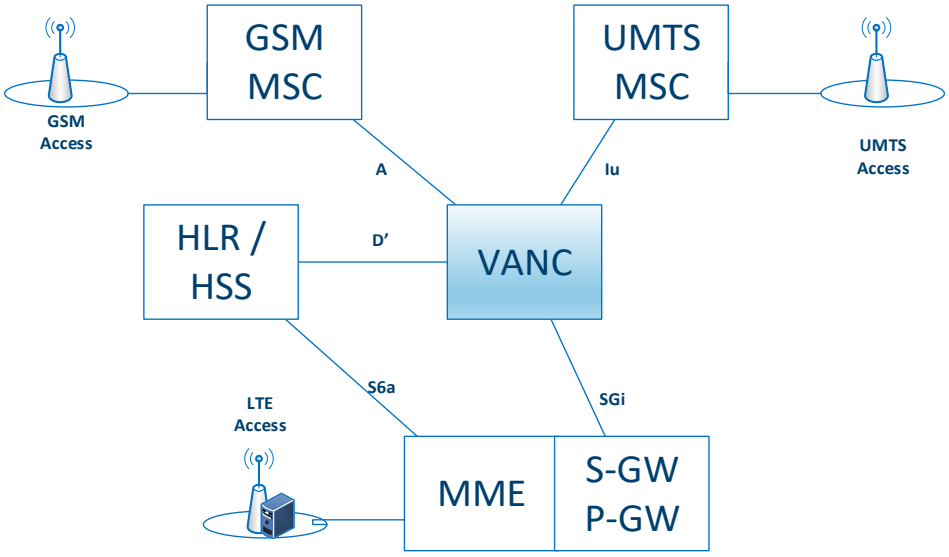


Figure II-3: La solution VoLGA.

Du côté du réseau à commutation de circuits: l'interface **A** est utilisée pour connecter le VANC à un centre de commutation mobile GSM (MSC) alors que L'interface **Iu** est utilisée pour connecter le VANC au UMTS MSC. Le VANC ressemble ainsi à un contrôleur de station de base GSM (BSC) à un MSC GSM et à un contrôleur de réseau radio UMTS (RNC) à un centre de commutation mobile UMTS. L'interface utilisée dans la pratique dépend des exigences de l'opérateur de réseau. Comme les interfaces **A** et **Iu** sont utilisées sans aucune amélioration, les MSC ne savent pas que les mobiles plutôt connectés via LTE ne sont pas directement connectés via leurs réseaux radio respectifs. Par conséquent, aucune modification n'est requise sur ces nœuds de réseau pour prendre en charge la voix, les SMS et d'autres services sur le réseau LTE **[8]**.

- **Inscription au réseau**

Lorsqu'un appareil mobile est allumé et détecte un réseau LTE, il s'enregistre d'abord auprès du MME sur le réseau d'accès LTE. Le MME utilise l'interface S6a pour le registre d'emplacement d'origine/serveur d'abonné domestique (HLR/HSS) pour récupérer les données d'abonné requises pour l'authentification et la gestion de l'utilisateur.

Après enregistrement auprès du réseau LTE, le mobile établit alors une connexion avec le VANC. La procédure à suivre dépend des informations de configuration spécifiques à VoLGA stockées dans l'appareil mobile.

Tout d'abord, une connexion IP appropriée doit être mise en place. Dans le réseau domestique, une connectivité par défaut peut être utilisée. Il est également possible d'utiliser une connectivité et une adresse IP distinctes à cet effet. Le nom d'hôte ou l'adresse IP du VANC peut être soit pré-approvisionné (stocké ou enregistré) dans le périphérique mobile, soit acquis en interrogeant un serveur DHCP (Dynamic Host Configuration Protocol) dans le réseau sur la connectivité qui a été établie pour VoLGA dans l'étape précédente.

Une fois que l'adresse IP du VANC est connue, le mobile lui établit un tunnel IPSec sécurisé sur le réseau radio LTE via le réseau central LTE et sur l'interface SGi. Pendant le processus, le VANC authentifie l'utilisateur à l'aide des informations d'authentification stockées dans le HLR / HSS, qu'il contacte via l'interface D'.

Ensuite, l'appareil mobile s'enregistre auprès du MSC via le tunnel sécurisé et le VANC. Le protocole DTAP (Direct Transfer Application Part) est utilisé à cet effet, qui est déjà connu du GSM et de l'UMTS. Les messages sont acheminés de manière transparente entre l'appareil mobile et le MSC par tous les composants réseau impliqués.

Le VANC ajoute simplement des informations telles qu'un identifiant de cellule (2G) ou l'identifiant de zone de service (3G) au message d'enregistrement initial tel que défini dans les normes GSM et UMTS respectivement.

- **Appels vocaux sortants sur LTE**

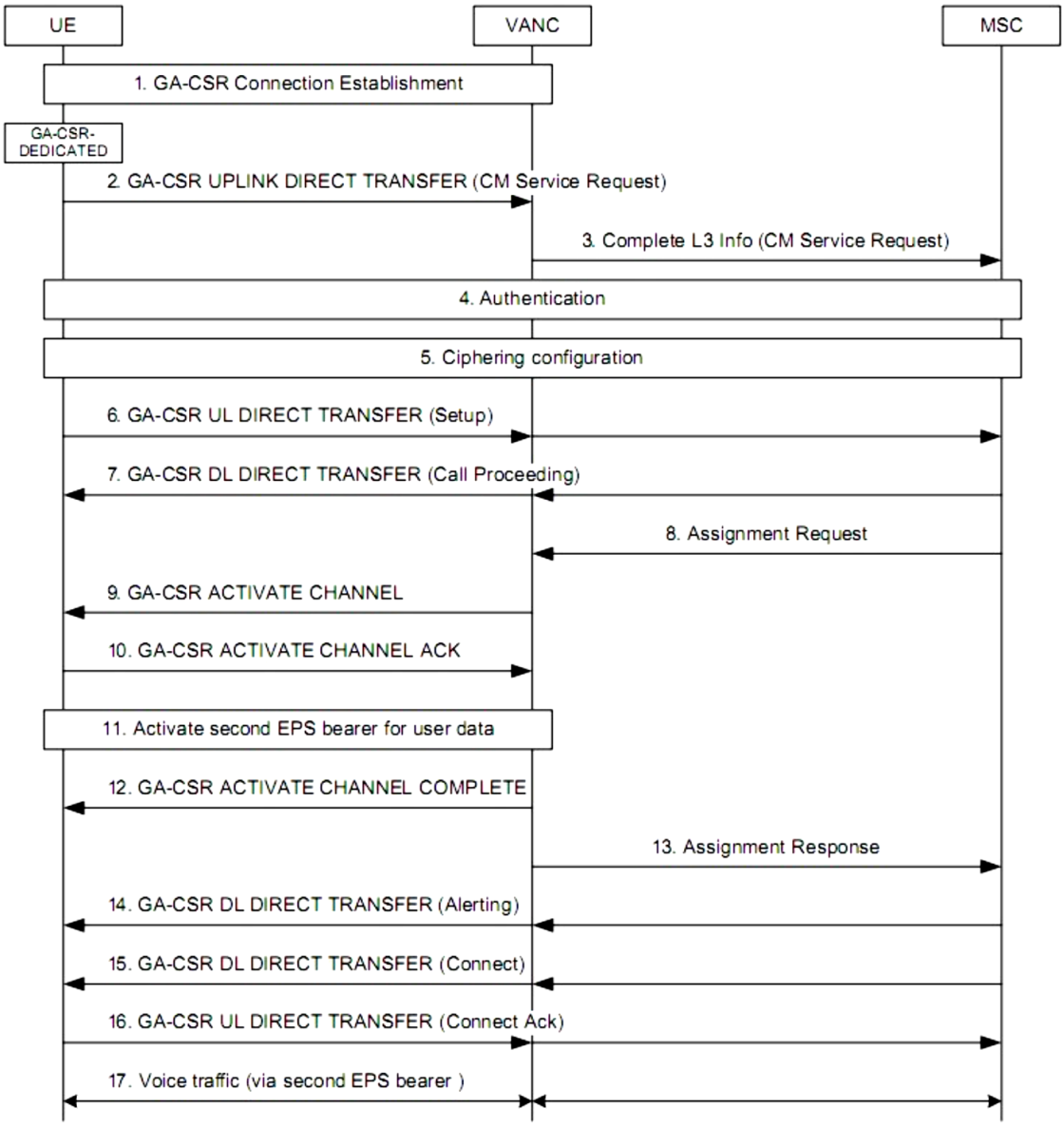


Figure II- 4: Flux d'appels pour un appel vocal d'origine mobile LTE (spécification VoLGA) **[8].**

- Au début, l'appareil mobile envoie un message au VANC pour changer la connexion de l'état inactif à l'état dédié.
- Un message de demande de service CM GSM / UMTS standard est envoyé pour établir une connexion avec le MSC.
- Une fois que le VANC reçoit le message, il crée une connexion de signalisation dédiée au MSC via l'interface **A** ou **Iu** pour cet utilisateur et transmet le message.

- Le MSC authentifie ensuite généralement l'utilisateur et active le chiffrement (étapes 4 et 5 de la figure).
- L'appareil mobile envoie un message de configuration à l'étape 6, qui contient entre autres le numéro de téléphone de la personne à appeler.
- Le MSC accuse réception de la demande avec un message de poursuite d'appel à l'étape 7.
- Comme le MSC considère le VANC comme un contrôleur de station de base GSM ou un contrôleur de réseau UMTS Radio, il envoie ensuite un message de demande d'assignation au VANC pour demander l'établissement d'un canal de support à commutation de circuits.
- Le VANC traduit ce message en un message Activate Channel sur l'appareil mobile à l'étape 9 pour le préparer à l'échange de paquets IP contenant des données vocales.
- Facultativement, la qualité de service pour les paquets vocaux peut être assurée en activant un deuxième support dans le réseau LTE (étape 11).
- Une fois que le dispositif mobile est préparé pour le flux de données vocales, un message de réponse d'assignation est renvoyé au MSC à l'étape 13 pour lui signaler la « pseudo » mise en place réussie d'un canal à commutation de circuits dans le réseau radio.
- Une fois l'appel établi avec l'autre partie, le MSC envoie des messages d'alerte et de connexion (étapes 14 et 15) que l'appareil mobile accuse réception.
- Le chemin vocal est alors établi et la conversation vocale peut commencer.
- Le signal vocal est transmis dans un intervalle de temps TDM à 64 kbit/s sur l'interface A dans le cas d'un MSC GSM ou via un flux de données IP dans le cas d'un MSC UMTS. Le VANC traduit ce flux de données en paquets IP pour la transmission sur le réseau LTE et vice versa.
- Le protocole de transfert en temps réel (RTP) normalisé est utilisé à cette fin et il s'agit du même protocole RTP qui est également utilisé par de nombreuses autres solutions de voix sur IP telles que celles utilisant SIP et IMS.

PS: les appels vocaux entrants fonctionnent de la même manière.

II-4-3) VoLTE (voice over LTE) via IP Multimedia Subsystem

L'IMS est une architecture normalisée de connectivité IP et de contrôle de service indépendante de l'accès. Il fournit le cadre des services multimédias basés sur IP dans un réseau mobile et constitue un choix optimal pour offrir des services de voix sur IP.

IMS a été spécifié pour la première fois dans la version 5 du 3GPP et amélioré dans les versions ultérieures du 3GPP grâce à un ensemble de fonctionnalités puissant prenant en charge une large gamme d'applications multimédias. D'un autre côté, les spécifications IMS sont devenues assez complexes, car elles contiennent un large éventail d'options. Entre autres raisons, cela a retardé le déploiement commercial d'IMS. depuis, de plus en plus de déploiements IMS commerciaux ont eu lieu **[9]**.

Aujourd'hui, l'industrie mobile considère IMS comme la principale solution de prise en charge des services voix et SMS en LTE. Un profil Voice over IMS a été défini et ne contient que les fonctionnalités du réseau et du terminal considéré comme essentielles pour le lancement de la voix basée sur IMS.

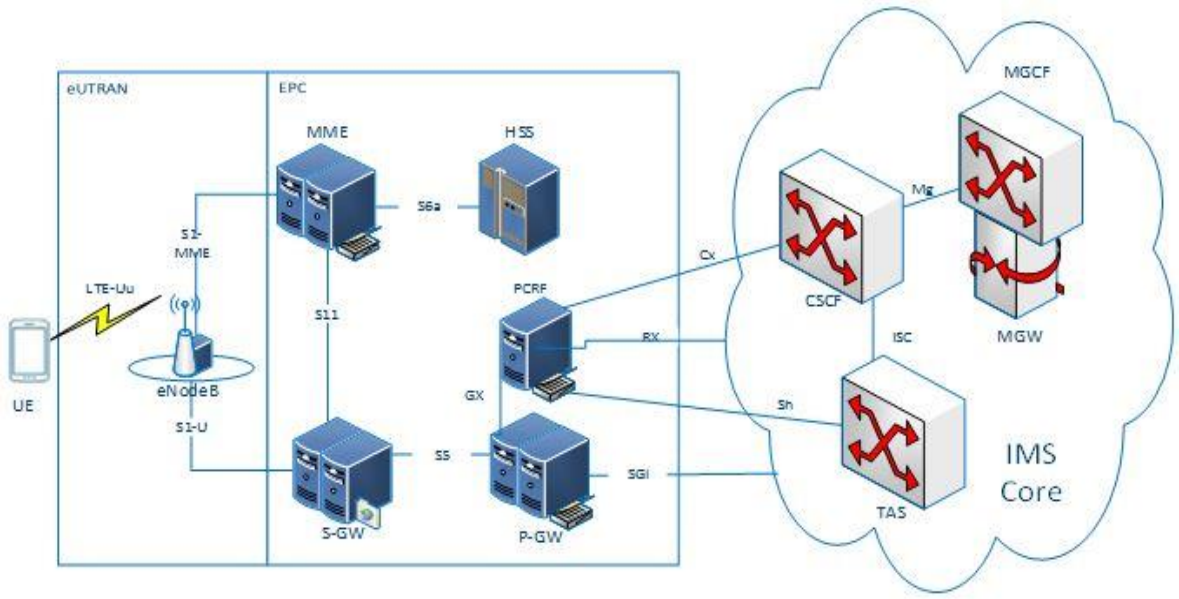


Figure II- 5: VoLTE utilisant l'architecture IMS.

Le réseau IMS est principalement utilisé pour fournir tous les services de base pour la voix fournis par les réseaux CS existants. En outre, il fournit également des services multimédias améliorés comme la vidéoconférence, les jeux en temps réel, etc. Le principal avantage de l'utilisation d'une solution basée sur IMS est qu'elle utilise complètement

l'architecture LTE plutôt que de s'appuyer sur les réseaux CS existants pour prendre en charge la fonction vocale. Le réseau IMS est également capable de s'intégrer aux réseaux 2G/3G hérités et peut ainsi prendre en charge la continuité des appels vocaux même lorsque l'abonné quitte la couverture LTE. Par conséquent, l'abonné peut bénéficier des mêmes services même lorsqu'il se déplace sur des réseaux hérités. Cette solution est projetée comme la solution à long terme car elle est capable de fournir des services améliorés au réseau LTE et prend également en charge l'intégration avec les réseaux 2G/ 3G existants.

II-5) Conclusion

La 4G LTE Long Term Evolution utilise une architecture simplifiée avec un réseau entièrement basé sur IP, cela devait faire évoluer le débit dans les services fournis et améliorer à la fois la QoS et la QoE, la voix reste le service le plus important, que le LTE peut offrir une multitude de solutions pour sa prise en charge.

La voix peut être prise en charge en utilisant la réélection de cellules vers des cellules 2G ou 3G avec un réseau à commutation de circuits, ou en s'inscrivant sur le centre de commutation mobile, mais cela ne semble pas être une vraie solution car elle nécessite et se base sur d'autres réseaux d'accès des générations précédentes qui utilisent le domaine CS pour la voix.

C'est pourquoi la solution IMS devient la mieux indiquée pour la VoLTE.

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

Chapitre III:

IMS
Solution pour la VoLTE

Chapitre III: IMS solution pour la VoLTE

III-1) Introduction

Par le passé, alors que les opérateurs mobiles fournissaient le service téléphonique numérique via des réseaux à commutation de circuits plutôt qu'IP, le développement des LAN et d'Internet faisait de l'IP de facto la méthode omniprésente de transfert de données. Des méthodes alternatives souvent propriétaires de voix sur IP (VOIP) ont vu le jour et sont devenues disponibles sur des Smartphones sans qu'elles ne soient standardisées.

Les travaux des organismes internationaux de normalisation ont abouti, au bout de quelques années, à l'adoption de l'IMS qui s'est alors imposée comme une architecture multimédia normalisée.

Depuis que l'introduction de l'IMS a affecté de manière significative le fonctionnement et le déploiement de réseaux sans fil, une grande partie de l'attention a été accordée au sous système multimédia IMS lui-même.

Ce chapitre fournit une vue d'ensemble de l'IMS, de son architecture et de ses applications du point de vue du LTE.

III-2) Sous-système multimédia IP

L'histoire de l'IMS a commencé avec le 3G.IP, un consortium désormais disparu des principaux influenceurs de l'industrie. Le concept de l'architecture IMS a été par la suite réapproprié et introduit par la 3GPP pour le réseau cellulaire en 2002 (release 5: "IMS avec UTRAN access"). D'autres extensions ont suivi.

L'IMS était donc originellement conçu pour les réseaux mobiles et visait à assurer la compatibilité entre les réseaux cellulaires, les réseaux à commutation de circuit (PSTN) et l'internet **[9]**.

L'organisme 3GPP avait repris sous forme d'extensions les concepts déjà définis et éprouves par l'IETF avec les deux grandes familles de protocole SIP et DIAMETER.

Il fut en 2005 adopté pour les réseaux fixes par le groupe de travail TISPAN relevant de l'ETSI pour permettre essentiellement la convergence fixe/mobile.

D'autre entités de normalisation tels que l'UIT ont été également impliquées. En 2010, le GSMA adoptait finalement -dans sa version 1.0 qui décrit le profil de la voix sur IMS- le travail du groupe one Voice call composé d'équipementiers tels que ALCATEL-LUCENT, Ericsson, Nokia, Siemens, Samsung etc, et d'opérateurs tels que ATT, Orange, Vodafone et Telefonica etc.

L'IMS est finalement une architecture standardisée définie par les 3GPP, l'ETSI et L'IETF basée sur le protocole SIP d'initialisation des sessions multimédias, et le protocole RTP pour le transport de flux multimédias.

Adaptée aux réseaux fixe et mobile, elle favorise la convergence fixe mobile et permet l'interfonctionnement avec les réseaux RTC.

L'IMS autant que sous réseau multimédia est une couche fédératrice qui vient se superposer aux réseaux actuels (d'accès et de services), dans la mesure où il permet:

- Le traitement des flux multimédias à partir de tout type réseau d'accès (Wifi, xDSL , GSM, Ethernet, UMTS...) qu'elle que soit sa nature fixe ou mobile;
- Aux opérateurs télécoms d'utiliser des services fournis par des architectures de réseaux sous jacentes **[9]**.

III-3) Architecture IMS

L'architecture IMS qui en résulte définit les éléments et les fonctions sur quatre (04) couches indépendantes:

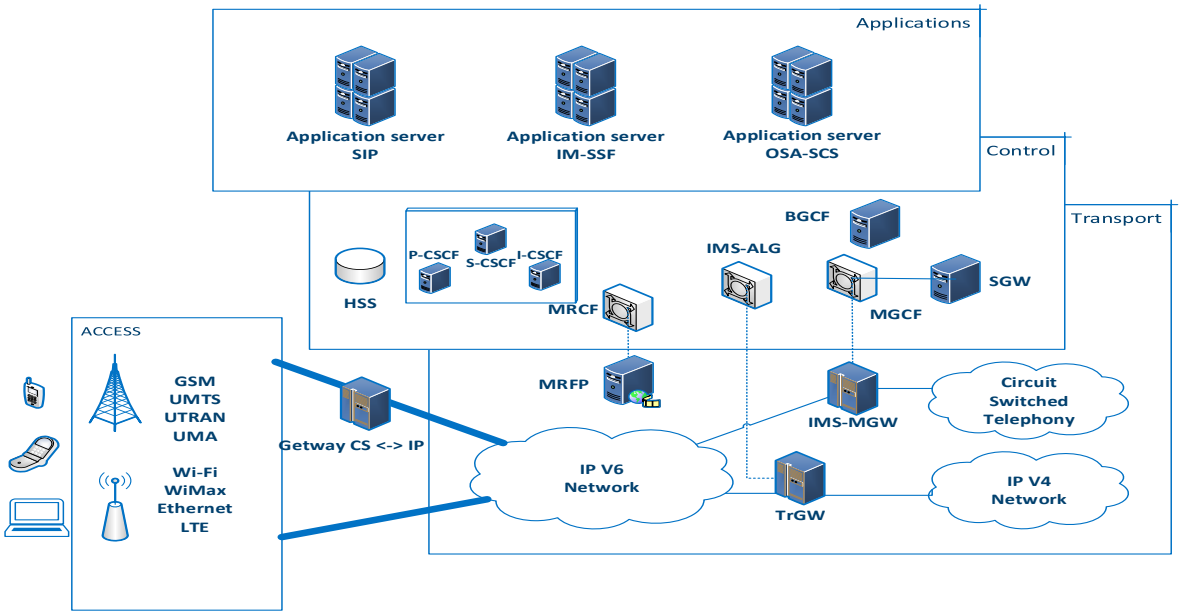


Figure III-1: Architecture IMS basée sur des couches **[9]**.

III-3-1) La couche d'accès

Elle définit la façon dont l'utilisateur se connecte au réseau. Parmi les réseaux d'accès figurent aussi bien les réseaux mobiles (E-UTRAN, GSM, UMTS ,CDMA 2000) que les réseaux fixes et sans fil (xDSL, WiFi, WiMax, Ethernet, fibre optique .. . etc).

III-3-2) La couche transport

La couche transport est une couche IP générique. Elle se compose d'un maillage de commutateurs et de routeurs qui assurent le routage des données multimédias dans le réseau IP. C'est à son niveau que se réalise via des passerelles PSTN la convergence entre réseau à routage par paquet et réseau à commutation de circuits.

III-3-3) La couche de contrôle

La couche de contrôle gère et contrôle le réseau. Elle est responsable de tous les messages de signalisation du réseau permettant d'ouvrir, de maintenir, de modifier et de mettre fin à une session entre utilisateurs. C'est la partie **intelligente** du modèle, qui offre toutes les fonctionnalités de gestion des utilisateurs et constitue la **véritable base** d'IMS.

III-3-4) Couche d'application

Cette couche consiste en la fourniture de services, qu'ils soient audio, vidéo ou texte. Cette couche implémente tous les services pouvant être proposés aux utilisateurs. Il s'agit de la partie la **plus ouverte du modèle**, car le réseau IMS ne spécifie pas les services eux-mêmes, mais offre une plateforme de déploiement unifiée, simple, rapide, productive et sécurisée pour le déploiement de nouveaux services **[9]**.

III-4) Les principaux composants de l'architecture IMS

L'architecture de l'IMS repose sur les entités logiques décrites ci-après, nécessaires à son bon fonctionnement.

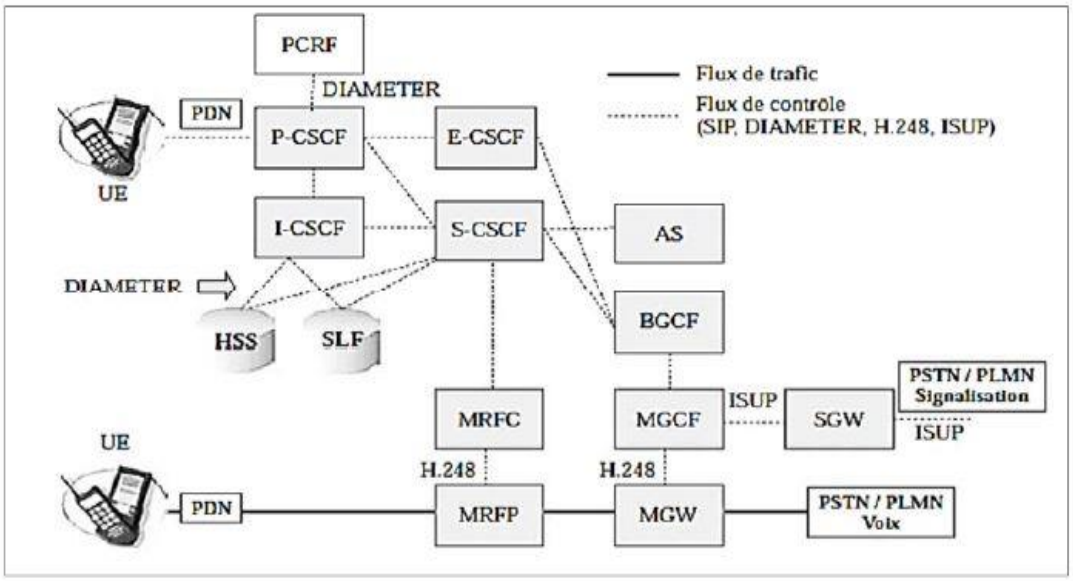


*Figure III-2: Les entités du réseau IMS **[10]**.*

III-4-1) Serveur d'abonné domestique (HSS)

Le HSS est une base de données qui contient les informations spécifiques à chaque utilisateur, à savoir:

- Les identités IMPI et IMPU;
- Les paramètres d'authentification qui servent au contrôle d'accès du mobile à l'EPS lors de l'attachement et à l'IMS lors de l'enregistrement;
- Le profil de service: qui détermine les services auxquels est souscrit l'utilisateur.

Le HSS est accessible au:

- S-CSCF pour la fourniture des données d'authentification et le profil de service;
- I-CSCF pour retrouver l'identité du S-CSCF rattaché à l'utilisateur;
- Serveur application pour indiquer les données de service afférentes à chaque utilisateur.

III-4-2) Fonction de localisation d'abonné (SLF)

Quand le nombre des utilisateurs est important, il est possible de les repartir entre plusieurs HSS. Dans pareil cas, il est nécessaire de faire appel à une autre entité le SLF qui a pour rôle d'assurer le suivi de plusieurs HSS dans un réseau domestique et être responsable d'en attribuer un à un utilisateur. D'autre part et au cas où un HSS tombe en panne, il peut être reconnu par un SLF dans le temps, et le chemin d'accès au CSCF peut être commuté automatiquement sur un HSS de secours, ce qui permet de garantir la validité du service.

III-4-3) les serveurs CSCF(Fonction de commande de session d'appel)

Le CSCF est responsable de l'établissement, du suivi, du soutien et de la diffusion des sessions multimédias. Il est composé de trois entités, qui peuvent être ou non des entités physiques distinctes:

Proxy CSCF (P-CSCF)

Le P-CSCF est le premier point de contact du mobile dans le réseau IMS et assure, à ce titre, la fonction de PROXY SERVER. Il reçoit les requêtes provenant de l'UE ou du S-CSCF et les transfère respectivement vers le I-CSCF ou l'UE.

Le P-CSCF génère les données nécessaires à la taxation .

Le P-CSCF établit un tunnel sécurisé IP Sec avec l'UE, lors de la phase de d'enregistrement.

L'entité P-CSCF est aussi responsable, lors de l'établissement d'une session, au contrôle du type de ressources requises par l'UE sur la base des capacités autorisés par le réseau EPS, à travers l'échange de messages avec le PCRF **[11]**.

Interrogating CSCF (I-CSCF)

La I-CSCF est l'entité qui initie l'affectation d'un utilisateur à un S-CSCF (en interrogeant le HSS) pendant l'enregistrement. Il sert de liaison pour la messagerie SIP entre l'utilisateur (via le P-CSCF) et le S-CSCF **[11]**.

Serving CSCF (S-CSCF)

Le S-CSCF est un serveur SIP considéré logiquement comme faisant partie du réseau domestique. le S-CSCF est la **cheville ouvrière** du réseau cœur IMS et joue à ce titre plusieurs rôles:

- L'authentification de l'utilisateur: Une fois désigné pour servir la session d'un utilisateur, il récupère auprès de la base HSS via le protocole DIAMETER, l'ensemble des paramètres du profil d'utilisateur pour l'enregistrer, l'authentifier et vérifier ses droits d'accès.
- Le contrôle de toute signalisation SIP provenant et à destination de l'utilisateur.
- Le maintien de l'état de la session en cours.
- Le routage des appels. En particulier, si l'adresse de destination n'est pas une adresse SIP, mais, par exemple, un numéro de téléphone standard, le serveur S-CSCF fournit les fonctionnalités de conversion pour joindre les passerelles téléphoniques.
- La sélection des serveurs d'applications: du fait qu'il connaît l'utilisateur et les applications disponibles pour l'utilisateur, il constitue un point de décision pour savoir si les messages SIP de l'utilisateur seront transmis aux serveurs d'application adéquats **[11]**.
- Fourniture de l'historique des communications utiles pour la facturation.
- Le serveur S-CSCF est déterminé grâce au serveur I-CSCF. Il en informe alors le P-CSCF, de manière que ce dernier puisse ultérieurement s'adresser directement au S-CSCF sans passer par l' I-CSCF.
- Parallèlement, le S-CSCF enregistre dans le HSS la position de l'abonné dans le réseau et indique au HSS son adresse, afin qu'une entité cherchant à joindre l'abonné détermine le S-CSCF auquel elle doit s'adresser.

III-4-4) Fonction de commande de passerelle de sortie (BGCF)

L'entité BGCF a pour fonction d'indiquer si une session courante se termine sur un réseau tiers IMS ou un réseau RTC et de déterminer laquelle des passerelles qui se chargera de la traiter.

Dans le cas d'une interconnexion avec les réseaux PSTN ou PLMN: l'entité BGCF traite la requête (INVITE) transmise par S-CSCF via l'interface Mi et détermine à partir du

numéro téléphone appelé, l'entité MGCF responsable de l'interfonctionnement avec les réseaux PSTN ou PLMN **[9]**.

III-4-5) Fonction de contrôle de passerelle média (MGCF)

L'entité MGCF (comme son nom l'indique) est responsable de la fonction de contrôle de passerelle média. Elle est, à ce titre, chargée de:

- Effectuer la traduction entre la signalisation SS7 du réseau téléphonique à commutation de circuit et la signalisation SIP, à travers le SGW;
- Commander via la signalisation H248 la passerelle d'interconnexion IMS-MGW en contrôlant l'établissement, le maintien et la libération des connexions de ladite passerelle.

La passerelle IMS-MGW adapte les formats de transport des flux de données entre les deux réseaux (la conversion des médias entre le protocole de transport en temps réel (RTP) utilisé dans l'IMS et la modulation codée par impulsions (PCM) utilisée par le réseau à commutation de circuits CS) et effectue les traitements sur les flux médias (Transcodage, annulation d'écho) **[9]**.

Dans le cas d'un appel sortant d'un domaine IMS à un autre IMS, l'entité BGCF se charge de la recherche de l'entité à laquelle est assigné le contrôle de l'interconnexion:

- L'entité IBCF (Interconnexion Border Control Function) est la passerelle qui permet l'accès de la signalisation SIP à un réseau tiers IMS;
- L'entité TrGW (Transition Gateway) est la passerelle qui permet le transfert du flux RTP à un réseau tiers IMS.

III-4-6) Fonction de ressource Multimédias (MRF)

L'entité MRF assure les fonctions de contrôle de medias et de ressources médias. Elle se décompose de deux entités logiques :

- **MRFC** (MultiMedia Resource Function Controller): Qui sert pour la partie signalisation à la négociation des paramètres sollicités par chaque utilisateur pour la mise en œuvre de la ressource média et à son contrôle lors de l'utilisation. Pour ce faire, il interagit, d'une part avec le MRFP (auquel il peut être intégré) via le protocole H248 et l'entité S-CSCF à travers l'interface Mr

supportée par le protocole SIP, d'autre part. il est, en outre, responsable de la génération de l'information de taxation selon un format standard défini par le 3GPP.

- **MRFP** (MultiMedia Resource Function Processor): Est l'équipement qui fournit la ressource média sous le contrôle du MRFC. Il est, à ce titre, chargé du traitement des flux de données, de la traduction et du mélange des flux média (ex. conférence).

Les principales fonctionnalités d'un MRFP consistent à :

- Fournir les ressources média sous le contrôle du MRFC.
- Délivrer les annonces: similaires par exemple au message courant "le numéro que vous avez composé n'est plus en service". L'utilisation d'un MRFP pour réaliser de tels services d'annonces permet de ne pas avoir à déployer un nouveau serveur d'annonces; réduisant ainsi le nombre d'éléments de réseau et simplifiant la gestion de réseau. Un équipement de stockage externe peut être utilisé.
- Enregistrer et restituer ultérieurement des messages multimédias tels que la messagerie vocale, la messagerie unifiée, le push-totalk et la conférence. Le MRFP utilise des serveurs de stockage existants chez l'opérateur de service.
- Gérer les conférences multimédias: Le MRFP doit être capable de fournir tous les mécanismes de contrôle des appels à plusieurs participants. Cette fonctionnalité est utilisée dans de nombreuses applications telles que la conférence ou le push to talk.
- Assurer le transcodage qui permet de convertir un schéma d'encodage numérique en un autre. Dans le cas d'une conférence ou les participants ne disposent pas d'un même codec commun, le MRFP assurera alors les traductions de média nécessaires **[9]**.

III-4-7) Les serveurs d'applications AS

Dans une architecture IMS, la couche application est totalement indépendante des autres couches. L'opérateur peut se positionner grâce à sa couche Contrôle en tant qu'agrégateur de services offerts par l'opérateur lui-même ou par des tiers.

Les serveurs d'applications ou AS (Application Server) sont des serveurs SIP qui hébergent et fournissent différent types de services aux utilisateurs. Invoques par le serveur S-CSCF via l'interface ISC supportée par le protocole SIP, ils influencent sur le déroulement de la session SIP en fonction de la demande de service.

Ils interagissent aussi, à travers DIAMETER, avec le HSS afin d'obtenir les données de service d'un utilisateur.

Un serveur d'application (AS) contient un ou plusieurs services et les utilisateurs peuvent associer plus qu'une AS en fonction de leurs profils.

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, messagerie instantanée, etc.) sont généralement implémentés au sein de ces serveurs.

- **IM-SSF (IP MultiMedia-Service Switching Function):**

La fonction IM-SS est conçue pour permettre aux opérateurs mobiles de réutiliser l'infrastructure de leur application existante 2G pour l'IMS, et ce pour éviter des surcouts.

L'IM-SSF est spécifiquement indiquée pour permettre au réseau IMS d'utiliser la plateforme déployée en 2G.

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 IM-SSF, afin de connecter l'abonné au serveur d'applications de son opérateur.

L'IM-SSF permet ainsi d'accéder à des services distants en réalisant l'interface entre, d'un côté, le serveur S-CSCF communiquant avec le protocole SIP et, de l'autre côté, des serveurs distants en communiquant avec le protocole CAP.

- **La passerelle OSA (OSA SCS, OSA Service Capability Server)**

Est un type particulier de serveur d'application qui termine la signalisation SIP et interagit avec les applications OSA.

Les serveurs OSA-SCS (Open Service Access-Service Capability Server) fournissent le moyen d'interagir avec les serveurs d'applications OSA. OSA conçue pour fournir une API qui facilite le développement des services, a été définie par le 3GPP et l'ETSI comme une architecture de gestion des services dans un réseau téléphonique de troisième génération. Son objectif est de permettre aux développeurs tiers d'offrir aux usagers leurs applications indépendamment des technologies utilisées. Ces applications sont accessibles à l'IMS grâce au serveur OSA-SCS.

Le S-CSCF interagit avec les OSA à travers la passerelle OSA-SCS via l'interface ISC, qui est donc vu comme un serveur d'application à l'instar de l'IM-SSF **[9]**.

III-5) Gestion des identités en IMS

Dans le système IMS, un nouveau concept d'identification est adopté mais qui reste compatible avec les anciens réseaux comme le GSM. Les utilisateurs dans IMS sont identifiés à travers un couple d'identifiants : un identifiant public et un identifiant privé.

- **Identité publique de l'utilisateur IMPU** (IP Multimedia public Identity)

L'Identité publique IMPU est une identité publique attribuée par l'opérateur à l'utilisateur IMS. Chaque utilisateur peut avoir un ou plusieurs identifiants publics qui est similaire au MSISDN (Mobile Station ISDN Number) dans les réseaux GSM et UMTS. C'est une adresse de contact qui permet **de joindre** un abonné et **de router** les messages SIP.

Comme le réseau IMS s'interconnecte avec un réseau RTC, ses utilisateurs ont besoin d'un numéro téléphonique classique pour appeler et être joints.

Ainsi, l'IMPU se présente sous deux formats :

Format SIP URI : "sip:user@domaine.com".

Format TEL URI : "tel: 514 000 0000".

- **Identité privée de l'utilisateur IMPI** (IP Multimedia Private Identity)

L'identité privée IMPI est une identité **unique** pour chaque utilisateur qui est stockée dans la carte à puce. Cette identité de la forme d'une **adresse e-mail** sert à

l'authentification et **l'enregistrement** de l'utilisateur au sein du réseau IMS. L'identité privée unique de l'utilisateur IMS est associée à l'ensemble des IMPU que l'utilisateur peut posséder.

L'ensemble des identités IMPI et IMPU de chaque utilisateur est stocké dans le profil de l'usager au sein de la base de données de HSS **[10]**.

III-6) Protocoles clés utilisés dans le réseau LTE-IMS

III-6-1) Le protocole DIAMETER

DIAMETER est un protocole particulier utilisé par le 3GPP pour les architectures LTE et IMS.

À l'origine ce protocole a été dérivé du protocole RADIUS qui permettait des services AAA aux ordinateurs afin de se connecter et d'utiliser un réseau. DIAMETER est une version améliorée de protocole RADIUS car il apporte de nombreuses améliorations dans la fiabilité da la livraison de messages et le traitement des erreurs. Il est le protocole le plus à même de répondre aux nouveaux besoins liés à la mobilité de **l'utilisateur**.

Le protocole DIAMETER est utilisé pour remplir les fonctions **AAA** suivantes:

- La fonction **d'authentification** permet de contrôler l'accès du mobile au réseau à partir de l'identité du mobile stockée d'une part dans le module USIM de la carte UIGC du mobile et d'autre part dans le HSS.
- La fonction **d'autorisation** permet de récupérer le profil de service et de trafic du mobile stocké dans les bases de données du HSS.
- La fonction **de comptabilité** (**Accouting**) permet la génération d'événements de la part du P-GW vers les entités de taxation, après la collecte des informations sur l'utilisation des ressources par le PCRF **[12]**.

Les messages DIAMETER sont échangés entre, d'une part, les entités CSCF du réseau IMS et l'entité HSS lors de l'enregistrement de l'UE ou du routage de la demande SIP et l'entité PCRF pour le contrôle des médias d'autre part **[13].**

Messages liés à l'enregistrement et au routage

La requête UAR et la réponse UAA (User-Authorization-Request /Answer): Utilisées entre les entités I-CSCF et HSS pendant les deux phases d'enregistrement de l'UE**:** À la réception d'une requête REGISTER, l'entité I-CSCF interroge l'entité HSS afin de récupérer la liste des entités S-CSCF qu'il est possible d'attribuer à l'entité UA (première phase) et l'adresse IP de l'entité S-CSCF attribuée à l'entité UA (deuxième phase).

La requête MAR et réponse MAA (Multimedia Auth-Request/Answer): Lors de la première phase d'enregistrement, à la réception de la requête REGISTER, l'entité S-CSCF fournit son adresse IP et récupère du HSS les données d'authentification de l'entité UA.

La requête SAR et la réponse SAA (Server-Assignment-Request /Answer): Utilisées entre les entités S-CSCF et HSS pendant la deuxième phase d'enregistrement, à la réception de la requête REGISTER, l'entité S-CSCF s'enregistre auprès de l'entité HSS et télécharge le profil de l'entité UA.

La requête RTR et réponse RTA (Registration-Termination-Request / Answer): Sont utilisées entre les entités HSS et S-CSCF lorsque l'entité HSS déclenche le désenregistrement de l'entité UA.

La requête LIR et la réponse LIA (Location-Info-Request/Answer): Utilisées entre les entités I-CSCF et HSS pour le routage de La Requête INVITE: Lors d'un appel entrant, à la réception de La Requête INVITE, l'entité I-CSCF récupère l'identité de la S-CSCF attribuée à l'agent de destination.

La requête PPR et la réponse PPA (Push-Profile-Request/Answer): Sont utilisées entre les entités HSS et S-CSCF. Ils permettent au HSS de notifier une modification du profil de l'entité UA **[13]**.

Messages liés au contrôle des médias

Les messages liés au contrôle des médias sont échangés entre les entités P-CSCF et PCRF lors de l'établissement d'une session.

La requête AAR (Authentication Authorization-Request): Est utilisée par le P-CSCF pour transmettre au PCRF les caractéristiques du support négocié dans le message SDP.

La réponse AAA (Authentication Authorization-Answer): De l'entité PCRF accuse réception de La requête, si les codecs multimédias sont autorisés.

La requête STR (Session-Termination-Request): Est utilisé par la fonction P-CSCF pour informer l'entité PCRF de la fin de la session SIP.

La réponse STA (Session-Termination-Answer): De l'entité PCRF accuse réception de la requête **STR**. A réception de cette requête, l'entité PCRF libère les ressources immobilisées dans le réseau EPS.

La requête ASR (Abort-Session-Request): Est utilisé par l'entité PCRF pour informer le P-CSCF que les ressources réservées par le réseau EPS ne sont plus disponibles.

La réponse ASA (Abort-Session-Answer): Accuse réception de la requête. Dès réception de cette demande, l'entité P-CSCF met fin à la session SIP en envoyant une demande BYE à chaque entité UA participant à la session.

III-6-2) Le protocole SIP (Session Initiation Protocol)

Le protocole SIP est le protocole clef de l'architecture IMS. c'est une norme conçue par l'IETF, retenue par le 3GPP pour permettre de créer des sessions interactives entre plusieurs entités (poste à poste, client/serveur) d'un réseau mobile. C'est un protocole de signalisation appartenant à la couche application du modèle OSI qui a l'avantage d'être indépendant du transport des couches basses.

Il sert à établir, modifier et terminer différentes sessions multimédias entre deux ou plusieurs utilisateurs.

Le protocole SIP utilise les principes des protocoles HTTP (les codes de réponse SIP sont issus du HTTP) et SMTP et est basé sur une paire requête/réponse. Chaque transaction consiste en **une requête**, utilisant une méthode particulière **et une ou plusieurs** réponses **[14]**.

La création et l'utilisation de sessions impliquent un ensemble de fonctionnalités auxquelles le protocole SIP répond:

- Localisation: SIP utilise les URI (Uniform Resource Indicator) afin de localiser les utilisateurs au sein d'un réseau. La syntaxe utilisée est courante car elle reprend celle des adresses e-mail. Au préalable, l'usager s'enregistre auprès

d'un serveur SIP via une requête afin d'être authentifié et reconnu comme joignable.

- Négociation: Avant que la session ne soit créée, les usagers doivent négocier les informations qui seront échangées telles que le choix du type de médias (vidéo, voix, texte…) selon un ordre de priorité des CODECs dépendant des terminaux de chacun des usagers. C'est à ce niveau que le protocole SIP est utilisé en corrélation avec le protocole SDP; en effet le corps des messages SIP utilise le protocole SDP, pour la description de flux issus de médias (adresses et ports utilisés, type de média, codage, etc.). SDP joue le rôle de support lors du processus préalable de négociation de la communication.
- Gestion: une fois la session initiée, il faut pouvoir intervenir sur son déroulement et la terminer. Il est possible de faire face à un changement de terminal et par conséquent à une renégociation des médias en jeu.

Les requêtes

Avant d'entamer cette partie, il importe de définir un agent utilisateur UA: Il s'agit d'un point d'extrémité (qui peut être un soft phone, un mobile ou un ordinateur portable) et de l'un des éléments des plus importants et des plus intelligents d'un réseau SIP.

Un point de terminaison peut lancer, modifier ou mettre fin à une session.

Les agents utilisateurs sont logiquement divisés en deux parties :

- User Agent Client (UAC): Entité qui envoie une demande et reçoit une réponse;
- Serveur d'agent utilisateur (UAS): Entité qui reçoit une demande et envoie une réponse.

SIP est basé sur une architecture client-serveur où le téléphone de l'appelant agit comme un client qui initie un appel et le téléphone de l'appelé agit comme un serveur qui répond à l'appel.

La requête est constituée de messages définissant la nature de la transaction (invitation, demande d'information, souscription etc.…).

Toute requête commence par une ligne contenant la **méthode**, un URI et la version du protocole. Elle contient ensuite un certain de champs d'en-têtes, d'une ligne vide et d'un corps de message.

La méthode REGISTER: Est utilisée par une entité UA pour notifier à l'entité REGISTRAR la correspondance entre l'adresse IP de l'UA et son identité d'entité URI. Cette correspondance est requise pour les appels entrants.

La méthode INVITE: Est utilisée par une entité UAS invitée à participer à une session. Les réponse définitives, positives ou négatives, doivent être validées par la demande ACK. La requête INVITE contient un corps de message décrivant le support que l'entité UAC appelante souhaite établie.

La méthode ACK: Est utilisée pour accuser réception qui confirme que le terminal appelant a bien reçu une réponse définitive (2xx, 3xx, 4xx, 5xx, 6xx) à une requête INVITE.

La requête ACK peut contenir un corps de message décrivant le support dans le cas où cette description n'est pas fournie dans la première demande INVITE.

La méthode BYE: Est utilisée par le terminal de l'appelé UAS à fin de signaler qu'il souhaite mettre un terme à la session. Une session n'est considérée comme établie que lorsque la réponse 2XX est reçue à la suite de la demande INVITE.

La méthode CANCEL: Est utilisée pour terminer une session infructueuse (non validée par une réponse finale). Elle est générée lorsqu'une réponse temporaire 1xx a été reçue, mais aucune réponse définitive. Si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête ACK, alors elle émet une requete CANCEL.

La méthode PRACK: La méthode PRACK est utilisée pour accuser réception d'une réponse temporaire (1xx), à l'exception de la réponse 100 Trying.

La méthode SUBSCRIBE: La méthode SUBSCRIBE est utilisée lorsqu'une entité UA souhaite s'abonner à un service qui lui permet de recevoir des notifications d'événements.

La méthode NOTIFY: La méthode NOTIFY permet à une entité de notifier l'occurrence d'un événement.

La méthode REFER: Est utilisée pour le transfert d'un client vers une ressource identifiée par la requête. À titre d'exemple, soit A l'entité à l'origine du transfert, B l'entité

transférée et C le destinataire du transfert. Le renvoi consiste à transformer l'appel en cours entre A et B en un nouvel appel entre B et C choisi par A. Quand le transfert aboutit, B et C communiquent alors que A ne pourra plus converser avec B et C.

La méthode MESSAGE: La méthode MESSAGE est utilisée pour transmettre de petits messages, contenus dans un corps de message, entre deux entités UA **[11]**.

Les réponses

Elles constituent les informations renvoyées par le serveur au client ou par le client au serveur et concernent autant l'évolution de la transaction que les erreurs pouvant survenir (transport, serveur, client, etc.). On distingue les réponses **provisionnelles**, qui donnent une information optionnelle, et les réponses **finales** qui clôturent une transition. Une transaction SIP est initiée par **une** requête, suivie **d'une ou plusieurs** réponses provisionnelles.

Type de Réponse	*Désignation*
1xx	Réponse provisoire
2xx	Réponse définitive et positive
3xx	Réponse de redirection définitive
4xx	Réponse définitive et négative, erreur client
5xx	Réponse définitive et négative, erreur réseau
6xx	Réponse définitive et négative, erreur globale

Tableau III-1: Désignation des messages de réponse **[10]**.

Quelques exemples de réponses:

La réponse 100 TRYING: La réponse 100 TRYING est générée par l'entité PROXY SERVER pour informer l'expéditeur de la réception du message SIP. Elle indique donc que la requête a été reçue par l'élément suivant.

Réponse 180 RINGING: La réponse 180 RINGING est utilisée par l'appelé pour indiquer à l'appelant que la demande INVITE a été reçue et que l'appelé est averti d'un appel entrant par une sonnerie.

La réponse 200 OK: La réponse 200 OK a deux utilisations. Lorsqu'il s'agit d'une réponse à une demande INVITE, il contient le corps du message décrivant le média mis en place par l'entité UAS. Pour les autres demandes, la réponse accuse réception de la demande.

401 Unauthorized: Indique que la demande nécessite une authentification de l'agent d'utilisateur. Elle est utilisée par l'entité REGISTRAR à réception d'une demande REGISTRE. La réponse comprend l'en-tête WWW-Authenticate qui contient un défi à partir duquel l'entité UA calcule les données d'authentification.

503 SERVICE INDISPONIBLE: Le service n'est pas disponible pour le moment par surcharge du serveur, maintenance ou dysfonctionnement.

600 BUSY EVERYWHERE: L'appelé a été rejoint, mais il est occupé sur tous les postes et ne peut pas prendre de communication.

III-6-3) Le protocole SDP

Le Protocole SDP fournit une **description** du flux de média pour lequel la configuration de session est mis en œuvre par le protocole SIP. Le message SDP est le corps de message attaché au message SIP. Il apparaît généralement dans la demande INVITE et dans la réponse 200 OK. Les paramètres qui caractérisent le flux des médias sont les suivants:

- Type de support (audio, vidéo, données);
- Le protocole de transport (par exemple RTP);
- Le format du support (par exemple le type de codec pour la voix et la vidéo);
- L'adresse IP à laquelle le média doit être transmis;
- Le numéro de port de destination.

Le message SDP est un ensemble de lignes de format <type> = <valeur>. Le champ <type> contient un caractère; Le contenu du champ <valeur> dépend du type.

Format<type>	Description
V	Version du protocole. Le contenu du champ <valeur> est <0>
O	Origine et ID de session
S	Le nom de la session. Le contenu du champ <valeur> est <->
C	Informations de connexion
T	Durée d'activité de la session. Le contenu du champ <valeur> est <00>
M	Description du média
A	Attribut complémentaire des médias

Tableau III-2: Description des messages SDP **[10]**.

III-6-4) Les protocoles RTP et RTCP

Les protocoles RTP et RTCP permettent respectivement le **transport** et le **contrôle** des flux de données **temps réel** (audio et vidéo) en utilisant aussi bien les modes Unicast (point à point) que Multicast (multipoint). Chacun d'eux utilise un port séparé d'une paire de ports, RTP utilise le port pair et RTCP le port impair qui suit.

le protocole RTCP est un protocole de contrôle des flux RTP qu'il assure le contrôle de qualité, voire même la demande de renégocier les codecs, si par exemple, la bande passante diminue.

Ces deux protocoles de la couche application utilisent les protocoles de transport sous-jacents TCP ou UDP.

Mais l'utilisation de l'UDP est préférée à celle du TCP car il est plus rapide puisqu'il ne nécessite pas d'aller-retour et donc du temps pour vérifier la bonne livraison des paquets, rôle déjà assumé par le protocole RTP.

III-6-5) Le protocole de contrôle de passerelle (H.248, Megaco)

Le protocole MEGACO / H.248 norme commune entre l'IETF et l'UIT a été choisie par le 3GPP pour les réseaux mobiles UMTS pour le contrôle des passerelles MGW.

Ce protocole est utilisé entre les éléments d'une passerelle **multimédia** physiquement décomposée, la passerelle multimédia et un ou plusieurs contrôleurs de

passerelle multimédia, et est l'architecture qui sépare le contrôle d'appel de la conversion **multimédia** entre des réseaux différents.

H.248 / Megaco est un protocole maître/esclave utilisé pour séparer la logique de commande d'appel de la logique de traitement des supports dans une passerelle. Il utilise la couche transport UDP ou TCP.

Bien que le protocole H.248 remplisse les mêmes fonctions que les autres protocoles de contrôle de la passerelle multimédia, à savoir MGCP, il utilise une syntaxe, des commandes et des processus différents et prend en charge une plus large gamme de réseaux.

III-7) La qualité de service QoS dans LTE

L'un des éléments clés d'un réseau IMS est la possibilité d'offrir de bout en bout des mécanismes de garantie de qualité de service qui se focalisent essentiellement sur la partie réseau d'accès.

L'un des avantages de l'utilisation du réseau IMS combiné avec le LTE est la possibilité d'établir des tunnels virtuels appelés "EPS bearer" pour fournir un service de qualité (QoS) qui définit la manière dont les données sont traitées lors de leur transport sur le réseau.

Un bearer EPS se caractérise donc par des paramètres de QoS, étant donné que les applications n'ont pas les mêmes besoins: la Visio et la phonie nécessitent un débit garanti (GBR) alors que le téléchargement se contente de Best Effort (Débit Non Garanti).

Pour différencier les bearer, les flux sont identifiés par deux critères :

- QCI : Identifiant de Qualité de Service QoS;
- ARP : La priorité d'allocation et de rétention.

Ces critères sont spécifiés lors de la mise en place de la connexion PDN (EPS session):

- Lorsque l'utilisateur se connecte au réseau LTE (attachement), il crée un support par défaut qui représente une connectivité permanente mais **sans débit binaire garanti**. Le support par défaut est établi avec les paramètres QCI et ARP fournis par le MME. Ces valeurs sont définies par les

données de souscriptions stockées dans le HSS. Le support par défaut fourni une connectivité IP, le débit n'est pas garanti.

- Lorsque l'utilisateur souhaite établir un appel qui nécessite une certaine qualité de service, comme un appel vocal ou la vidéophonie, le réseau peut établir pour la durée de l'appel un **support dédié** (dedicated bearer) qui prend en charge la qualité de service requise par le flux de service et en particulier qui a un **taux garanti** afin d'émuler le mode circuit. Lors de la requête INVITE , le terminal IMS contacte le CSCF pour négocier un ensemble de caractéristiques média (e.g. les codecs) et de services nécessitant de la QoS spécifique (latence, débit,..). Le P-CSCF à travers le PCRF autorise les flux IP des composants média choisis par le terminal en réalisant une translation des paramètres de la description SDP en des valeurs de QoS IP. Ces valeurs sont ensuite passées à l'aide protocole DIAMETER par le PCRF au PCEF puis au P-GW et transférées ensuite au S-GW. Enfin, le MME transfère les valeurs recrues par le S-GW vers l'eNodeB.

Les supports sont établis après l'authentification et l'enregistrement réussis de l'utilisateur dans le réseau LTE.

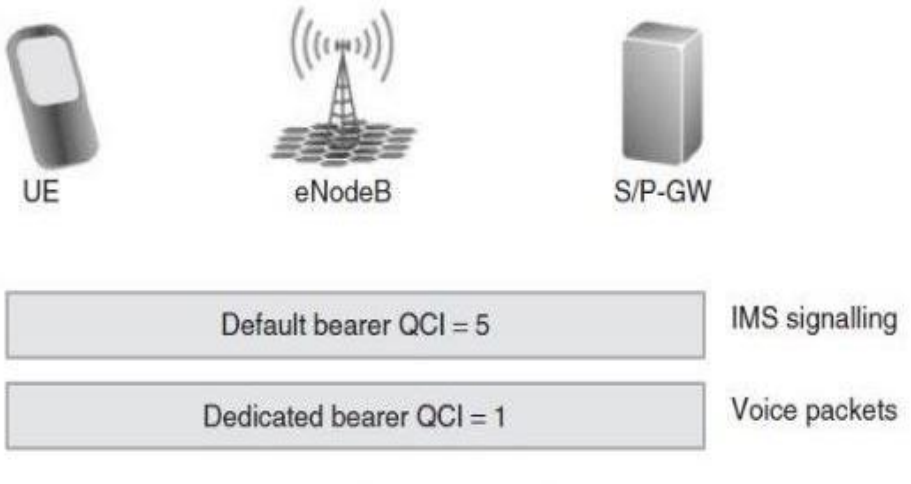


*Figure III-3: Plusieurs porteurs pour la différenciation des QoS **[15]**.*

Le 3GPP définit la classe d'identifiants QoS pour chaque type de média, ces QCI vont de 1 à 9, et deux types de supports, GBR (Guaranteed Bit Rate) et non GBR, selon l'importance de l'application exécutée.

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Services
1	GBR	2	100	10^{-2}	Voice.
2	GBR	4	150	10^{-3}	Voice Conversation (Real Time Streaming).
3	GBR	3	50	10^{-3}	Real Time Gaming.
4	GBR	5	300	10^{-6}	Non Conversational Video (buffered video).
5	Non-GBR	1	100	10^{-6}	IMS Signalling.
6	Non-GBR	6	300	10^{-6}	Video (Buffered Streaming).
7	Non-GBR	7	100	10^{-3}	Interactive Gaming.
8	Non-GBR	8	300	10^{-6}	Video (Buffered Streaming).
9	Non-GBR	9	300	10^{-6}	Video (Buffered Streaming).

*Tableau III-3: Définitions des supports de QoS EPS **[16].***

III-8) Enregistrement et établissement d'appel dans IMS

Ces deux procédures s'appuient pour leur concrétisation sur le protocole SIP et accessoirement sur le protocole DIAMETER **[17]**.

La phase d'attachement de l'UE au réseau LTE préalable à l'enregistrement d'un terminal au réseau IMS n'est pas examinée dans ce chapitre, l'attention est focalisée sur la voix sur IP dans le cœur de la signalisation IMS.

Toutefois, il est utile de préciser que préalablement à toute procédure d'enregistrement réseau IMS, le terminal IMS doit réussir son l'attachement à son réseau

d'accès pour l'obtention d'une connectivité IP qui lui permet d'acquérir une adresse IP et de découvrir celle de son P-CSCF de rattachement.

III-8-1) Enregistrement d'un terminal dans le réseau

L'enregistrement d'un utilisateur dans le réseau est la première action effectuée par un terminal dès sa mise en service, nécessitée par le fait qu'elle permet à l'utilisateur à la fois d'appeler et d'être appelé par ses correspondants.

La méthode associée à cette fonctionnalité est **REGISTER**, à partir du protocole de signalisation SIP.

La figure ci-après illustre les étapes associées au scénario d'enregistrement.

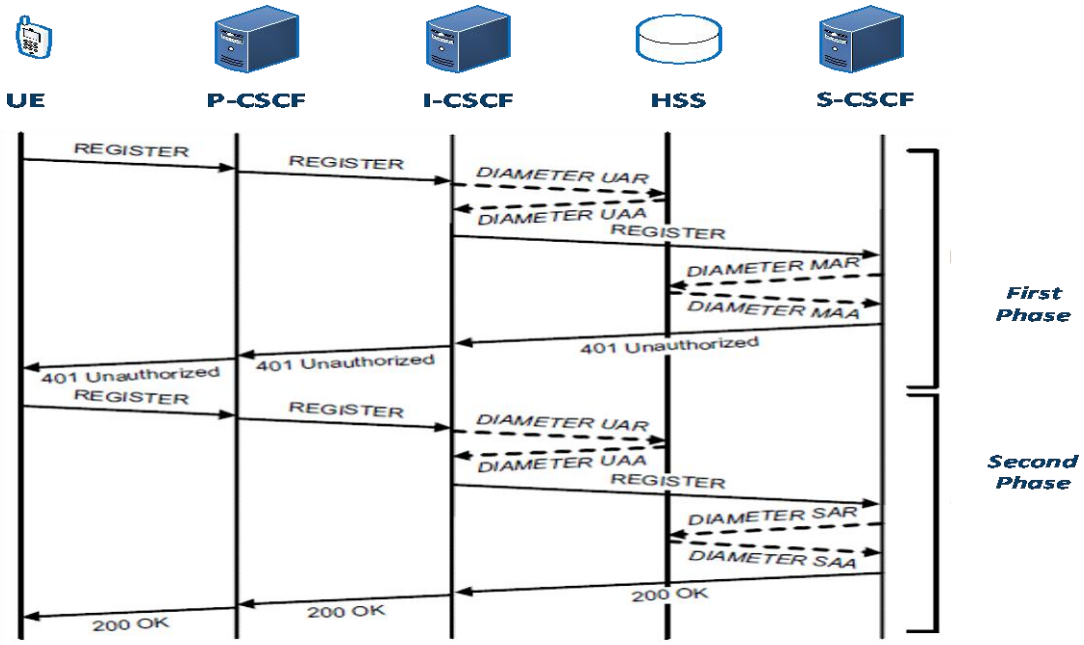


*Figure III-4: Processus d'enregistrement d'un terminal auprès de l'IMS **[17]**.*

Première phase d'enregistrement:

1- Le terminal IMS envoie une demande d'enregistrement REGISTER contenant ses identités IMPI et IMPU au serveur P-CSCF.

2- Le P-CSCF localise le serveur I-CSCF en utilisant DNS qui fait la correspondance entre le nom du domaine fourni par l'utilisateur et l'adresse de l'I-CSCF puis lui transmet la demande de l'utilisateur.

3- L'I-CSCF fait la demande avec une requête UAR au HSS pour sélectionner le S-CSCF.

4- La base de données HSS répond avec la réponse UAA et propose l'ensemble des S-CSCF disponibles. L'I-CSCF en choisit un.

5- Le S-CSCF contacte alors la base de données HSS pour l'informer qu'il a été désigné pour supporter la session de l'utilisateur (demande MAR). il est clair qu'à ce niveau, l'adresse IP de S-CSCF est enregistrée dans le HSS et celle du P-CSCF dans le S-CSCF.

6- Il reçoit en retour une réponse MAA qui confirme l'enregistrement du S-SCSF attribué à l'utilisateur et lui transmet **les vecteurs d'authentification** (dont notamment la réponse attendue **XRES**) de ce dernier qui permettent de générer le challenge.

7- Lorsque le S-CSCF les reçoit, il répond au serveur I-CSCF avec un message SIP 401 Unauthorized, contenant le challenge sous la forme d'un champ d'en-tête appelé WWW-authenticate. Cette réponse est relayée de proche en proche, en passant par I-CSCF d'abord, puis P-CSCF et enfin terminal client **[10]**.

8- À la réception de ce message 401 Unauthorized, le réseau IMS est **authentifié** par le mobile.

Deuxième phase d'enregistrement

1-Lorsque le client reçoit le message de réponse 401, il détecte le challenge et prépare automatiquement une réponse adaptée. Cette réponse est générée dans une nouvelle requête REGISTER qui contient en plus de **l'identité privée** la réponse **RES**, routée en suivant le même chemin que la première requête lors de la première phase.

2- Lorsque la demande atteint le serveur I-CSCF, il fait la même requête (UAR) au HSS qui dans sa réponse (message UAA) fournit l'adresse IP du serveur S-CSCF en charge de la session en cours.

3- A la réception de la requête contenant le RES, le S-CSCF procède à l'authentification de l'utilisateur en reprenant les vecteurs d'authentification contenant le XRES fournis par le HSS à l'étape précédente et qu'il a stockés. Si les paramètres d'authentification RES et XRES sont égaux , **l'authentification du terminal** par le réseau réussit.

4- Le serveur S-CSCF en informe le HSS (via un message SAR) qui répond alors au S-CSCF (via un message SAA) en lui envoyant le profil complet de l'utilisateur, qui est temporairement stocké et sera utilisé pour paramétrer et personnaliser les services de ce dernier.

5- Pour terminer, le serveur S-CSCF envoie un message de réponse 200 OK qui est en fait un message de notification à l'utilisateur du succès de son enregistrement au réseau.

6- Ce message de réponse contient l'adresse SIP de l'utilisateur enregistrée auprès du HSS et l'adresse SIP URI du S-CSCF **[10].**

III-8-2) Connexion de deux utilisateurs

Une communication implique d'abord une première étape de recherche des abonnés suivie d'une deuxième étape de vérification des autorisations d'accès et de négociation de paramètres de qualité de service, conclue par une troisième étape de connexion des correspondants.

La méthode associée à cette dernière fonctionnalité est **INVITE**.

Pour expliquer le processus de déroulement de ces différentes phases d'établissement de communication entre deux utilisateurs, nous considérons le cas le plus général et le plus complet à savoir que les utilisateurs sont d'opérateurs différents et sont situés dans des réseaux visités c'est-à-dire qui n'appartiennent pas nécessairement à leur opérateur respectif.

Ce scénario de liaison de deux terminaux, peut être divisé, comme suit, en sept étapes principales:

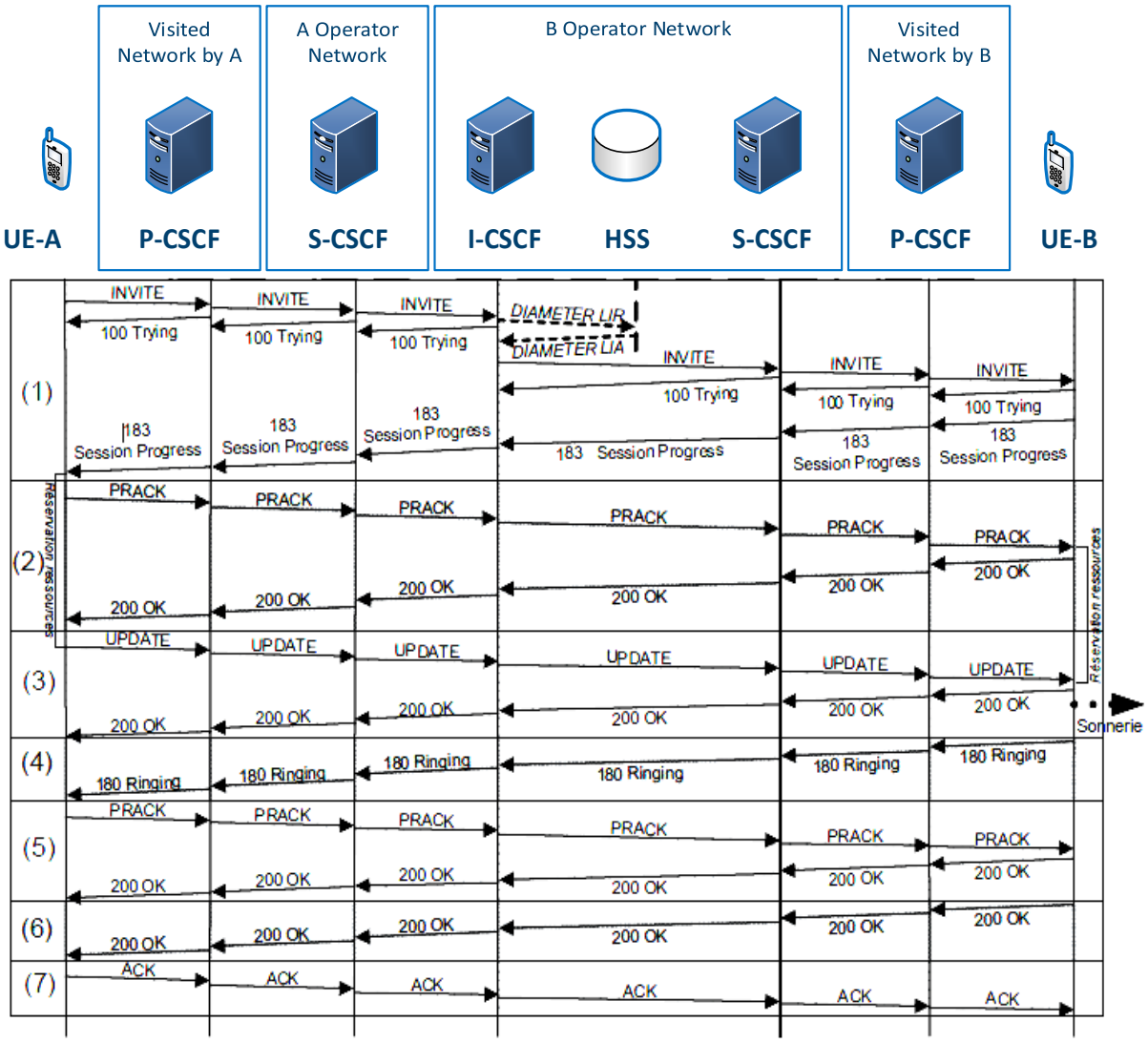


*Figure III-5: Connexion de deux utilisateurs **[17]**.*

1. Message d'invitation INVITE de A vers B:

- La requête INVITE contient un message SDP qui décrit le media que l'utilisateur A souhaite utiliser pour la session ainsi que le codec correspondant.
- Quand le S-CSCF de A reçoit la requête INVITE, il examine le contenu du SDP et le compare avec le profil du l'utilisateur A stocké au niveau du HSS qui contient le type de media autorisé:

  En cas de non concordance, il envoie à A une réponse négative 488.

  Dans le cas contraire, il relaye la requête vers l'I-CSCF de B qui le localise après une requête DIAMETER.

À la requête INVITE, sont associées deux réponses : les réponses provisoires 100 TRYING et 183 Session Progress.

Dans sa réponse 183 Session Progress, B délivre un message SDP qui décrit en autre le choix du codec souhaité par A.

2. L'émetteur A doit assurer B d'avoir bien reçu sa réponse 183 en lui envoyant un accusé de réception temporaire sous forme d'une requête PRACK à laquelle répond B par un message de réponse 200 OK.

3. L'utilisateur A, confirme la réservation de la ressource nécessaire à l'établissement de la session (Qos) dans un message SDP contenu dans sa requête UPDATE.

L'utilisateur B indique qu'il a également réservé les ressources nécessaires à la communication dans le réseau en envoyant la réponse 200 OK.

4. Quand les réservations de ressource sont effectuées aux deux extrémités (A et B), le terminal B commence à sonner et une réponse 180 RINGING est transmise au terminal A qui reçoit une tonalité de retour d'appel.

5. Afin de s'assurer que cette réponse est reçue du terminal A, qui doit en accuser réception par une demande d'accusé de réception PRACK, qui attend elle-même une réponse 200 OK.

6. Une fois que l'utilisateur du terminal B a répondu, la réponse finale 200 est envoyée à la demande d'invitation initiale et qui met fin à la tonalité de retour d'appel chez l'utilisateur A.

7. La demande finale d'accusé de réception valide l'initialisation de la communication, qui peut alors commencer à permettre aux terminaux d'échanger des flux de données multimédias **[17]**.

III-9) Conclusion

Ce chapitre montre que IP Multimedia subsystem est une plateforme IP NGN complète, qui peut offrir en plus d'autres services des applications vocales aux réseaux LTE.

IMS se distingue par sa capacité d'offrir des applications IP à tout réseau d'accès IP, ce qui constitue un moyen très pratique pour les opérateurs de minimiser les coûts d'installation du réseau en déployant une plateforme IMS et en y connectant leurs réseaux.

Dans le même ordre d'idée, IMS peut également être un nœud vers d'autres réseaux NGN.

Le quatrième chapitre présente l'implémentation d'une plateforme IMS en utilisant OpenIMSCore ainsi que la simulation de certains services en utilisant cette plateforme.

Chapitre IV:

Implémentation de l'IMS et simulation

Chapitre IV: implémentation de l'IMS et simulation

IV-1) Introduction

Ce chapitre constitue le cadre applicatif des différentes notions théoriques du noyau IMS abordées et décrites dans le précédent chapitre.

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

Cette plateforme qui donne la possibilité d'implémenter un réseau cœur IMS nous permet d'expérimenter des services s'appuyant sur ce type de réseaux.

La simulation, à travers la plateforme OpenIMSCore, aura donc comme double objectif d'étudier les fonctionnalités et analyser les performances d'un réseau IMS d'une part et de mettre en pratique nos connaissances théoriques en matière d'enregistrement de terminaux IMS et d'échange de flux de signalisation SIP et d'appels (vocaux et messages) sur IMS d'autre part.

IV-2) Open IMS Core

OpenIMSCore est un Projet lancé en 2006 qui a été développé par FOKUS (Institute for Open Communication System), le centre de recherche et développement en télécommunications de l'institut Fraunhofer, basé à Berlin, en Allemagne.

Il a été adopté par les opérateurs des télécommunications comme banc d'essai pour tester les fonctionnalités de l'IMS à l'effet de promouvoir l'adoption de la technologie IMS dans les réseaux de prochaine génération, et ainsi amener le développement de nouveaux services basés sur IMS.

OpenIMSCore est un cœur de réseau IMS basé sur la solution Open Source.

Cette solution garantit les fonctions de contrôle d'un cœur de réseau IMS assurées par les trois serveurs CSCF. Elle fournit également la fonction HSS permettant de provisionner un nombre déterminé d'abonnés et leur associer un profil de service nécessaire à l'invocation des services.

L'OpenIMSCore est finalement une implémentation de fonctions CSCF basées sur des logiciels open source et d'une base de données HSS ou FHoSS (FOKUS Home Subscriber Server) basée sur MySQL **[18]**.

L'essentiel de l'architecture de base de l'OpenIMSCore, illustrée par la figure donnée ci-après, s'articule autour de quatre composantes (PCSCF, ICSCF, SCSCF et HSS) qui forment les éléments de base de toute infrastructure IMS/NGN.

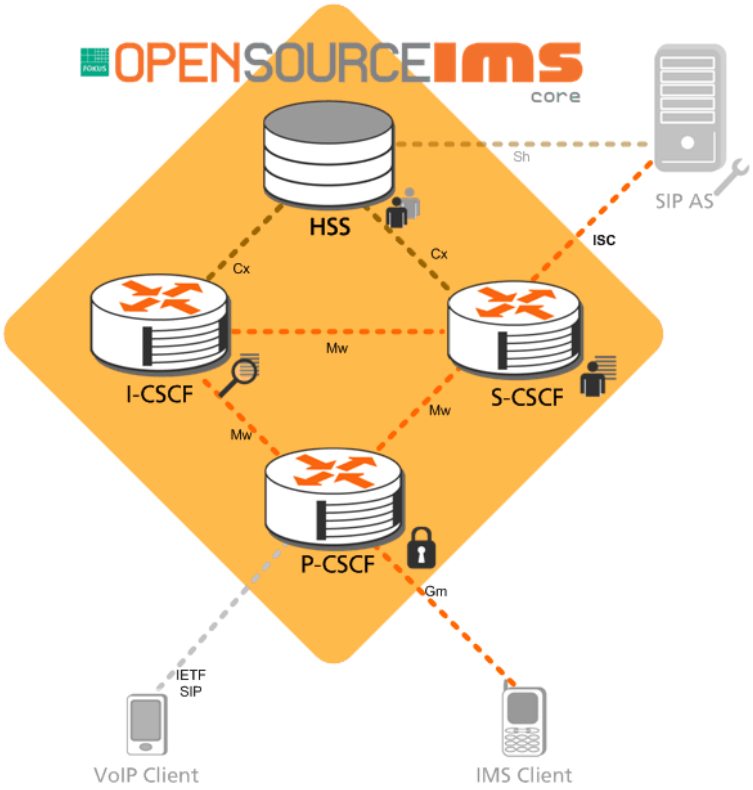


Figure IV-1: Architecture d'OpenIMScore **[19]**.

IV-2-1) Logiciels utilisés

Pour tester les fonctionnalités d'OpenIMSCore, nous avons fait usage des logiciels suivants:

IV-2-1-1) Logiciel UCT IMS Client

C'est un des terminaux les plus utilisés dans l'environnement OpenIMS car il permet une forte émulation des caractéristiques principales d'un terminal IMS.

Le client UCT IMS, dont seule une version Linux existe, est conçu pour être utilisé conjointement avec FOKUS Open IMS Core. Il a été développé par un groupe de recherche de l'Université du Cap, en Afrique du Sud.

IV-2-1-2) Logiciel Monster

FOKUS MONSTER, est conçu pour simuler un téléphone cellulaire de la 4éme génération avec une configuration spéciale permettant de configurer le nom de domaine et le numéro de port du serveur P-CSCF, ainsi que d'autres paramètres.

IV-2-1-3) Logiciel Wireshark

Wireshark est l'analyseur de protocole réseau le plus utilisé dans le monde. Il permet de visualiser ce qui se passe sur le réseau, c'est-à-dire, qu'il permet de capturer les paquets de trafic circulant dans le réseau.

IV-3) Mise en œuvre d'OpenIMScore

Sa mise en œuvre nécessite des ressources matérielles et quelques logiciels nécessaires au fonctionnement de la plateforme.

IV-3-1) Mise en place Machine virtuelle

L'installation d'un cœur réseau IMS OpenIMSCore, nécessite au préalable, la préparation d'une machine virtuelle nommée Ubuntu qui est dans notre cas la version Ubuntu 12.04.

Sa configuration requiert les ressources suivantes:

- Processeur Dual Core.
- 2 Go de RAM.
- 15 Go d'espace libre sur le disque dur (ou sur le disque SSD).
- Pour notre cas, nous avons choisi d'utiliser Oracle VM VirtualBox et de l'installer (Ubuntu 12.04).

IV-3-2) Installation d'un cœur réseau IMS

1. Les pré-requis

Avant de commencer, nous avons eu besoin de certains packages à installer, pour cela, les commandes suivantes ont été utilisées:

```
sudo apt-get install libcurl4-gnutls-dev
sudo apt-get install bison
sudo apt-get install curl
sudo apt-get install debhelper cdbs lintian build-essential fakeroot devscripts pbuilder
dh-make debootstrap dpatch flex libxml2- dev libmysqlclient15-dev ant docbook-to-man
```

```
sudo apt-get install ipsec-tools
sudo apt-get install subversion
 sudo apt-get install mysql-server-5.5
sudo apt-get install mysql-server libmysqlclient15-dev libxml2 libxml2-dev bind9 ant flex bison
sudo apt-get install subversion curl libcurl3 libcurl3-dbg libcurl3-gnutls libcurl4-openssl-dev
```

Installation du JDK version 7:

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

Une fois, tous ces outils installés et lancés, nous passons à l'étape suivante:

2.Téléchargement et installation d'OPEN SOURCE IMS CORE

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

Correction du bug: Un problème est survenu sur Ubuntu 12.04 suite à un bug dans le fichier client.h, corrigé par la commande suivante:

```
sudo sed -i '/include <curl\/types.h>/d' ser_ims/lib/lost/client.h
```

Installation d'OPENIMS CORE:

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

Compilation du composant FHoSS:

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

3.Configuration DNS et MySQL

configuration MySQL:

Copie des fichiers de la base donnée au serveur mysql:

```
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
```

configuration DNS:

La plateforme est configurée pour fonctionner en localhost (127.0.0.1) avec un nom de domaine par défaut "open-ims.test".

```
sudo apt-get install bind9
sudo cp ser_ims/cfg/open-ims.dnszone /etc/bind/
sudo sed -i '3azone "open-ims.test" {\n\ttype master;\n\tfile "\/etc\/bind\/open-ims.dnszone";\n};' /etc/bind/named.conf.local
sudo sed -i '2a127.0.0.1\topen-ims.test mobicents.open-ims.test ue.open-ims.test presence.open-ims.test icscf.open-ims.test scscf.open-ims.test pcscf.open-ims.test hss.open-ims.test' /etc/hosts
```

Redémarrage du serveur DNS:

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

4.Copie des fichiers de configuration de Open IMS Core

Copier les fichiers de configuration .cfg et .xml, ainsi que les scripts de lancement .sh des serveurs CSCF dans le répertoire de votre 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/
```

[20].

5.Lancement de Open IMS Core

Lancement de I-CSCF, P-CSCF, S-CSCF et HSS

Démarrage du service OpenIMS sur 4 consoles, chaque commande sur une console comme indiqué sur la figure suivante:

cd opt/OpenIMSCore

sudo ./pcscf.sh

sudo ./scscf.sh

sudo ./icscf.sh

cd FHoSS/deploy

sudo sh startup.sh

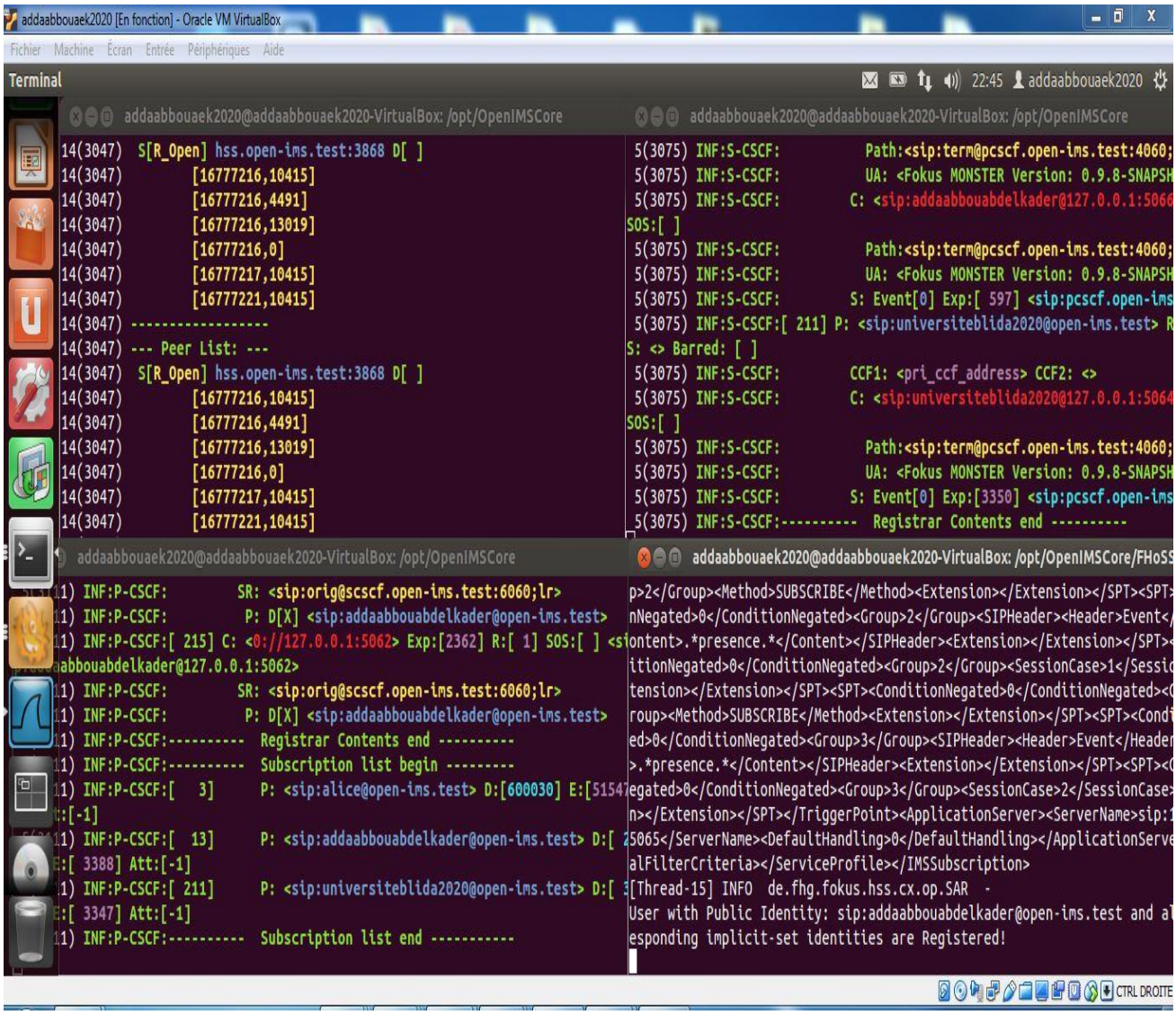


Figure IV-2: Lancement de I-CSCF, P-CSCF, S-CSCF et HSS.

Configuration de l'abonné

Par défaut, FHoSS contient deux utilisateurs alice et bob déjà enregistrés comme suit :

• alice@open-ims.test

• bob@open-ims.test

Pour accéder au FHoSS, on utilise l'URL suivante: http://hss.open-ims.test:8080 accessible par l'introduction du nom d'utilisateur Login: hssAdmin et du mot de passe: hss.

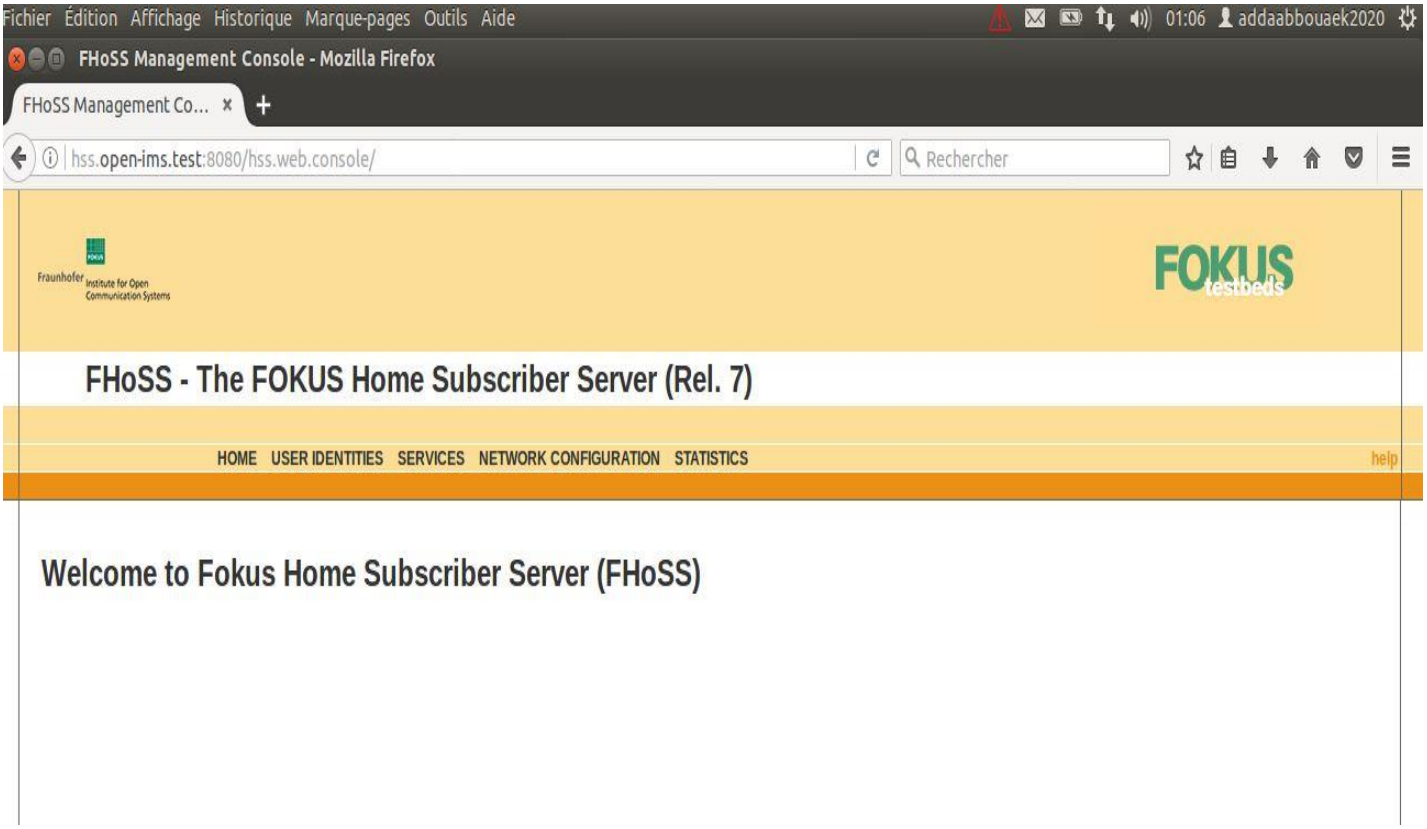


Figure IV-3: Interface OpenIMScore.

IV-4) Simulation et résultats

Après avoir installé et lancé OpenIMScore, nous entamons les tests de la simulation en trois scénarios selon que les clients soient préconfigurés par défaut ou à configurer:

IV-4-1) Premier scénario : (cas de deux clients déjà préconfigurés)

Il consiste à faire une simulation d'un appel vocal suivi d'un message texte entre alice et bob.

Il est à signaler que les utilisateurs alice et bob sont déjà **configurés par défaut** sur OpenIMScore et le logiciel UCT IMS Client, il reste seulement à les enregistrer dans le réseau en utilisant le logiciel UCT IMS Client.

IV-4-1-1) Enregistrement des utilisateurs dans le réseau

Pour cela, nous avons utilisé le client UCT IMS pour enregistrer et connecter les utilisateurs par défaut d'Alice et de Bob.

pour l'utilisateur Alice:

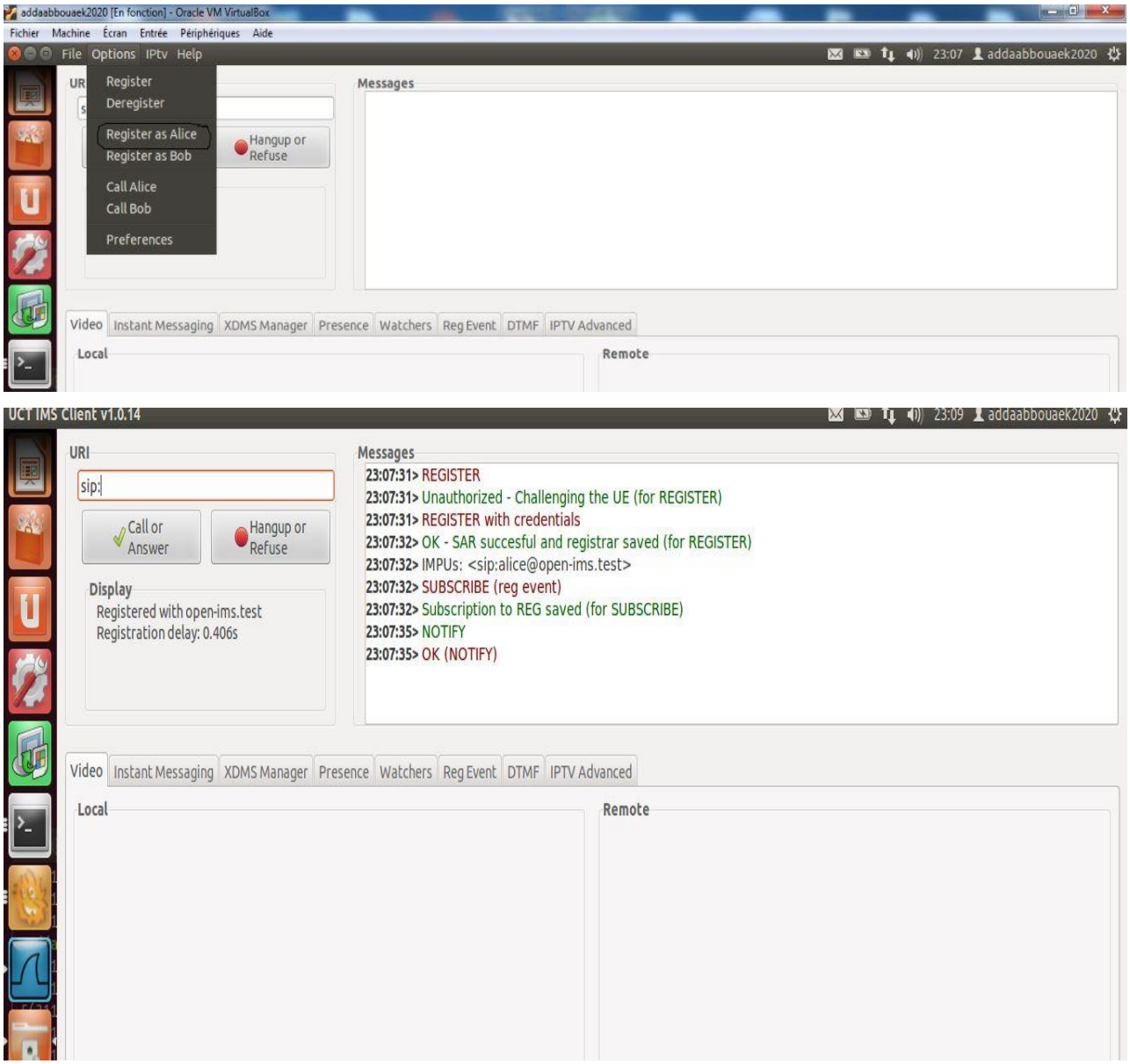


Figure IV-4: Enregistrement l'utilisateur Alice dans le réseau.

pour l'utilisateur Bob:

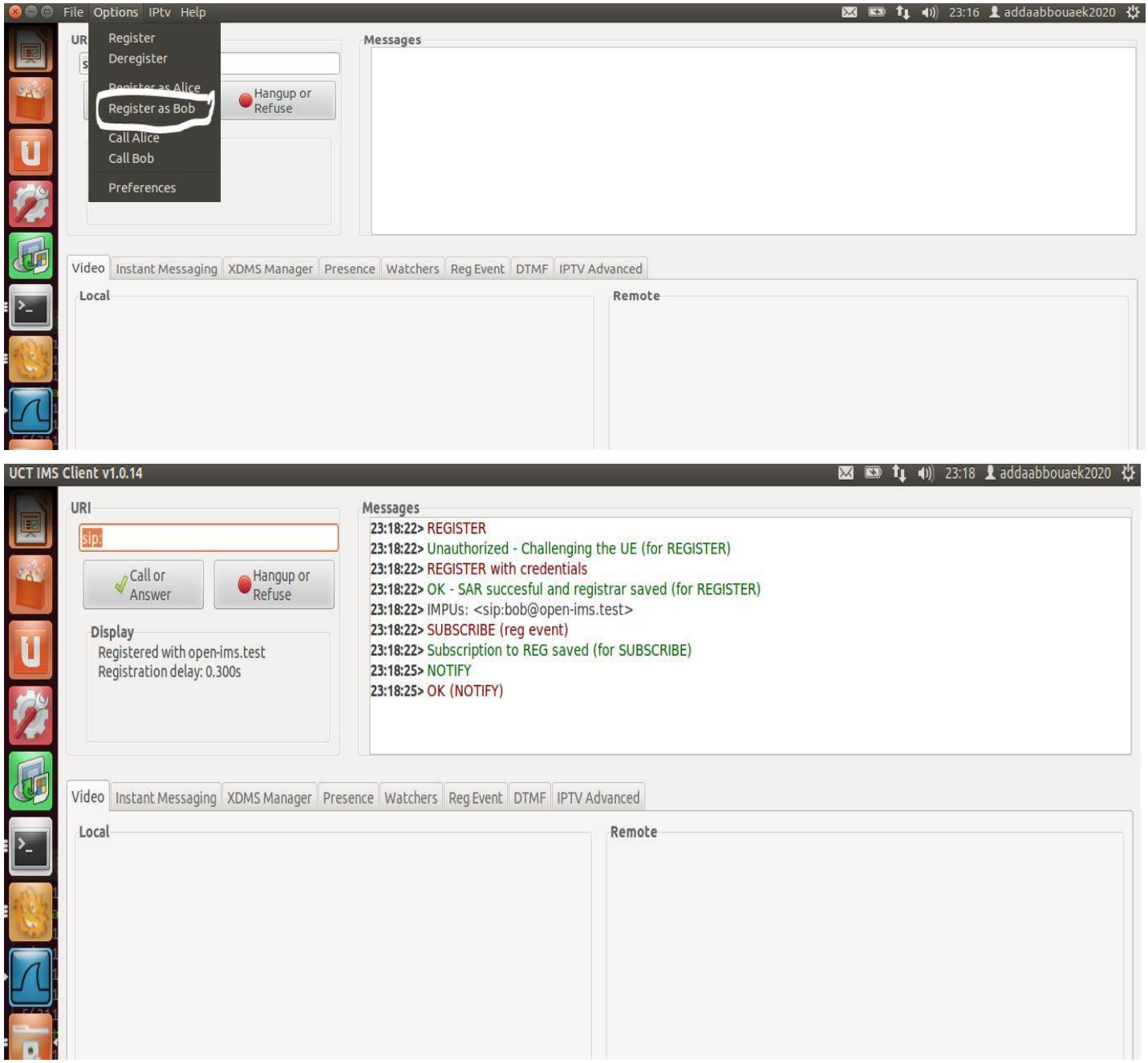


Figure IV-5: Enregistrement l'utilisateur Bob dans le réseau.

Ces figures montrent les échanges des messages SIP entre P-CSCF et UE.

L'UE (équipement utilisateur) envoie une première demande d'enregistrement au proxy PCSCF en utilisant un message "REGISTER". Le P-CSCF doit d'abord vérifier l'identité de l'utilisateur final sur la base de son profil stocké dans la base de données FHoSS à l'aide des autres entités S-CSCF et I-CSCF.

Après cette vérification, l'UE envoie un deuxième message d'enregistrement "REGISTER" qui sera reconnu par "200 OK" qui confirme que la demande d'enregistrement est réussie et que l'utilisateur peut établir une session voix, vidéo ou données.

IV-4-1-2) Test d'appel vocal

UCT IMS permet de connecter les deux utilisateurs au réseau IMS dans le même environnement OS et la même machine, et également de simuler le flux d'appels IMS et la messagerie comme nous pouvons le voir sur les figures suivantes.

Dans notre cas, l'établissement d'un appel entre alice et bob (alice appelle bob) se déroule comme suit:

Appel d'Alice:

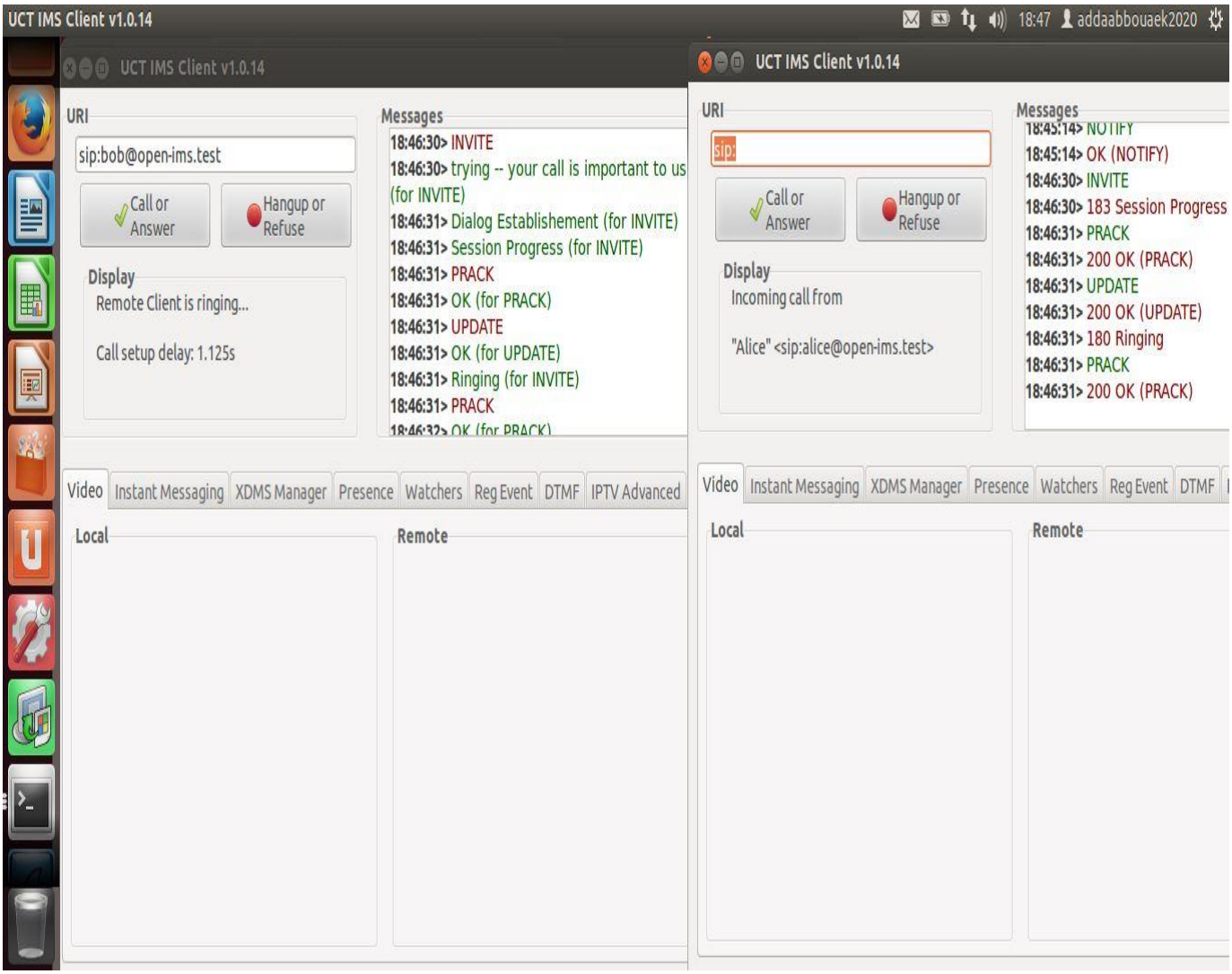


Figure IV-6: Alice appelle Bob.

Réponse de Bob:

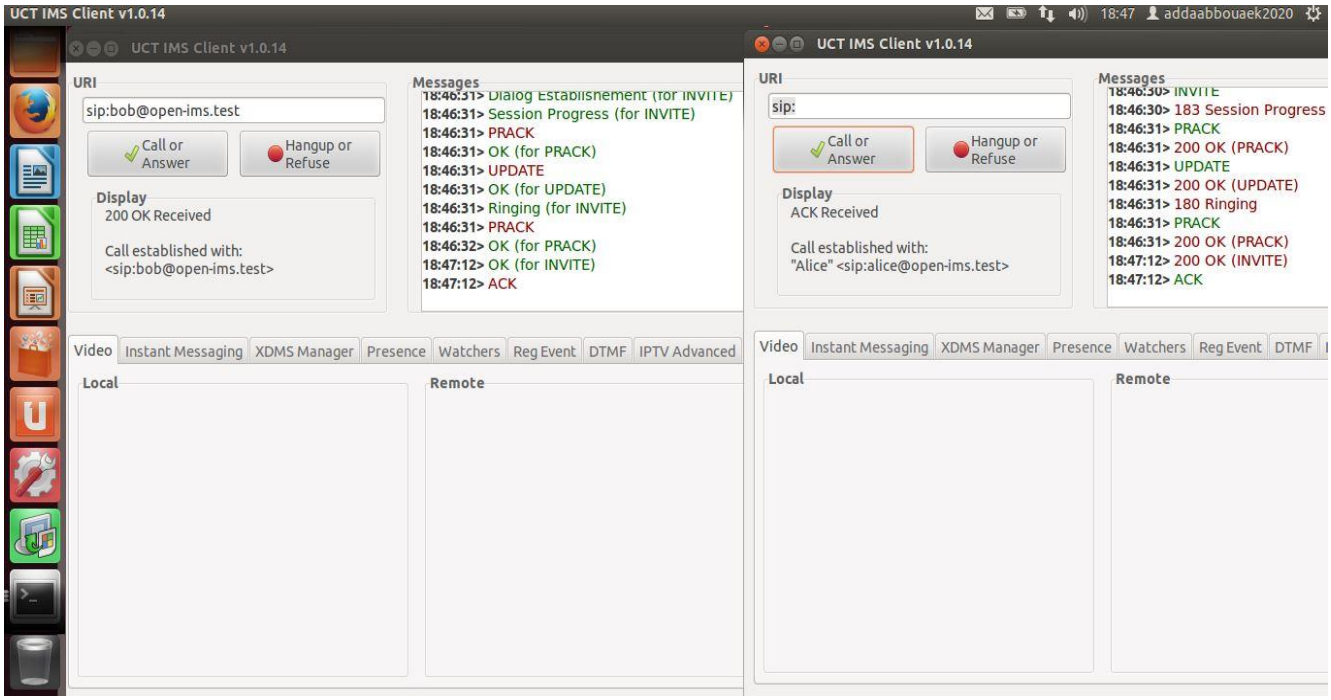


Figure IV-7: Bob répond à Alice.

Fin d'appel:

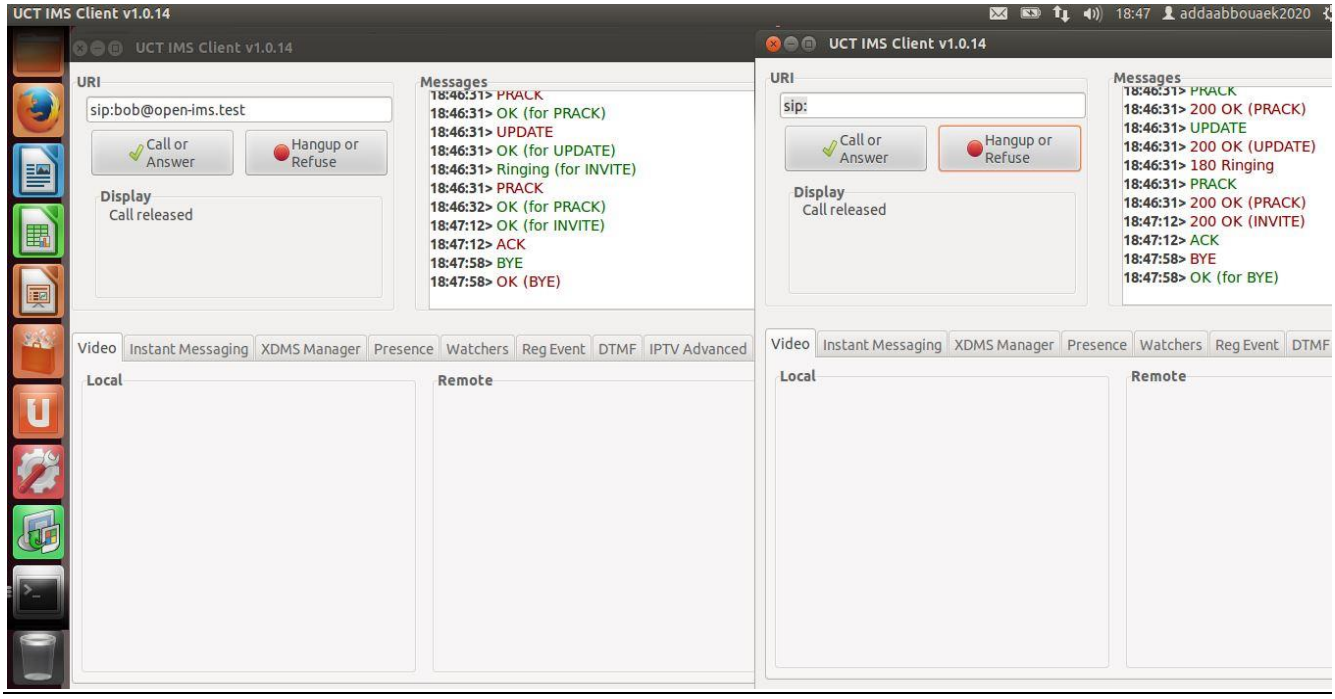


Figure IV-8: Flux d'appels d'un utilisateur à l'autre (fin appel).

Tout d'abord, une demande "INVITE" est envoyée par Alice pour initier un appel téléphonique avec Bob.

Ensuite, les deux participants négocient les paramètres de session (codecs, type de média, etc.) ainsi que la réservation des ressources par des messages "SIP / SDP".

Lorsque tous les paramètres de session sont négociés et configurés, les deux UE échangent un message «200 OK», puis échangent un message «ACK» indiquant que la session a été créée avec succès. À ce stade, la session est déjà établie entre les deux clients, le trafic audio ou vidéo est acheminé entre eux en utilisant RTP comme protocole de transport, à la fin de la session les deux clients échangent un message "BYE" confirmé avec une réponse "200 OK".

IV-4-1-3) Test de session data (message)

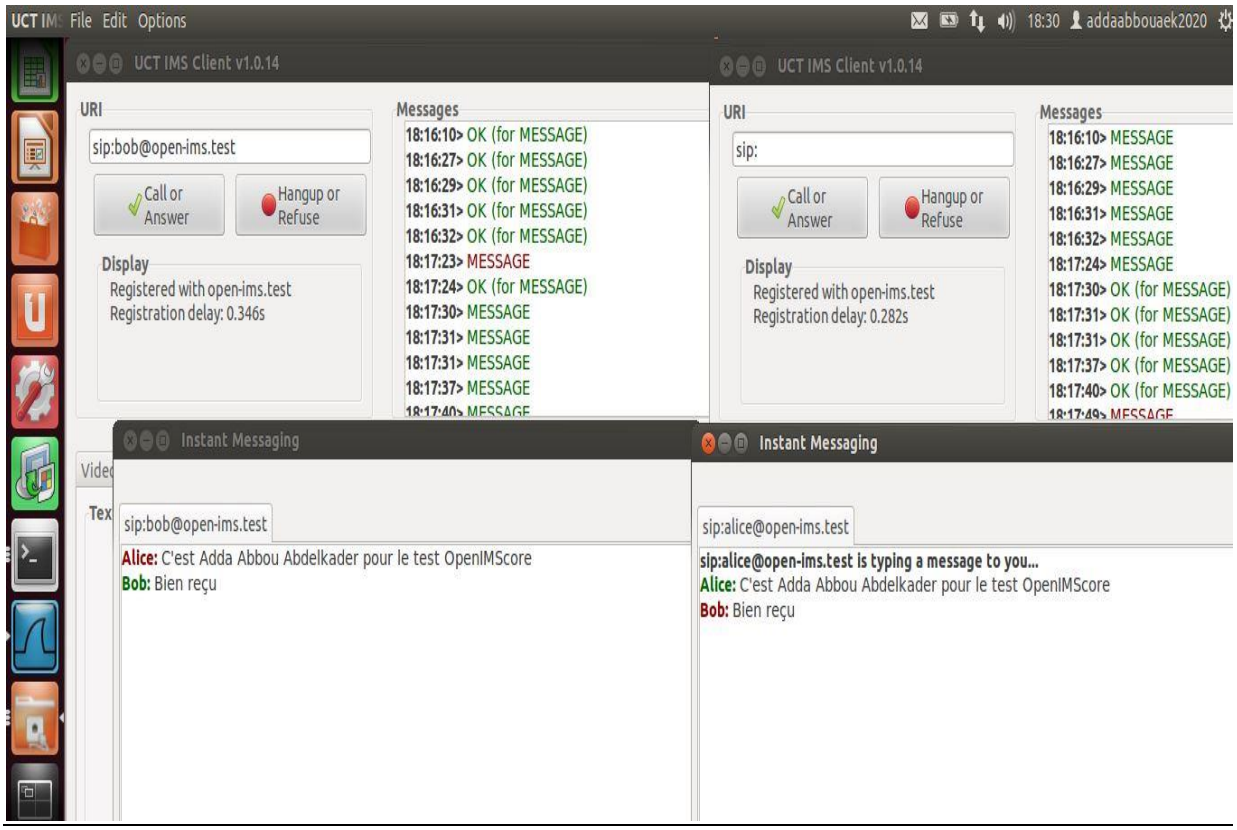


Figure IV-9: Établissement d'une session de données entre utilisateurs.

Pour établir une session de données entre les deux abonnés "Alice" envoie un message de requête "MESSAGE" contenant le message instantané à envoyer. Le message est reçu par "Bob", affiché une réponse "200 OK" est générée et envoyée à "Alice" pour indiquer que le message a été reçu.

IV-4-2) Deuxième scénario : (cas de deux clients à configurer)

Ce deuxième scénario décrit de façon détaillée toutes les phases de la simulation:

La première phase touche à la création et la configuration des deux nouveaux abonnés (addaabbouabdelkader et universitéblida2020) sur **OpenIMScore** et ce grâce à l'utilisation de logiciel Client **IMS Monster.** Il est à faire remarquer que dans notre cas, le logiciel **UCT IMS** Client ne peut être utilisé car il ne permet pas de créer nouveaux utilisateurs et contient par défaut les deux utilisateurs standard alice et bob.

Quand à la deuxième phase, elle traite de l'enregistrement des nouveaux utilisateurs sur le réseau.

La troisième phase a trait à une simulation d'un appel vocal dans sa partie contrôle puis établissement d'une session.

La quatrième phase est consacrée à la simulation d'un envoi de message texte.

IV-4-2-1) Configuration des deux utilisateurs

La configuration des nouveaux utilisateurs se fait en leurs fournissant des identifiants pour cela nous allons suivre les quatre étapes suivantes:

- **La première étape: création de l'IMPU**

Tout d'abord, pour la configuration du premier identifiant qui est l'identité publique **IMPU** pour les deux nouveaux utilisateurs (addaabbouabdelkader et universitéblida2020) afin de leur attribuer une adresse **SIP**, nous devons préalablement déterminer le nom du domaine du réseau visité et les noms d'utilisateur.

Comme montré sur les figures suivantes, le nom du domaine du réseau visité est donné par défaut et est **open-ims.test.**

Les adresses SIP des utilisateurs, dans notre exemple, deviennent alors respectivement:

- sip:addaabbouabdelkader@open-ims.test
- sip:universitéblida2020@open-ims.test

Les informations afférentes au profil de service et à la fonction de Charging sont configurées par défaut. La configuration de Charging-info set est nécessaire pour renseigner au moins l'adresse du "Primary CCF (Charging Collection Fuction)". Le CCF

implique toutes les entités du réseau SIP (P-CSCF, I-CSCF, S-CSCF, BGCF, MRFC, MGCFN, AS) alloué à un utilisateur.

La figure suivante montre la configuration d'une IMPU de l'utilisateur nommé **addaabbouabdelkader.**

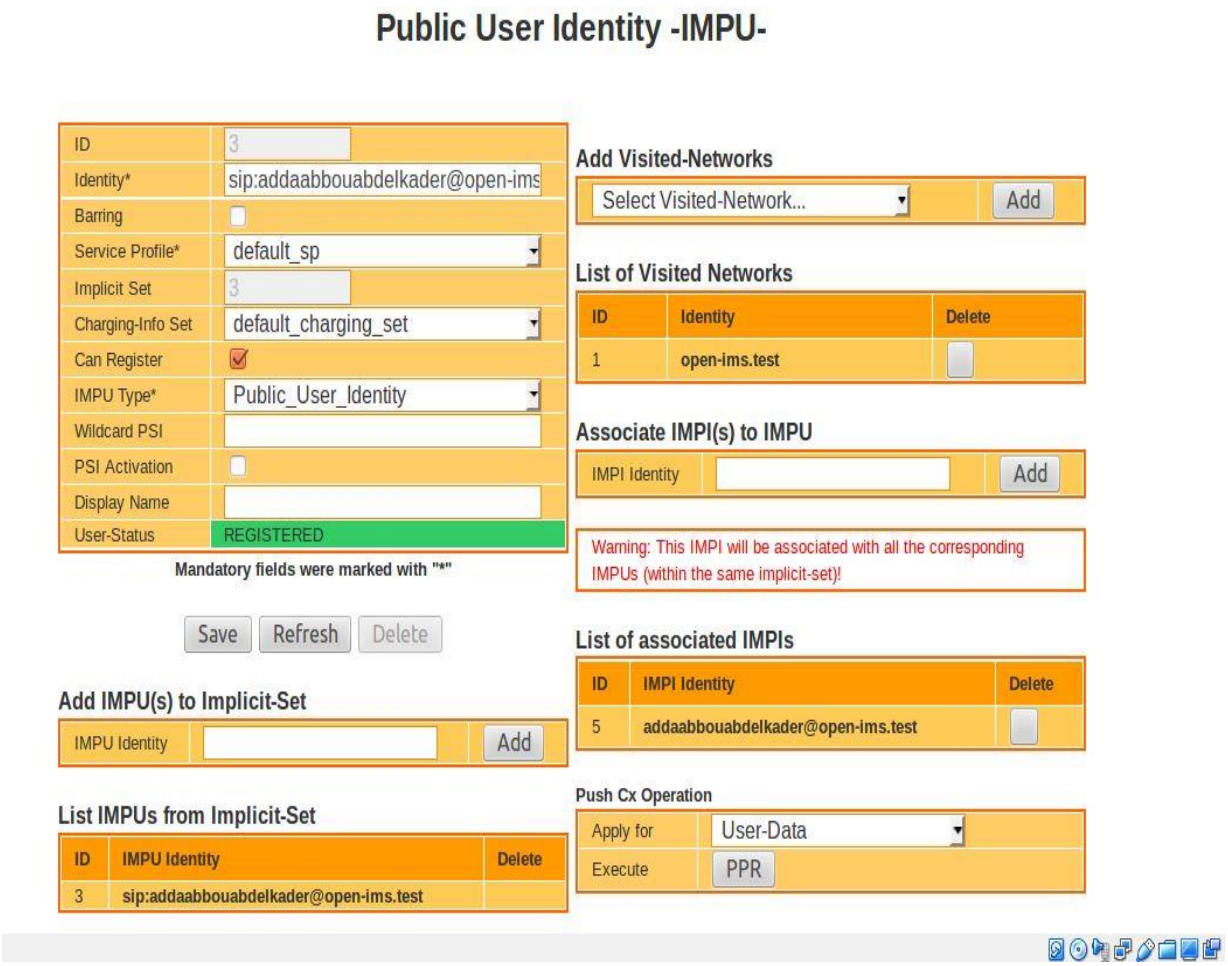


*Figure IV-10: Configuration de l'**IMPU** addaabbouabdelkader.*

La figure suivante montre la configuration d'une IMPU de l'utilisateur nommé **universitéblida2020.**

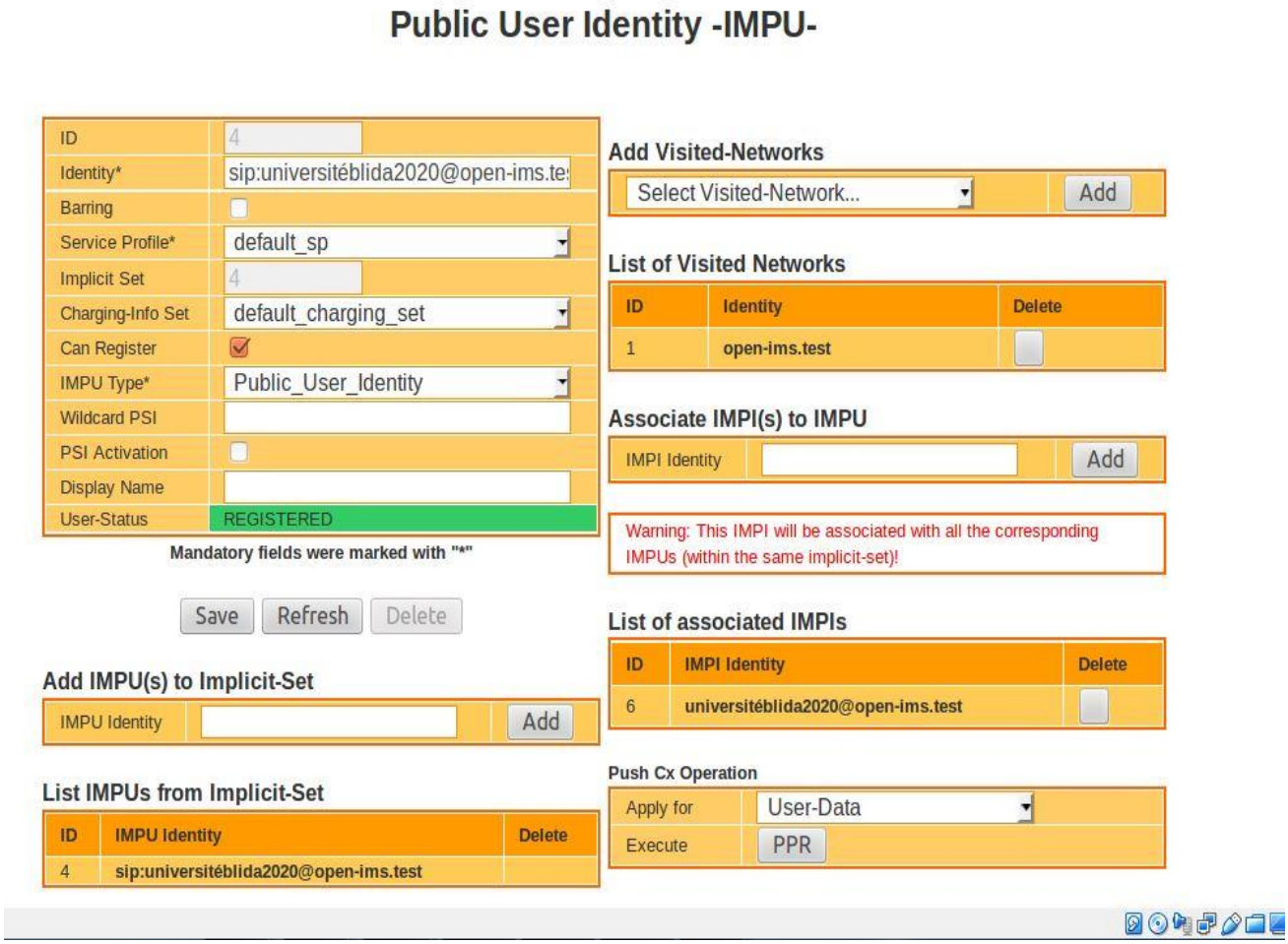


Figure IV-11: Configuration de l'IMPU universitéblida2020.

- **<u>La deuxième étape: création de l'IMPI</u>**

Il s'agit dans cette étape, d'attribuer aux utilisateurs une identité privée.

Au regard de la syntaxe à faire respecter pour l'IMPI qui est: utilisateur@domaine, les identités privées des deux utilisateurs sont dans notre cas:

- addaabbouabdelkader@open-ims.test
- universitéblida2020@open-ims.test

Pour assurer la sécurité de l'IMPI, l'utilisateur IMS doit avoir un **mot de passe** et une **méthode d'authentification** afin de bénéficier des services auxquels il est abonné. Il est à préciser que l'IMPI sert à identifier et authentifier un abonné et n'a aucun rôle de routage.

Les figures ci-dessous illustrent la configuration de l'IMPU pour les deux utilisateurs addaabbouabdelkader et universitéblida2020.

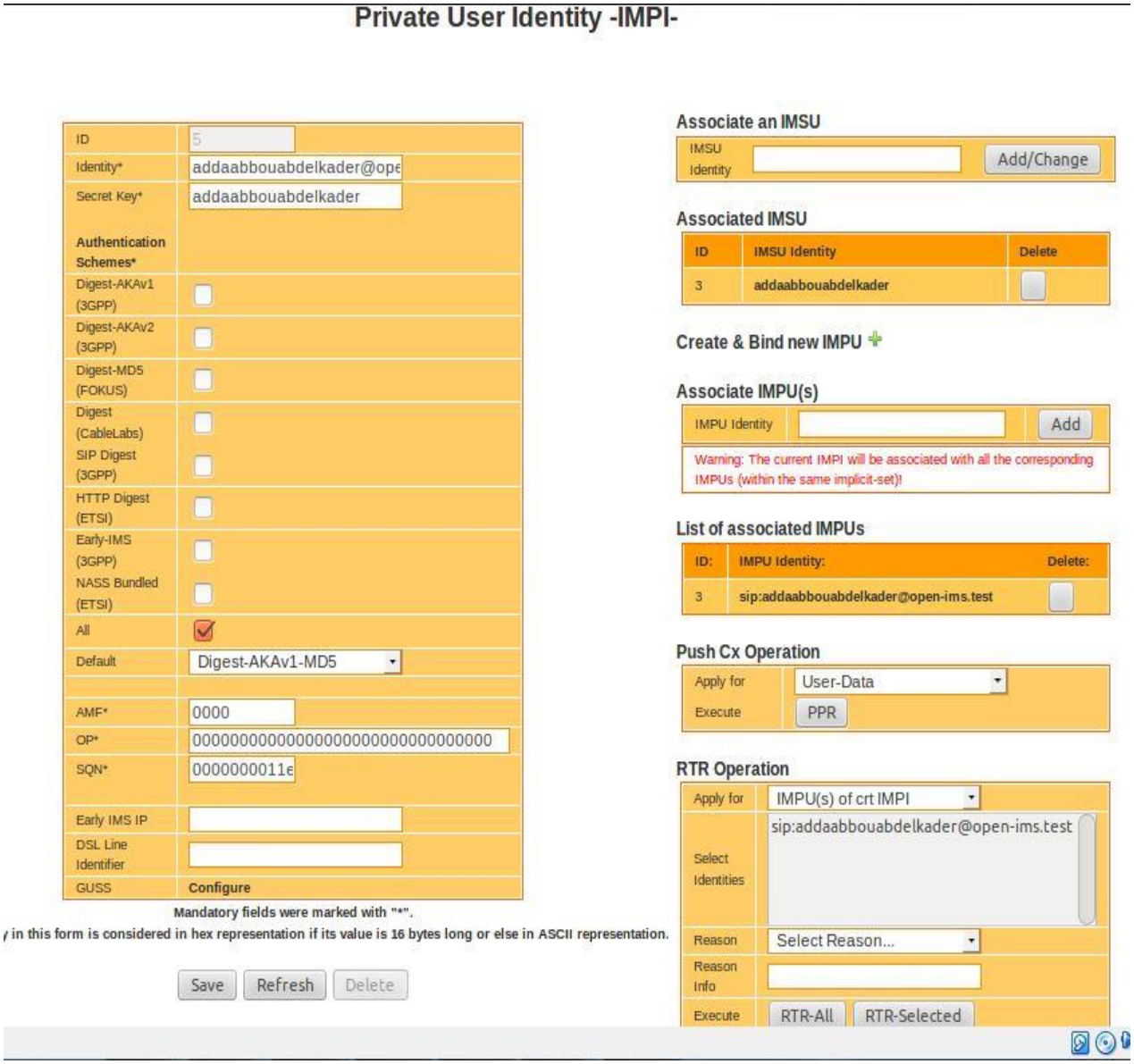


*Figure IV-12: Configuration de l'**IMPI** addaabbouabdelkader.*

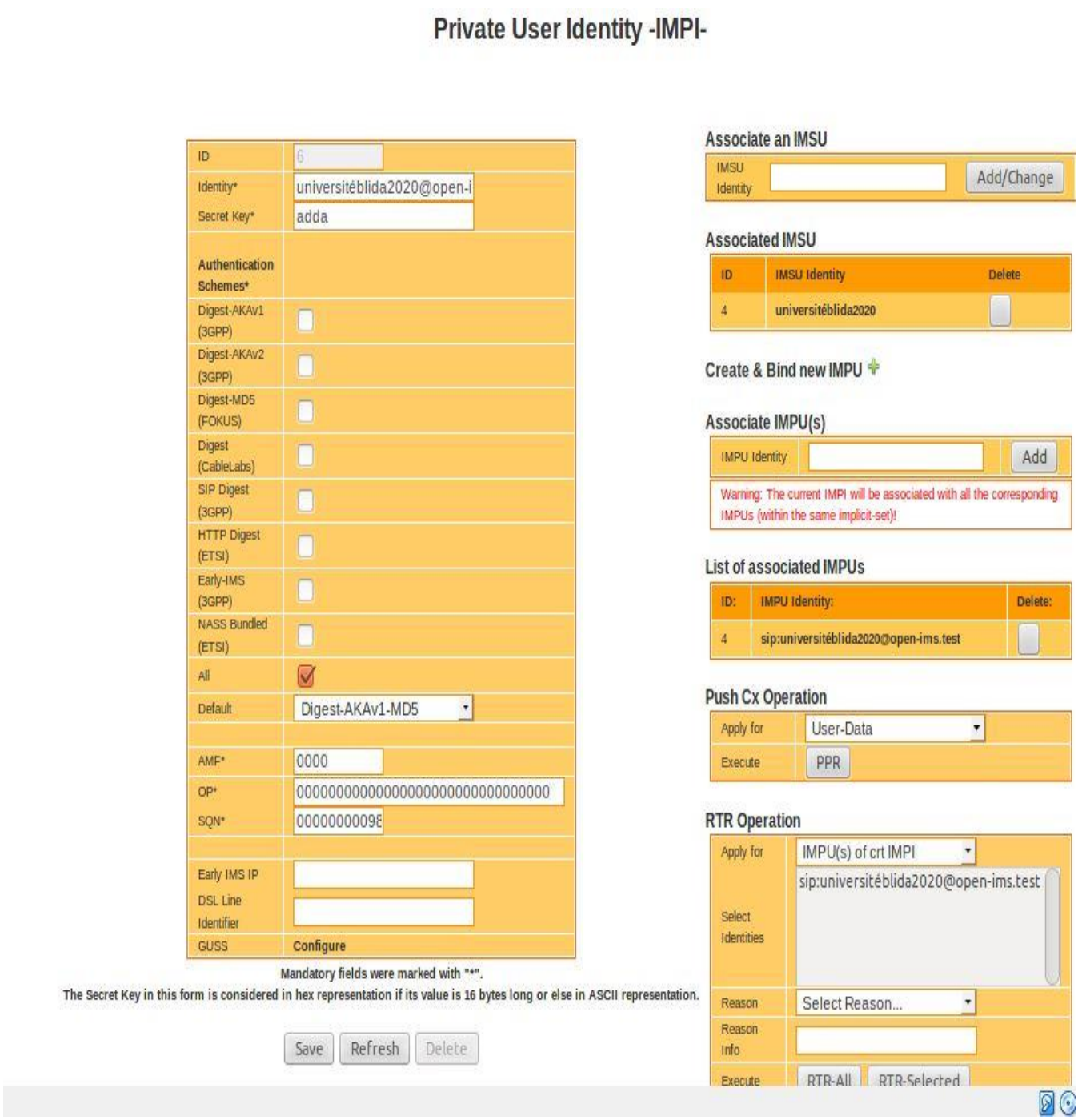


*Figure IV-13: Configuration de l'**IMPI** universitéblida2020.*

- **<u>La Troisième étape: création de l'IMSU</u>**

Cette étape constitue la dernière phase de la configuration d'un utilisateur.

Il est clair que les utilisateurs, même enregistrés dans la base de données HSS, ne peuvent bénéficier d'aucun service, en l'absence de leur abonnement.

C'est pourquoi il est essentiel à présent de créer une souscription utilisateur, ou IMSU (pour IMSU Souscription).

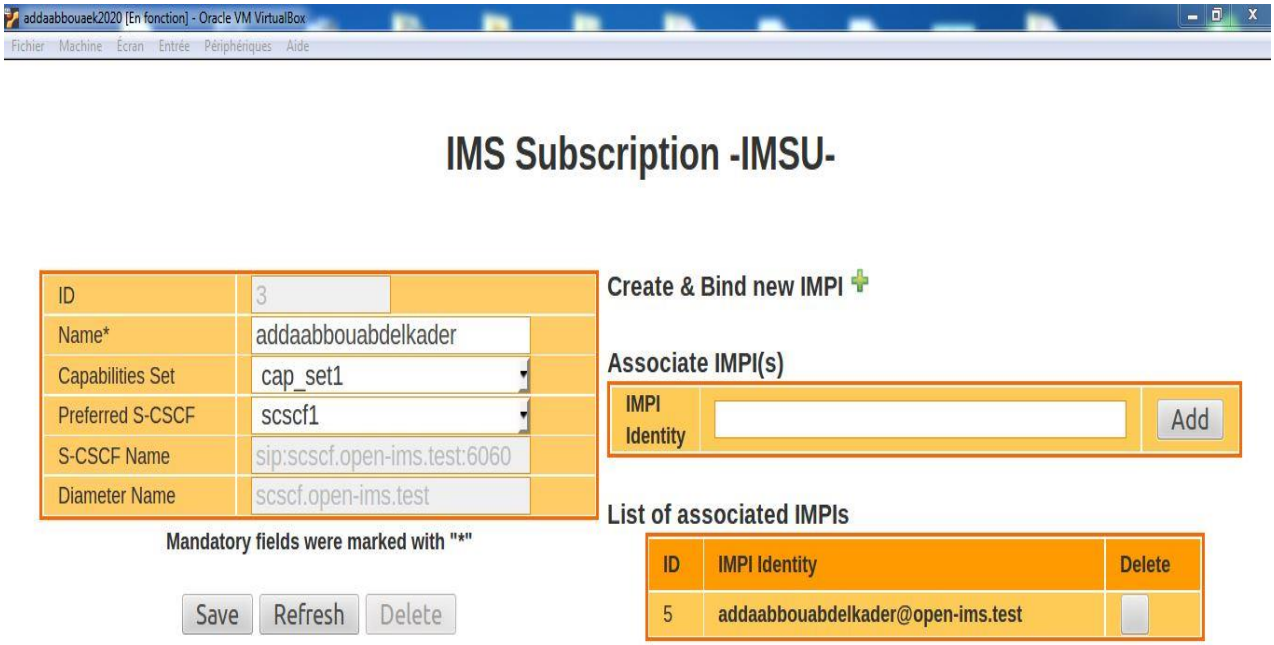


Figure IV-14: Configuration d'IMS Suscription pour addaabbouabdelkader.

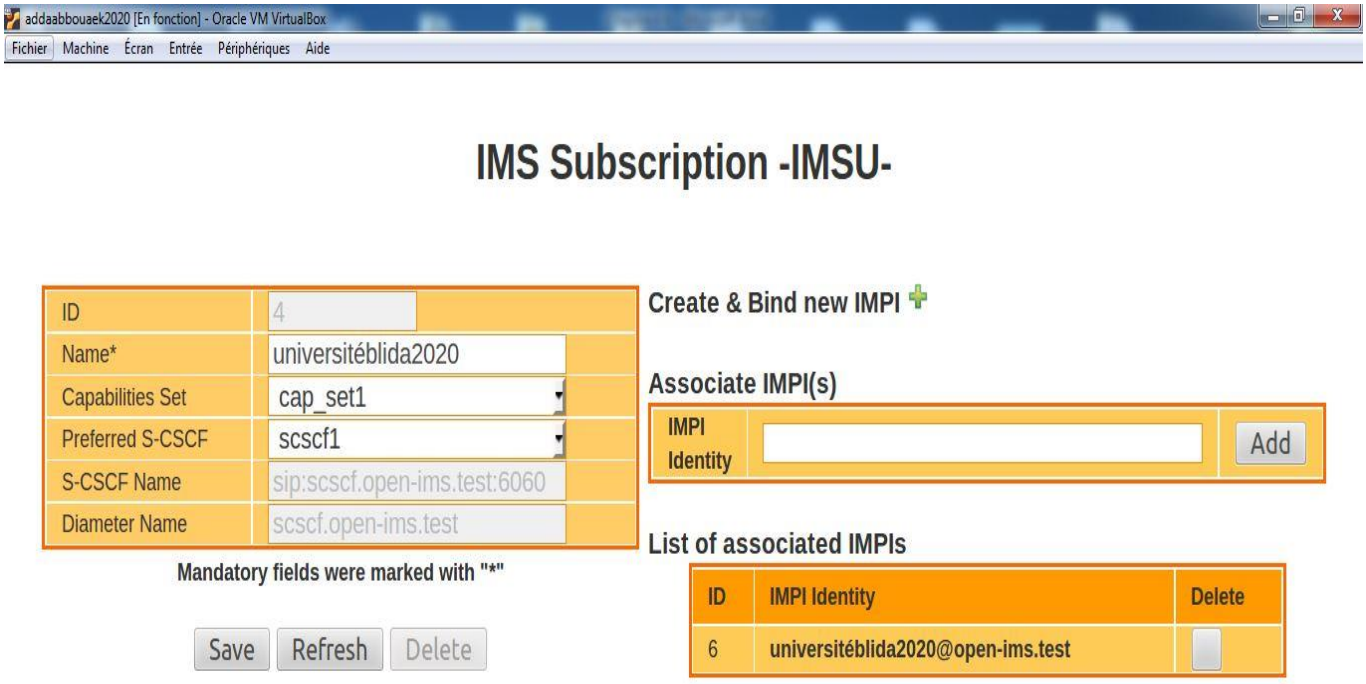


Figure IV-15: Configuration d'IMS Suscription pour universitéblida2020.

- **La Quatrième étape: configuration IMS Monster**

Elle consiste en la configuration de client IMS Monster pour qu'il puisse fonctionner avec des profils déjà déclaré dans HSS (FHoSS).

Le client IMS Monster sous Linux est considéré comme étant un des clients SIP gratuits et compatibles avec la plateforme IMS.

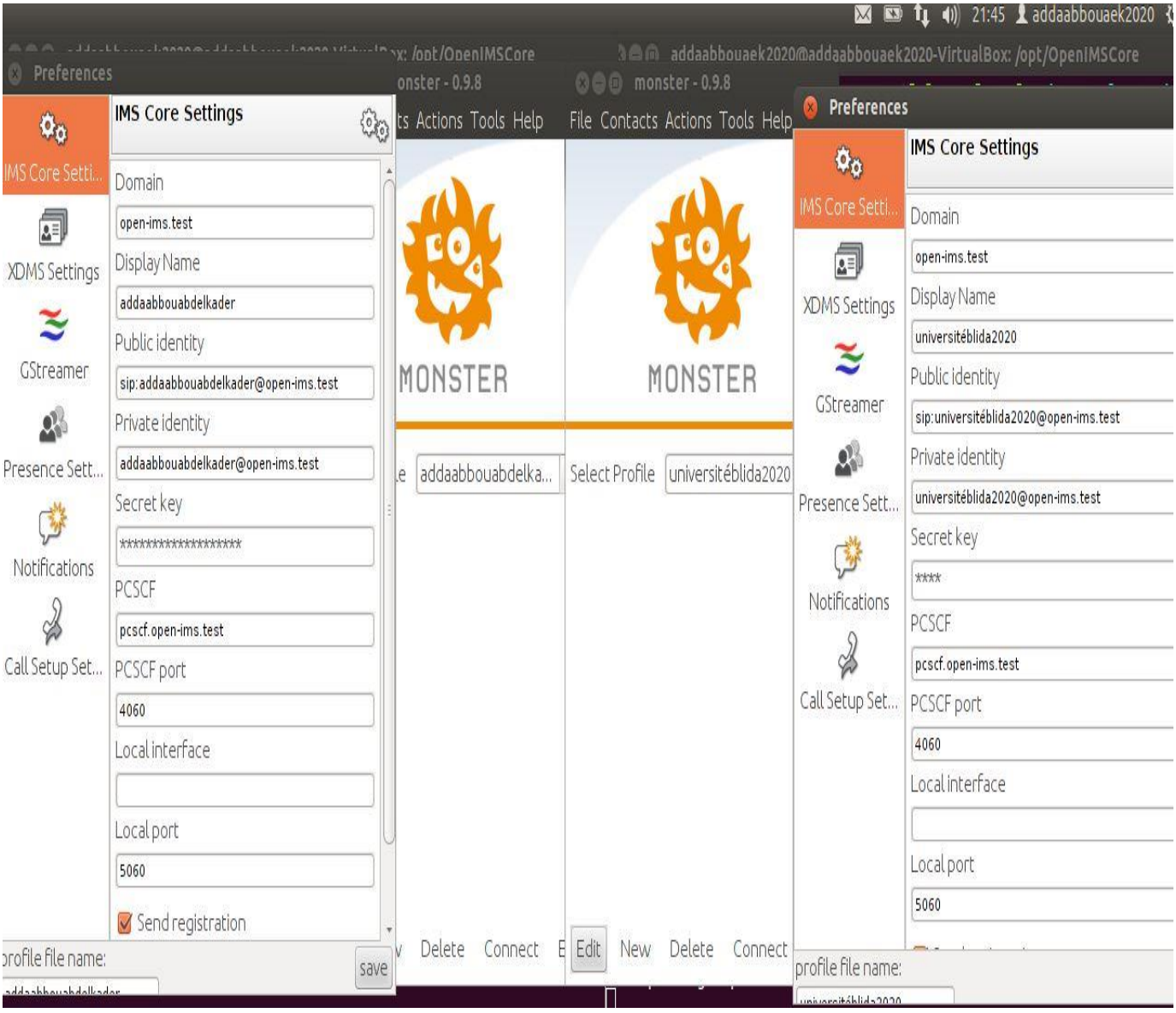


Figure IV-16: Configuration IMS Monster.

IV-4-2-2) Demande d'enregistrement

Après avoir configuré les deux utilisateurs sur OpenIMScore et sur Client IMS Monster, ils peuvent désormais être enregistrés sur le réseau.

À l'aide de l'utilisation de logiciel Wireshark, nous pouvons capturer les paquets échangées lors d'une demande d'enregistrement des utilisateurs.

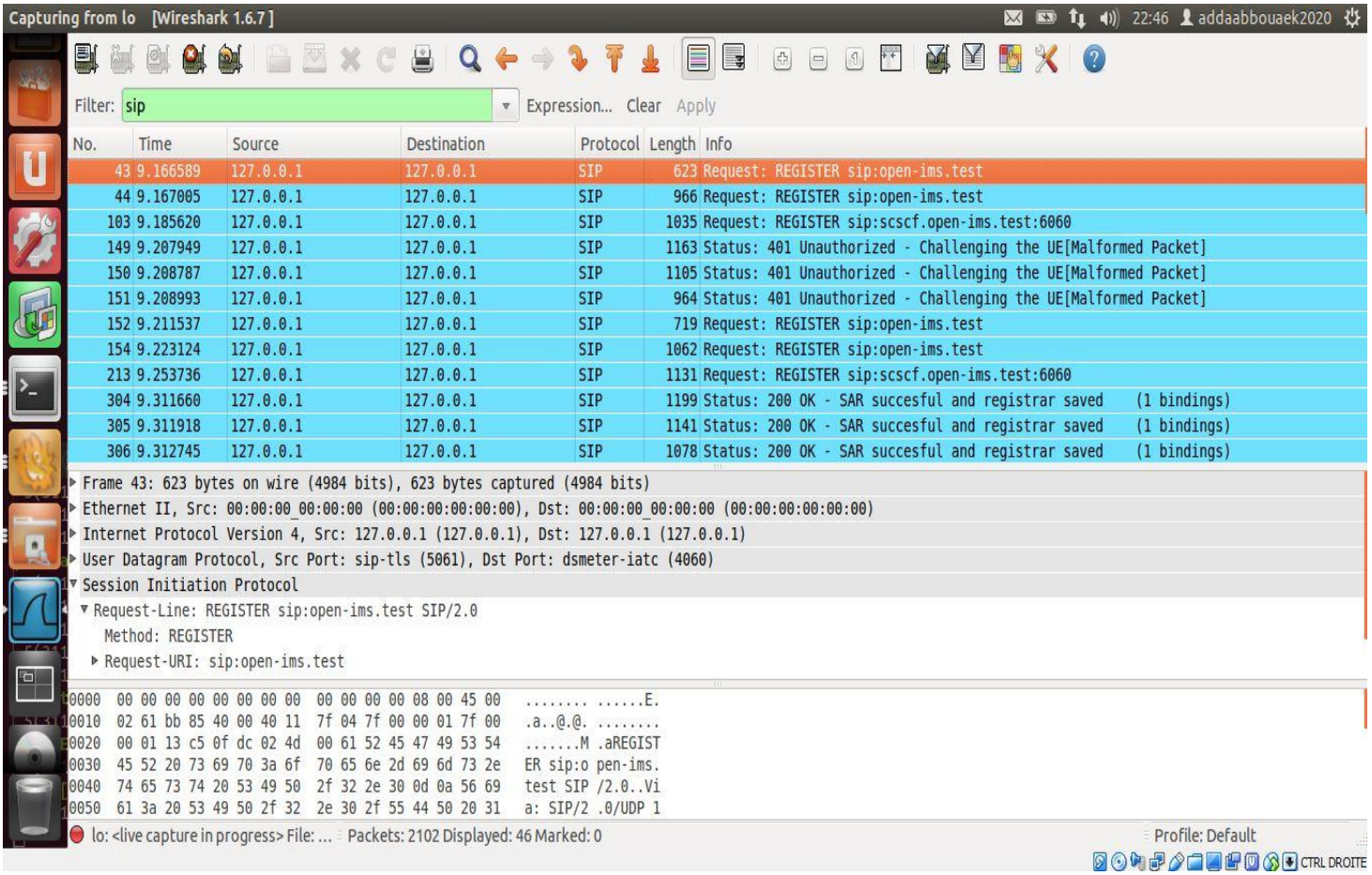


Figure IV-17: Capture des paquets lors d'une demande d'enregistrement.

L'enregistrement dans le réseau est la première action effectuée par un terminal dès son mise en route pour qu'il effectue des appels et soit joignable par ses correspondants. La méthode associée à cette fonctionnalité est REGISTRER du protocole SIP.

Le client envoie une première demande d'enregistrement au proxy PCSCF à l'aide d'un message "REGISTER". Le P-CSCF doit d'abord vérifier l'identité de l'utilisateur final à travers son profil stocké dans la base de données FHoSS à l'aide des autres entités S-CSCF et I-CSCF. L'utilisateur reçoit un message réponse "401 Unauthorized" qui contient les paramètres d'authentification.

Après cette vérification, l'utilisateur envoie un second message d'enregistrement "REGISTER" qui sera acquitté par "200 OK" qui indique que la demande d'enregistrement est réussie et que l'utilisateur peut établir une session multimédia.

Exemple de la méthode "REGISTER":

Figure IV-18: Exemple de la méthode "REGISTER".

IV-4-2-3) Test d'appel vocal

Le test d'appel SIP considéré comme le plus répandu, permet de vérifier le bon fonctionnement de la plateforme IMS.

Les deux figures suivantes concluent à l'aboutissement de l'appel vocal lancé par addaabbouabdelkader et accepté par universitéblida2020: La première figure montre que l'utilisateur "universitéblida2020" a reçu l'appel de l'utilisateur addaabbouabdelkader, quand à la deuxième indique l'acceptation par l'universitéblida2020 de l'appel lancé par addaabbouabdelkader, la conversation peut alors commencer.

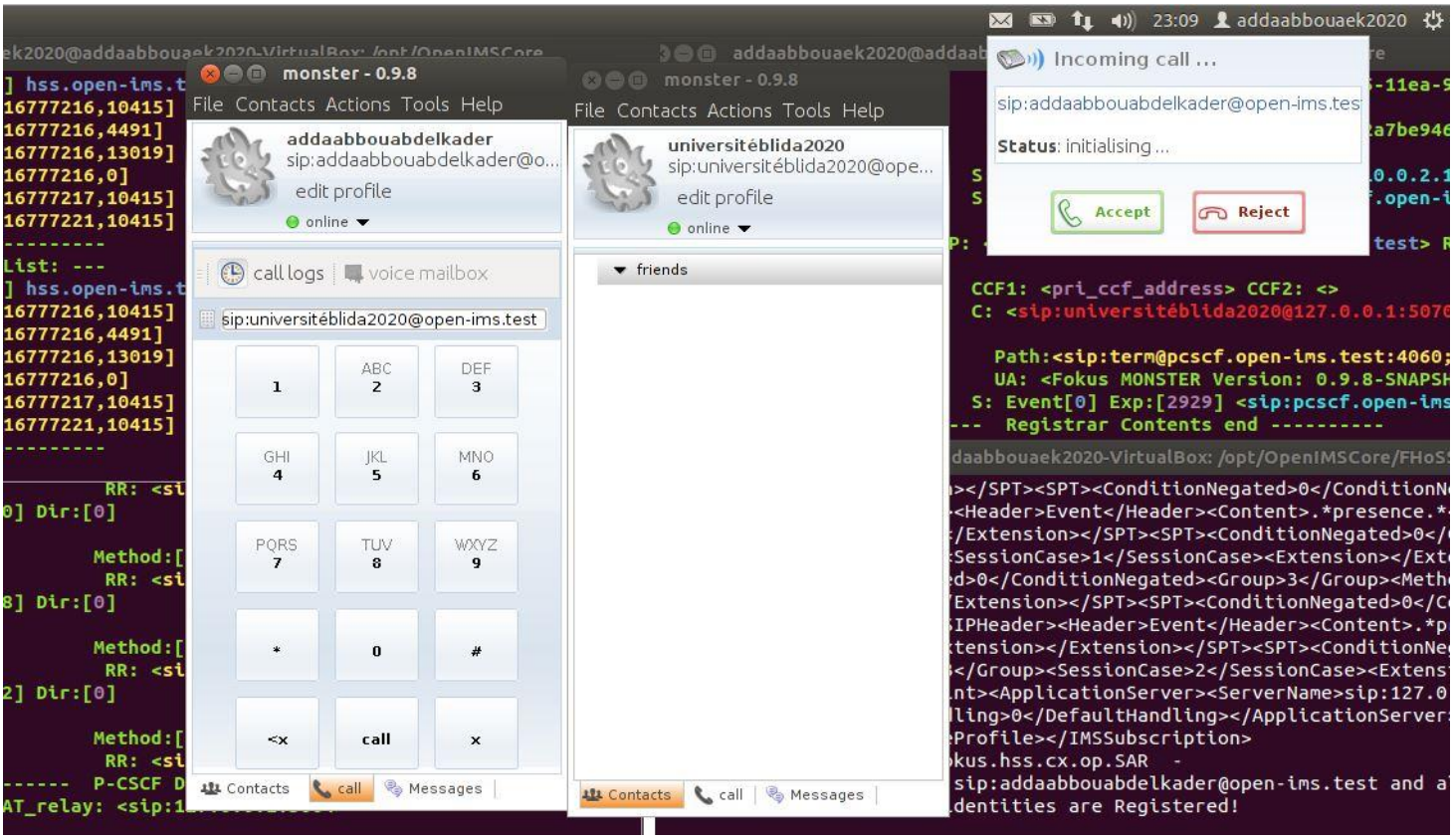


Figure IV-19: Lancement d'appel entre addaabbouabdelkader et universitéblida2020.

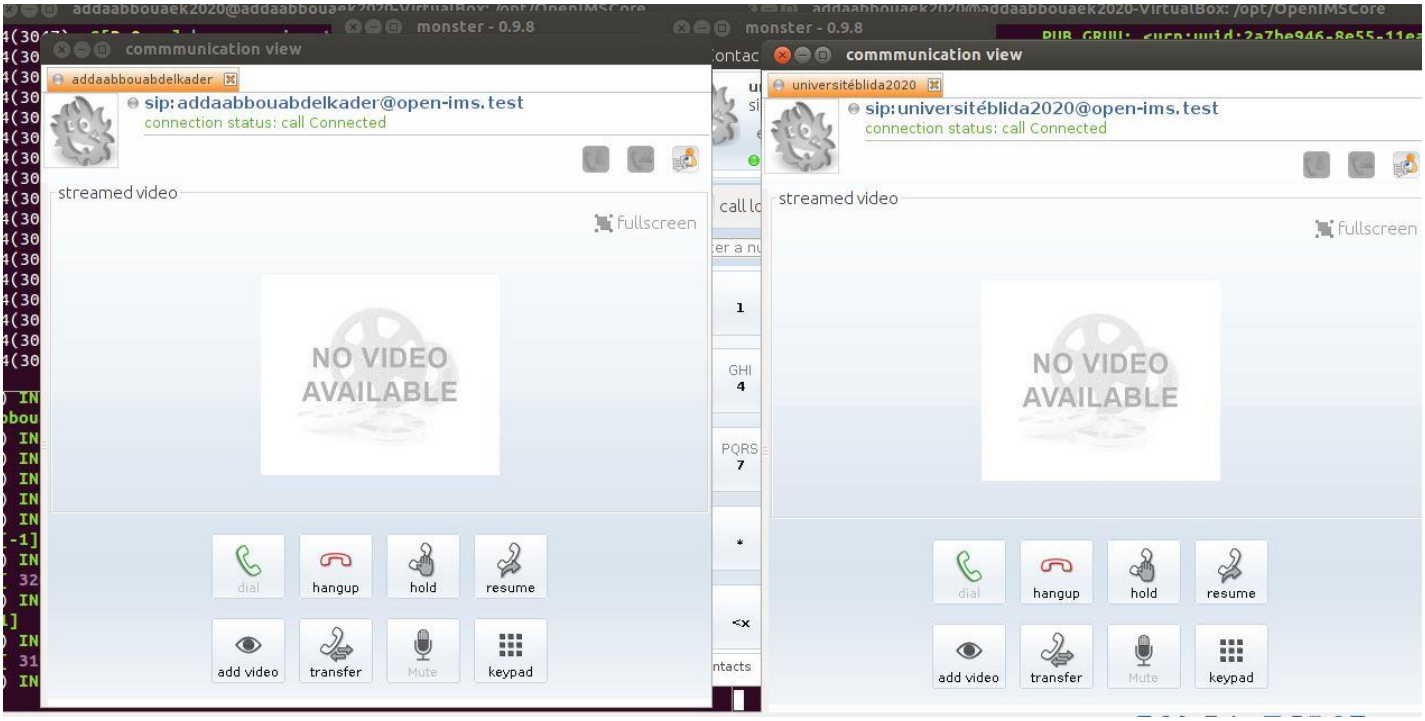


Figure IV-20: Conversation vocale entre addaabbouabdelkader et universitéblida2020.

On s'intéresse maintenant aux échanges de flux de signalisation SIP ayant présidé au contrôle du processus d'établissement de la communication.

La figure suivante extraite grâce au logiciel Wireshark, donne une description détaillée des différentes méthodes de signalisation du protocole SIP (INVITE, 100 trying, 180 Ringing, 200 OK et ACK) échangées sur le réseau et qui ont permis le contrôle de l'établissement de la communication avant son aboutissement avec succès.

Une fois que l'appelé (univeristéblida2020) accepte l'appel, le protocole RTP prend le relais par la prise en charge du transport du flux du trafic vocal.

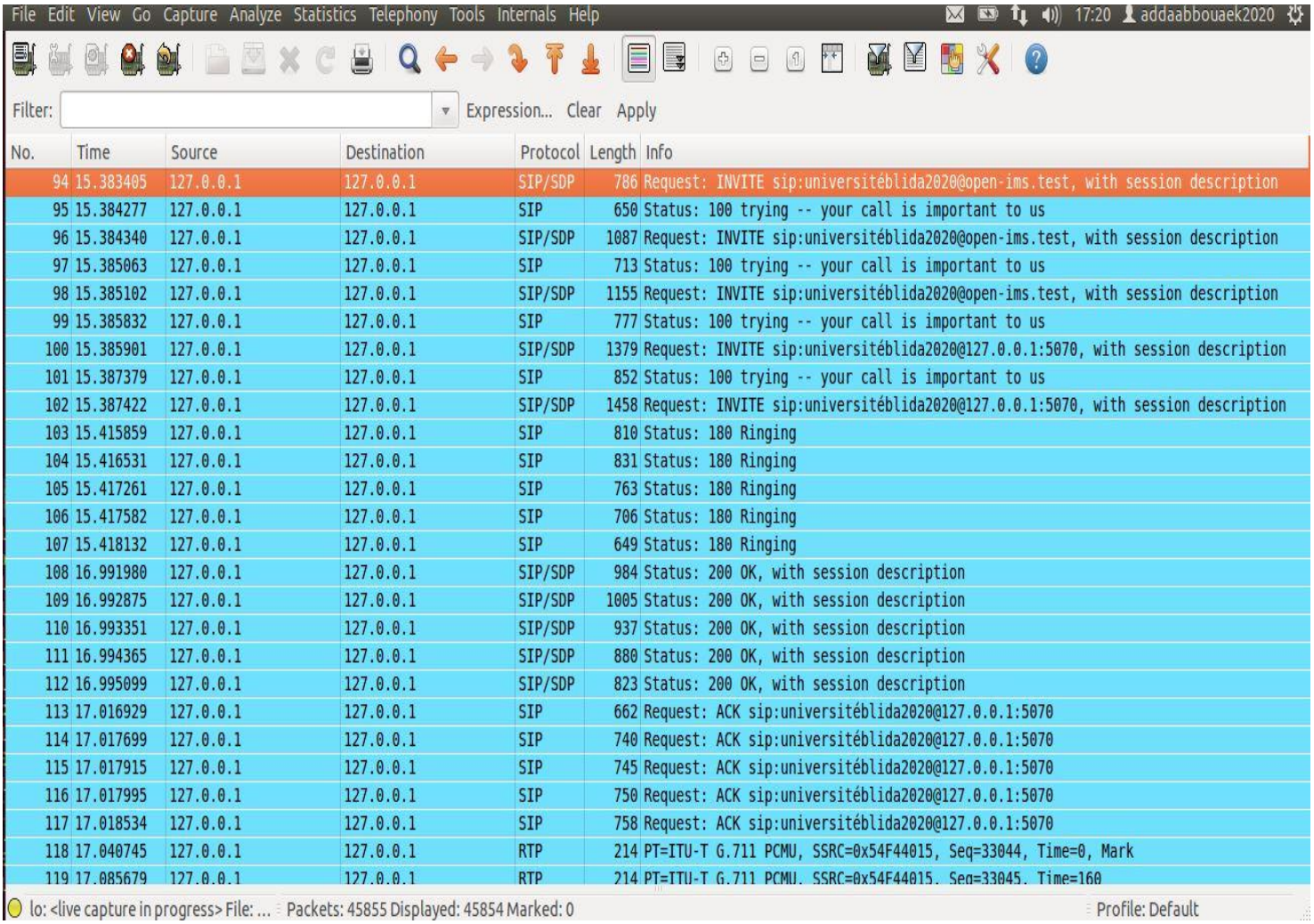


Figure IV-21: Capture des paquets échangées lors de la signalisation et de l'appel.

L'exploitation du résultat de la capture montre qu'à la suite d'une demande "INVITE" envoyée par addaabbouabdelkader pour initier un appel téléphonique avec

universitéblida2020, les deux participants négocient les paramètres de session (codecs, type de média, etc.) ainsi que la réservation des ressources par des messages "SIP/SDP".

Lorsque tous les paramètres de session sont négociés et configurés, les deux UE échangent un message «200 OK», puis un message «ACK» indiquant que la session a été créée avec succès.

À ce stade, la session est déjà établie entre les deux clients et le trafic est acheminé entre eux en utilisant pour le transport le protocole **RTP** comme montré sur la figure suivante.

On a aussi volontairement simulé une fin de session (raccrochage de l'appelé) dont le contrôle est assuré par le protocole SIP comme montré à la fin de la figure suivante: les deux clients échangent un message "BYE" confirmé par une réponse "200 OK".

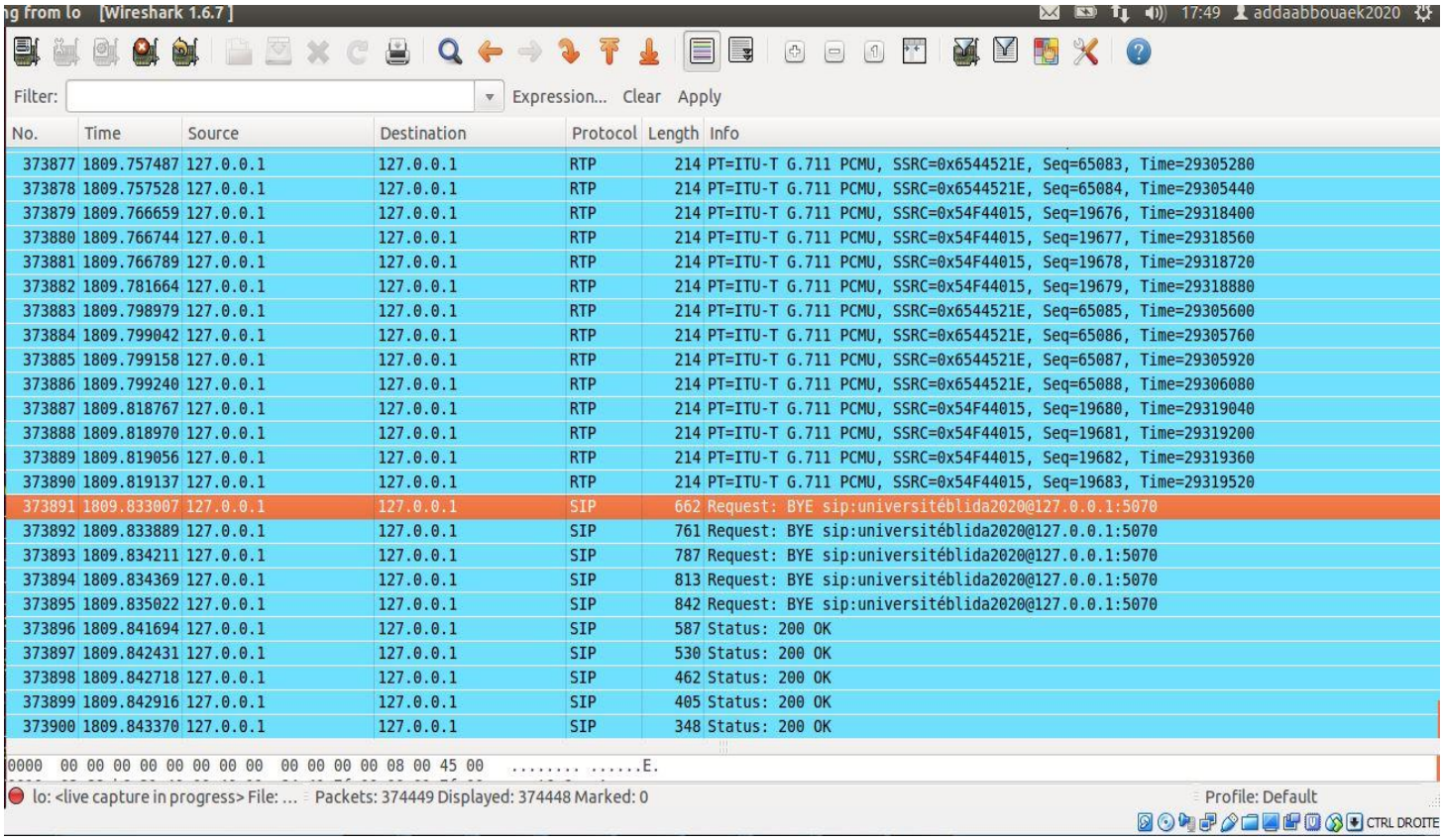


Figure IV-22: Capture des paquets (fin de session).

Exemple de la méthode " INVITE ":

```
▼ Session Initiation Protocol
  ▼ Request-Line: INVITE sip:universitéblida2020@open-ims.test SIP/2.0
      Method: INVITE
    ▶ Request-URI: sip:universitéblida2020@open-ims.test
      [Resent Packet: False]
  ▼ Message Header
      Call-ID: 20369efba6e671d9f15c8f7d2cb243cc@127.0.0.1
    ▶ CSeq: 8 INVITE
    ▶ From: <sip:addaabbouabdelkader@open-ims.test>;tag=1009
    ▶ To: <sip:universitéblida2020@open-ims.test>
    ▶ Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bK209dec6a4d3ce0ec3eb9c3d862aea801
      Max-Forwards: 20
      Route: <sip:orig@scscf.open-ims.test:6060;lr>
      Content-Type: application/sdp
    ▶ Contact: <sip:addaabbouabdelkader@127.0.0.1:5062>
      User-Agent: Fokus MONSTER Version: 0.9.8-SNAPSHOT
      Content-Length: 216
  ▼ Message Body
    ▼ Session Description Protocol
        Session Description Protocol Version (v): 0
      ▶ Owner/Creator, Session Id (o): addaabbouabdelkader 3798311160 3798311160 IN IP4 127.0.0.1
        Session Name (s): A Funky MONSTER Stream
      ▶ Connection Information (c): IN IP4 127.0.0.1
      ▶ Time Description, active time (t): 0 0
      ▶ Media Description, name and address (m): audio 23002 RTP/AVP 0 8 14
      ▶ Media Attribute (a): rtpmap:0 PCMU/8000
      ▶ Media Attribute (a): rtpmap:8 PCMA/8000
      ▶ Media Attribute (a): rtpmap:14 MPA/8000
```

Figure IV-23: Exemple de la méthode " INVITE ".

IV-4-2-4) Test d'une session data (message)

Le service de messagerie instantanée permet aux utilisateurs connectés de s'envoyer des messages.

La figure suivante montre la réussite de l'envoi du message de l'utilisateur "addaabbouabdelkader" vers l'utilisateur "universitéblida2020".

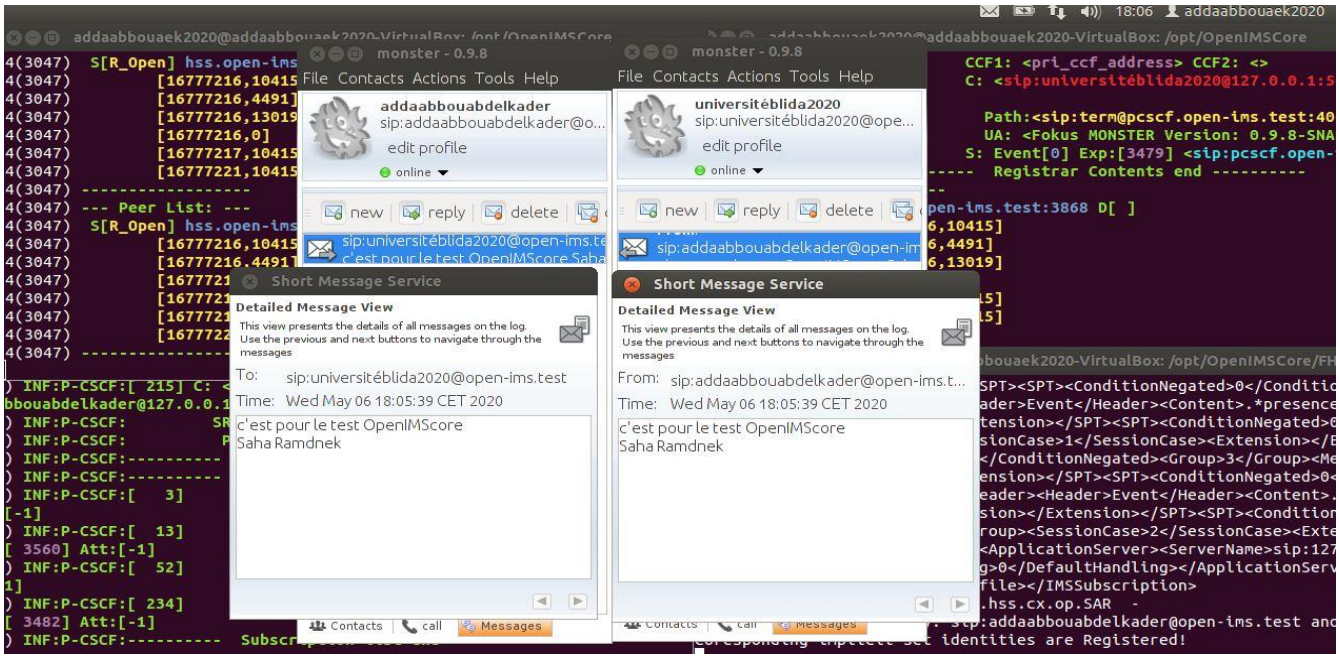
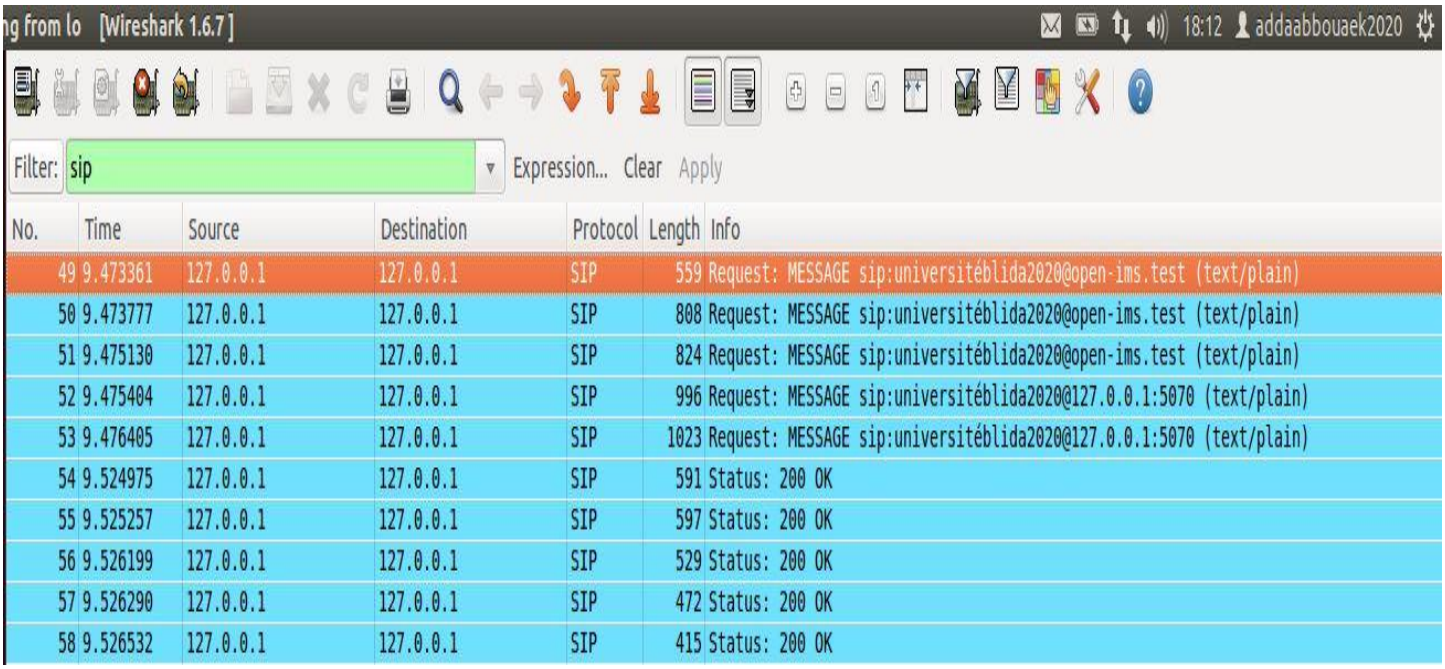


Figure IV-24: Établissement d'une session de données entre utilisateurs.

Le résultat de la capture montre, comme illustrée par la figure suivante, qu'une méthode "MESSAGE" contenant le message instantané à envoyer est expédiée par addaabbouabdelkader pour établir une session de donnée avec universitéblida2020.

Les deux utilisateurs échangent ensuite un message «200 OK» qui indique que le message en question a été bien reçu avec succès.



No.	Time	Source	Destination	Protocol	Length	Info
49	9.473361	127.0.0.1	127.0.0.1	SIP	559	Request: MESSAGE sip:universitéblida2020@open-ims.test (text/plain)
50	9.473777	127.0.0.1	127.0.0.1	SIP	808	Request: MESSAGE sip:universitéblida2020@open-ims.test (text/plain)
51	9.475130	127.0.0.1	127.0.0.1	SIP	824	Request: MESSAGE sip:universitéblida2020@open-ims.test (text/plain)
52	9.475404	127.0.0.1	127.0.0.1	SIP	996	Request: MESSAGE sip:universitéblida2020@127.0.0.1:5070 (text/plain)
53	9.476405	127.0.0.1	127.0.0.1	SIP	1023	Request: MESSAGE sip:universitéblida2020@127.0.0.1:5070 (text/plain)
54	9.524975	127.0.0.1	127.0.0.1	SIP	591	Status: 200 OK
55	9.525257	127.0.0.1	127.0.0.1	SIP	597	Status: 200 OK
56	9.526199	127.0.0.1	127.0.0.1	SIP	529	Status: 200 OK
57	9.526290	127.0.0.1	127.0.0.1	SIP	472	Status: 200 OK
58	9.526532	127.0.0.1	127.0.0.1	SIP	415	Status: 200 OK

Figure IV-25: Capture des paquets de message.

Exemple de la méthode " MESSAGE ":

```
▼ Request-Line: MESSAGE sip:universitéblida2020@open-ims.test SIP/2.0
    Method: MESSAGE
  ▶ Request-URI: sip:universitéblida2020@open-ims.test
    [Resent Packet: False]
▼ Message Header
    Call-ID: f658986053a60c0f9a63040b7330de07@127.0.0.1
  ▶ CSeq: 10 MESSAGE
  ▶ From: <sip:addaabbouabdelkader@open-ims.test>;tag=1011
  ▶ To: <sip:universitéblida2020@open-ims.test>
  ▶ Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKbab8cf7ca70f73490c60c4188befa7e8
    Max-Forwards: 20
    Route: <sip:orig@scscf.open-ims.test:6060;lr>
    Content-Type: text/plain
    User-Agent: Fokus MONSTER Version: 0.9.8-SNAPSHOT
    Content-Length: 4
▶ Message Body
```

Figure IV-26: Exemple de la méthode "MESSAGE".

IV-4-3) Troisième scénarios: (cas d'un client par défaut et un autre à configurer)

Dans ce dernier cas, nous allons faire la simulation d'un appel vocal et de l'envoi de message texte entre deux utilisateurs à savoir:

"addaabbouabdelkader" configuré et enregistré par nos soins sous logiciel client IMS Monster et "bob" déjà préenregistrés sous logiciel UCT IMS Client.

La Figure ci-après confirme l'aboutissement de l'appel de l'utilisateur "bob" vers l'utilisateur "addaabbouabdelkader".

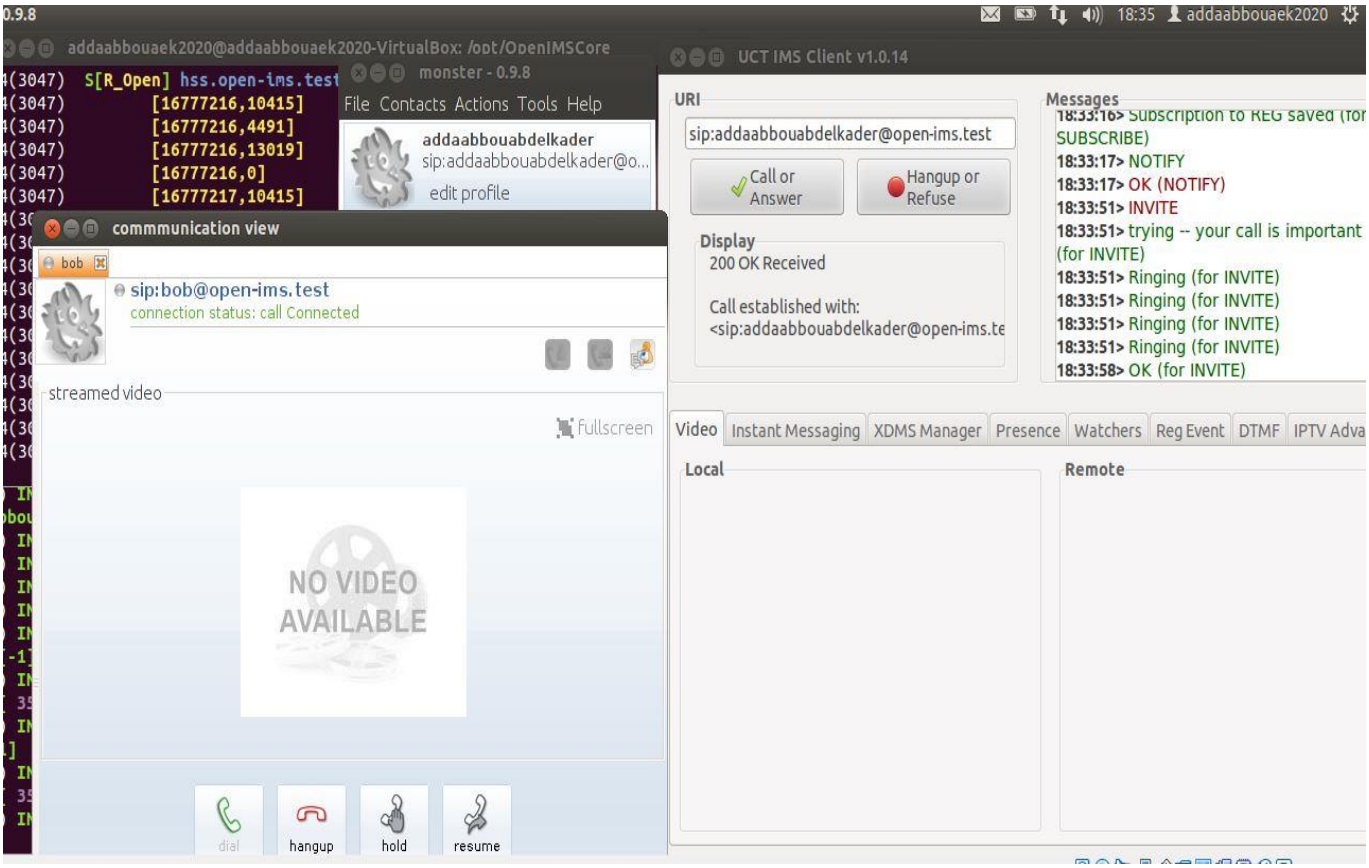


Figure IV-27: Conversation vocale entre Bob et addaabbouabdelkader.

La figure suivante montre la réussite de la réception du message texte par l'utilisateur "addaabbouabdelkader", envoyé par l'utilisateur "bob".

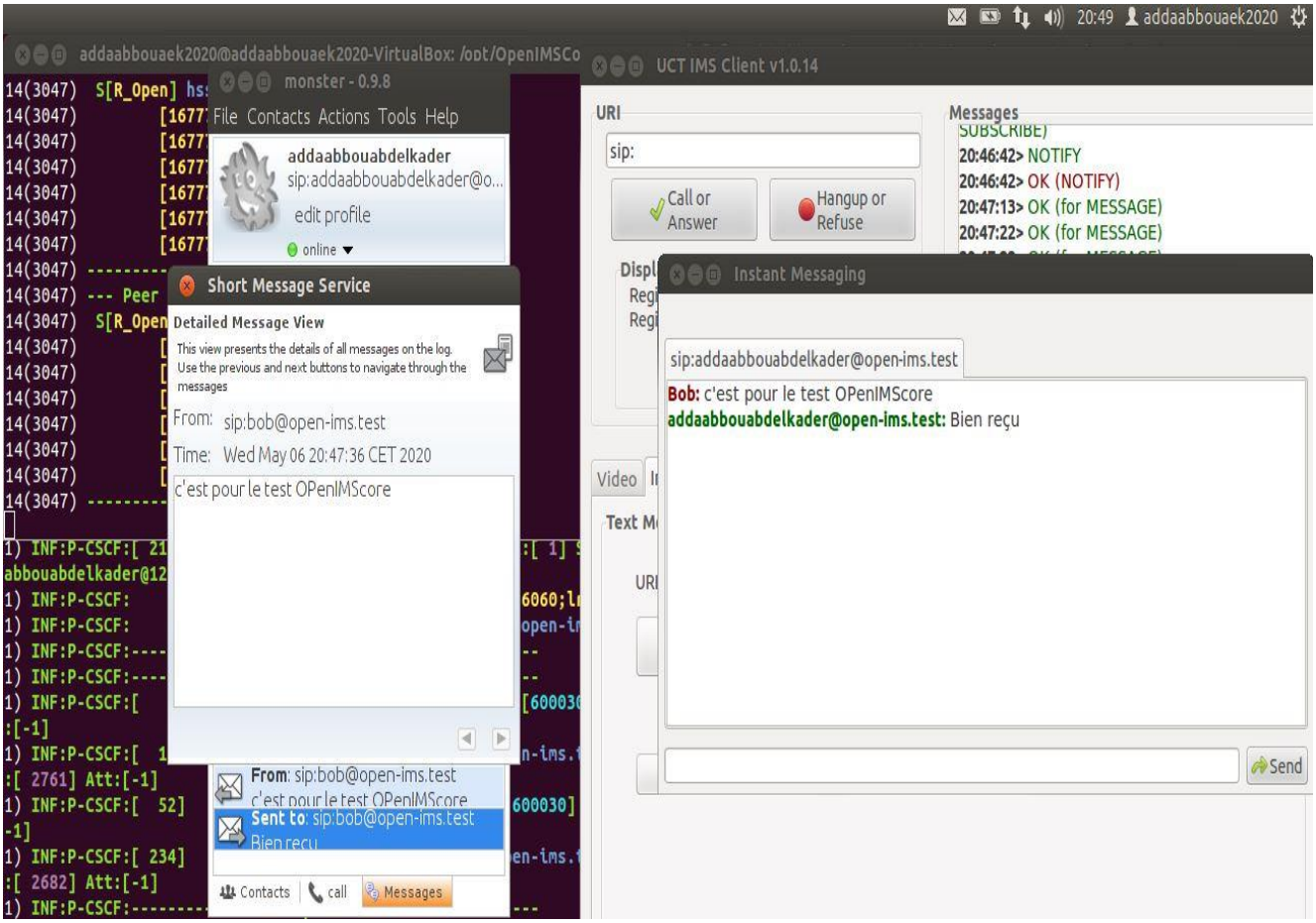


Figure IV-28: Établissement d'une session de données.

Ce dernier scénario a été volontairement rajouté pour démontrer qu'une implémentation Opensource correctement installée peut parfaitement fonctionner quels que soient les terminaux IMS utilisés.

IV-5) Conclusion

Dans ce chapitre, on a mis en œuvre une plateforme IMS par l'implémentation Opensource de plusieurs éléments du réseau IMS qui sont les composants de base de l'architecture IMS telle que définie dans NGN.

Toutes les étapes afférentes à l'installation, la configuration et au test de la solution Opensource nécessaires à la mise en œuvre de la plateforme ont été décrites.

Le déploiement de cette plateforme nous a permis de mieux comprendre la création d'utilisateurs dans la base de données HSS et l'enregistrement de ces utilisateurs dans le réseau IMS notamment avec P-CSCF.

Il nous a également permis d'approfondir nos connaissances en matière d'analyse des échanges des messages du protocole SIP lors de l'enregistrement des utilisateurs et du contrôle d'établissement de sessions multimédias ainsi que des transferts des flux RTP une fois les sessions établies.

La plateforme pourra, bien entendu, être étendue à d'autres services multimédias.

Conclusion Générale

La 4G LTE a apporté une très grande amélioration dans la prise en charge du trafic de données à la fois dans E-UTRAN et EPC, ainsi que dans le développement des services.

Cette technologie utilisant une architecture IP complète pour tous ses services, y compris le service vocal, s'appuie sur un réseau parallèle qui est l'IMS dont la finalité est le traitement des flux et services multimédias dans un but de convergence des réseaux d'accès (fixe ou mobile) à déployer et des terminaux utilisés.

La VoLTE, objet de notre mémoire et faisant donc partie des services multimédias, a contribué à l'amélioration des services vocaux (des appels plus rapides et meilleure qualité vocale) dans la technologie mobile, en utilisant des paquets IP complets qui prennent en charge un débit élevé dans l'infrastructure IMS qui d'ailleurs propose plusieurs services à un réseau d'accès multiple à côté du LTE. C'est à ce titre qu'elle devient incontournable comme solution des services vocaux dans les réseaux radio mobiles par les opérateurs.

Notre projet a eu pour objectif de simuler une plateforme IMS en travaillant sur l'inscription des abonnés et l'échange de services entres eux.

les tests de fonctionnement du banc d'essai ont été mené avec succès.

L'implémentation de l'infrastructure IMS présentée, nous a été d'une expérience bénéfique et très utile pour comprendre à la fois l'enregistrement d'un utilisateur et les flux de signalisation et d'd'appel entre deux utilisateurs dans IMS.

Nous concluons aussi qu'utiliser la technologie IMS et la rendre compatible avec les réseaux de la nouvelle génération NGN était la bonne décision aussi bien dans le domaine technologique que sur le plan économique, car en se basant sur la même plateforme les operateurs n’auront pas des problèmes de compatibilité et le développement en général de leurs services sera plus facile.

Bibliographie

[1]: Martin Sauter, *« From GSM to LTE-Advanced: An Introduction to Mobile Networks and Mobile Broadband »*, Second Edition John Wiley & Sons, 2010.

[2]: Ajay R Mishra, *« GSM: Global System for Mobile Communications Architecture, Interfaces and Identities »*, Edition EFFORT, 2008.

[3]: Ajay R Mishra, *« Nokia Networks ADVANCED CELLULAR NETWORK PLANNINGAND OPTIMISATION 2G/2.5G/3G.EVOLUTION TO 4G »*, John Wiley & Sons Ltd Nokia Networks 2007

[4]: Lairedj Khalil Ibrahim*, « 3g++ radio network dimensioning, planning and optimization»*, TELECOM Engineering Graduation Project, INTTIC & HUAWEI, 2015.

[5]: Moray Rumney, *« LTE and Evolution to 4g wireless, Design and measurement Challenges »*, Aglient Technologies, by John Wiley & Sons, July 2009.

[6]: *« The LTE Network Architecture A comprehensive tutorial »*, Acatel Lucent white paper, 2009.

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

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

[9]: *« IMS Architecture, the LTE User Equipment Perspective »*, SPIRENT WHITE PAPER, 2014.

[10]: André Pérez, *« La voix sur LTE (réseau 4G et architecture IMS) »*, Edition Lavoisier, 2013.

[11]: NAOUI Khaled & BENAHMED Sidali, *« ETUDE ET MISE EN PLACE DE LA SOLUTION VOIP OVER LTE, DIMENSIONNEMENT ET MESURE DE LA QoS »*, USTHB, Master Degree thesis, 2015.

[12]: 3GPP TS 29.229, *« Cx and Dx interfaces based on the Diameter protocol; Protocol details »*, Sept 2007.

[13]: RFC 3588, P. Calhoun et al., *« Diameter Base Protocol »*, Sept 2003.

[14]: 3GPP, TS 24.229 V9.3.1, *« IP Multimedia Call Control Protocol Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) »*, Stage 3 (Release 9). December 2009.

[15]: Miikka Poikselk¨a, Harri Holma, Jukka Hongisto, Juha Kallio and Antti Toskala, *« Voice over LTE: VoLTE »*, John Wiley & Sons Ltd Nokia Networks 2012.

[16]: 3GPP Technical Specification 23.203, *« Policy and charging control architecture (Release 11) »*, www.3gpp.org, 2012.

[17]: Laurent Ouakil - Guy Pujolle, *« Téléphonie sur IP 2éme Edition »*, EYROLLES, 2012.

[18]: Openims-core-project , *https://www.ims-way.com/openims-core-project, 2011*.

[19]: *http://openimscore.sourceforge.net/ .*

[20]: Hani Nemati, «https://sites.google.com/site/haninemati/developing-ims/installing-openimscore-on-ubunto-12-04».Personal Website