ROYAUME DU MAROC
AGENCE NATIONALE DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS
INSTITUT NATIONAL DES POSTES ET TÉLÉCOMMUNICATIONS

INPT

المملكة المغربية
الوكالة الوطنية لتقنين المواصلات
المعهد الوطني للبريد والمواصلات السلكية واللاسلكية

Rapport de stage d'été 2008

INE 2

Etude de l'architecture IMS et configuration d'OpenSer comme serveur de présence au dessus de l'OpenIMS

Présenté par

BAHA Rachid
FARAJ Abderrahim
NIHARMINE Lahcen

Encadrant :

Mr .MEZRIOUI Abdellatif

Table des matières

Chapitre 2: La plate forme Open Source IMS

Chapitre 3: Le service de présence dans l'IMS

Remerciement

Nous tenons à adresser nos sincères remerciements à notre encadrant M. Abdellatif MEZRIOUI. D'une part, il nous a confiés ce projet de stage et pour son encadrement. Et d'autre part pour le large délai qu'il nous a donné pour accomplir ce projet.

Nous témoignons aussi notre profonde reconnaissance à tous ceux qui ont participé de près ou de loin à la réalisation et la réussite de ce projet.

Résumé

Le monde des télécommunications a beaucoup évolué durant les dernières années avec l'apparition de nouveaux services basés sur le protocole IP tel que la voix sur IP et la vidéo sur IP. L'Internet supporte depuis déjà plusieurs années de nombreux services à succès tels que l'e-mail, le web, le streaming audio/vidéo, le « chat » et des applications de téléphonie et des communications multimédia (Skype, AOL…) sont déjà présents sur ce marché.

Dans cette optique les opérateurs de télécommunications se trouvent face à recentrer leurs business autour des applications sur IP. Ceci à travers le développement d'une architecture IMS seule normalisée.

Le but de ce stage est l'étude de l'architecture IMS et la configuration d'OpenSer comme serveur de présence au dessus d'OpenIMS.

Introduction générale

Aujourd'hui, avec le développement de la prochaine génération de réseau (NGN), de nouvelles normes à venir sont mise en place pour la voix et de vidéo. VoIP (Voice over IP) est en train de devenir très populaire. Il se développe rapidement, remplacent peu à peu les traditionnels services de téléphonie progressivement en raison de sa flexibilité et son coût moins cher. En outre, la VoIP a le potentiel pour ouvrir la voie à la convergence voix données et réseaux qui peuvent offrir des applications de communications pour les utilisateurs, n'importe où, n'importe quand. Différents protocoles de VoIP et des solutions ont créé la compatibilité et l'interopérabilité des obstacles. La sécurité et la QoS sont très importants pour les entreprises.

Comme l'élément clé dans les réseaux NGN, IMS (IP Multimedia Subsystem) joue un rôle important en offrant des fonctionnalités clés telles que la QoS, la sécurité, la gestion de groupe, et de messagerie vocale instantanée. IMS, il est plus facile pour les opérateurs d'offrir de nouveaux services, par rapport au GSM, lorsque cela est très limité L'IMS est un processus ouvert, architecture normalisée qui vise à fusionner les services multimédias à travers le monde cellulaire et les réseaux IP, en utilisant les mêmes protocoles standard pour les mobiles IP fixe et des services. Elle est définie par la 3rd Generation Partnership Project (3GPP). Pour les fournisseurs de services, IMS (IP Multimedia Subsystem) permettra le déploiement de nouveaux services basés sur les normes tout en réduisant les coûts. Pour les utilisateurs finaux, IMS peut se permettre une nouvelle, flexible et personnalisée en temps réel service de communication à travers n'importe quel réseau et n'importe quel dispositif, qu'il s'agisse d'un PDA, PC, téléphone mobile ou la télévision. Avec ces caractéristiques, IMS serait le cœur de réseau NGN.

L'Open Source IMS est un système multimédia IP pour l'épreuve. Il a été développé par l'Institut Fraunhofer FOKUS. Ils font remarquer que cette plateforme Open Source IMS Core System n'est pas destinée à devenir ou à agir comme un produit dans un contexte commercial. Son seul but est de fournir une base de référence IMS mise en œuvre de la technologie de test IMS et le prototypage d'applications à des fins de recherche.

Ce document présente le travail qui est réalisé dans ce stage. Pour en arriver là aujourd'hui, il a fallu passer par différentes étapes qui sont expliquées tout au long de ce rapport. Après une brève introduction générale au projet, nous présenterons l'environnement technique IMS qui est l'architecture visée. Ensuite, nous étudierons les différentes solutions de serveurs d'applications SIP open source, puis on va parler sur le service de présence dans l'architecture IMS et enfin nous terminerons par quelques tests de notre application.

Chapitre 1
L'IP Multimedia Subsystem

1. Contexte général :

À l'heure actuelle, les réseaux cellulaires ont déjà fourni un large éventail de services cellulaires et les utilisateurs peuvent accéder à l'Internet en utilisant une connexion de données et l'accès des services Internet. Alors, pourquoi avons-nous besoin de l'IMS ?

Dans le réseau 3G et dans le domaine circuit les circuits sont utilisés pour le transport de la voix et la vidéo, ou sont utilisés pour le transport des messages instantanés. Il existe deux différents plans dans les circuits réseaux: le plan de signalisation et les médias avion. «Le plan de signalisation comprend les protocoles utilisés pour établir un circuit commuté-chemin entre les terminaux et le plan médias comprend les données transmises sur les circuits chemin entre les terminaux." Et le plan médias comprend également le codage voix échangées entre les utilisateurs.

La raison pour laquelle l'IMS est crée est de permettre à des accusations de sessions multimédia de façon appropriée. «L'IMS fournit des informations sur le service soit invoqué par l'utilisateur, et avec cette information, l'opérateur décide d'utiliser un taux forfaitaire pour le service, appliquer traditionnelle basée sur le temps de charge, s'appliquent QoS fondé, ou d'effectuer une nouvelle type de tarification »

L'autre principale raison de l'existence de l'IMS a été de fournir des services intégrés pour les utilisateurs. Service développeurs utilisent l'interface standard défini par le SSI, de sort que les opérateurs peuvent intégrer les services et de créer de nouveaux services.

Les opérateurs veulent aujourd'hui plus de fournir des paquets de services pour les utilisateurs, c'est l'Internet mobile doit devenir plus attrayant à ses utilisateurs. Dans cette condition, l'IMS a été mis en place. Ainsi, l'IMS a pour but de:

- Combiner les dernières tendances à la technologie
- Faire le paradigme de l'Internet mobile devient réalité
- Créer une plate-forme commune pour développer divers services multimédias
- Créer un mécanisme permettant de renforcer les marges supplémentaires en raison de l'usage de la téléphonie mobile de paquets réseaux

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

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

2. Historique de la normalisation de l'IMS

2.1 - IMS Forum

- **1999** - Création de l'IMS Forum par des industriels de la téléphonie mobile (3GPP2) avec l'idée de réaliser la convergence de services mobiles et filaires voix et multimédia sur la base de IPv6.
- **2001** - Réalisation de prototypes et d'essais de compatibilité en IPv4.
- **2005** - Publication de la version 5 de la norme de l'IMS Forum.
- **2006** - Publication de la version 6.

2.2 - TISPAN (ETSI)

- **2003** - Fusion à l'ETSI des groupes de travail SPAN, Signaling System N°7, R1 et TIPHON (Telephony on Internet) en un seul groupe appelé TISPAN NGN (100, puis 300 membres). Décembre 2005 - Publication de la première édition de la norme ETSI sur IMS, centralisée sur l'accès fixe à haut débit en DSL, la 3G et le GPRS en IPv4 (50 normes, dont certaines à finaliser). Il reste encore à traiter du transit, de l'encapsulation ISUP, des appels d'urgence, des interceptions légales; etc.
- **2006** - TISPAN travaille avec le DSL Forum, l'UIT-T, le 3GPP, l'IETF, le DVB Forum et les groupes OMA/Parlay spécialisés dans le Réseau Intelligent.
- **2007** - Sortie prévue de la version 2 de la norme IMS de l'ETSI avec IP/TV, VoD, QoS, accès "entreprise", "content delivery", etc.
- **2009** - Sortie annoncée de la version 3 relative à la mobilité généralisée et à la convergence.

2.3 -Le 3GPP

Le 3GPP (www.3gpp.org) est né en 1998 grâce à un accord de collaboration entre différents organismes de normalisation régionaux dont l'ARIB1 du Japon, le CCSA2 de la Chine et l'ETSI. A l'origine, le 3GPP avait pour but de développer les spécifications et rapports techniques d'un réseau mobile de troisième génération basé sur le GSM3. Aujourd'hui, le 3GPP s'occupe aussi du développement et de la maintenance des spécifications du GSM.

2.4 -L'IETF

L'IETF définit et promeut les standards du monde Internet en collaboration avec le W3C4 et l'ISO5. L'IETF s'occupe particulièrement des protocoles de la pile TCP/IP (Transmission Control Protocol/Internet Protocol). C'est un organisme ouvert composé de personnes volontaires et qui n'impose aucune contrainte : toute personne physique ou morale peut participer à l'effort de normalisation.

[1] Association of Radio Industries and Business
[2] China Communications Standards Associations
[3] Global System for Mobile communication
[4] World Wide Web Consortium
[5] International Standards Organization

3. Les protocoles de l'IMS:

Lorsque le 3GPP a commencé à développer l'IMS, un système basé sur les protocoles IP (sont généralement développés par l'IETF), il s'est appuyé sur le travail déjà accompli par l'IETF et l'ITU-T6 réduisant ainsi le temps et le coût de développement.

3.1 Contrôle de la session : SIP

Le protocole qui contrôle les appels joue un rôle très important dans tout système de téléphonie. Spécifié par l'IETF comme protocole pour l'établissement et la gestion de sessions multimédia sur les réseaux IP, SIP était très célèbre lors du choix du protocole de signalisation par le 3GPP. SIP[7] (RFC 3261) utilise le modèle client/serveur comme c'est le cas de la plupart des protocoles développés par l'IETF. Les principes de SIP ont été empruntés de SMTP[8] (RFC 2821) et plus particulièrement de HTTP[9] (RFC 2616). SIP a ainsi hérité des deux protocoles les plus célèbres du monde Internet. Contrairement à BICC et H323, SIP ne fait pas de différence entre les connexions Hôte-Réseau (UNI : User to Network Interface) et Réseau-Réseau (NNI : Network to Network Interface). SIP est aussi un protocole textuel ce qui facilite son extension, le débogage et la création des services (SIP étant basé sur HTTP, les développeurs de services peuvent utiliser toute la puissance de l'architecture HTTP comme les CGI[10] ou encore les Servlets Java).

SIP a été choisi comme protocole pour le contrôle de la session dans l'IMS et le fait que SIP facilite le développement de services a joué un grand rôle dans le choix du 3GPP. Une présentation du protocole SIP se trouve en **Annexe A**.

3.2 Autorisation/Authentification/Accounting : Diameter

En plus du protocole de gestion de la session, il existe d'autres protocoles qui jouent un rôle significatif dans l'IMS. Diameter (RFC 3588) a été choisi comme protocole AAA[11] dans l'IMS. Diameter est une évolution du protocole RADIUS[12] (RFC 2865) qui est un protocole très utilisé sur Internet pour faire l'AAA. Diameter consiste en un protocole de base auquel on ajoute ce que l'on appelle les applications Diameter. Les applications Diameter sont des extensions ou des implémentations spécifiques de Diameter pour une application particulière dans un environnement donné.
L'IMS utilise Diameter dans un certain nombre d'interfaces bien que toutes les interfaces n'utilisent pas forcément la même application Diameter.

[6] International Telecommuications Union - Telephone
[7] Session Initiation Protocol
[8] Simple Mail Transfer Protocol
[9] Hyper Text Transfer Protocol
[10] Common Gateway Interface
[11] Authentication Authorisation Accounting
[12] Remote Authentication Dial In User Service

3.3 Autres protocoles

En plus de Diameter et de SIP, l'IMS utilise d'autres protocoles :

- SDP[13](RFC 4566) est utilisé pour initialiser ou modifier les paramètres media utilisés par la session.
- COPS (RFC 2748) est utilisé pour le transfert des politiques entre les PDP[14] et les PEP[15].
- H.248 est utilisé par les nœuds de signalisation pour contrôler les nœuds situés dans le plan media (exemple le media gateway controller qui contrôle le media gateway). H.248 a été développé par l'ITU-T et l'IETF et porte le nom de MEGACO[16].

- RTP[17] (RFC 3550) et RTCP[18] (RFC 3550) sont utilisés pour transporter les medias temps réel comme l'audio ou la vidéo.

4. L'architecture de l'IMS :

4.1 L'architecture fonctionnelle de l'IMS :

Dans cette partie, on va faire une description synthétique des différents composants de l'architecture IMS

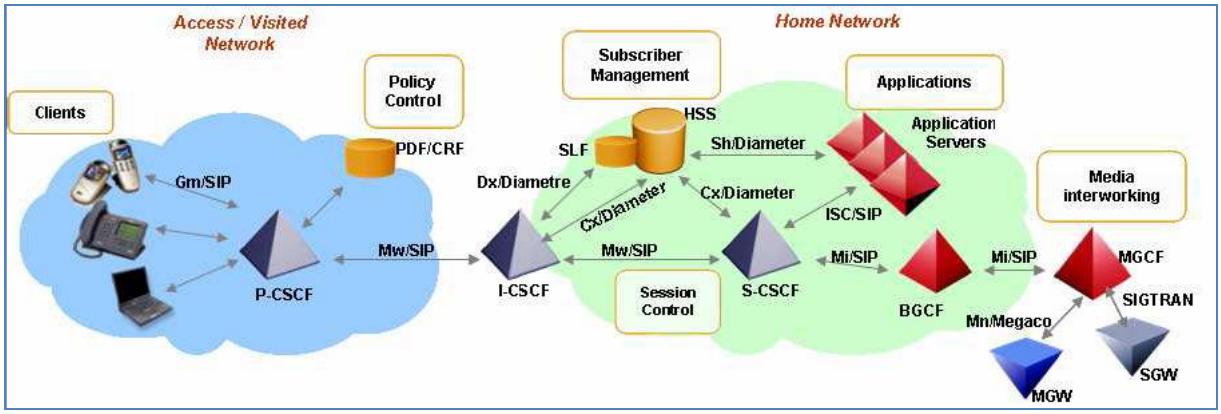

Figure 1.1 : Architecture fonctionnelle de l'IMS

[13] Session Description Protocol
[14] Policy Decision Point
[15] Policy Enforcement Point
[16] MEdia GAteway COntrol
[17] Real-Time Transport Protocol
[18] RTP Control Protocol

4.1.1 HSS : Home Subscriber Server

- Le HSS est l'équivalent du HLR de GSM. Elle contient toutes les informations nécessaires à un utilisateur pour ouvrir une session multimédia :
  - Des informations sur la localisation de l'utilisateur.
  - Le profil de l'utilisateur c'est à dire l'ensemble des services auxquels l'utilisateur est abonné.
  - L'adresse du S-CSCF alloué à l'utilisateur.
  - Des informations de sécurités.
- Le SLF est une base de données contenant pour chaque utilisateur le HSS correspondant dans le cas ou le réseau contient plusieurs HSS.

4.1.2 C-CSCF: Call/Session Control Function

Le C-CSCF est un serveur SIP qui traite la signalisation SIP en IMS. Il existe 3 types de C-CSCF :

- ✓ **P-CSCF: Proxy CSCF**

Le P-CSCF est le premier point de contact usagers avec IMS : Toute la signalisation SIP du UE et vers le UE passe via le P-SCSF. Le P-CSCF est alloué à l'utilisateur dans la phase de registration et ne change pas durant toute la durée de registration. Le P-CSCF peut être localisé dans le home network, comme dans le visited network

Les différentes fonctionnalités :

- Sécurité :
  - Il maintient des associations de sécurité IPsec entre lui et l'équipement terminal.
  - Authentification de l'utilisateur.
- Il maintient un cache local pour la localisation du S-SCSF associé à l'utilisateur.
- La compression / décompression des messages SIP.
- Le P-CSCF inclut les fonctionnalités du Policy Décision Function (PDF). Le PDF gère les exigences QoS pour les services et autorise l'allocation des ressources.
- La génération de CDRs (Call Detailed Record) taxation.

- ✓ **I-CSCF : Interrogating – CSCF**

- L'I-CSCF est localisé dans le home network.
- Fait une première autorisation pour l'accès au réseau IMS.
- Pour une requête SIP, il contacte le HSS pour identifier le S-CSCF correspondant et renvoie les messages de cette session à ce S-CSCF (Protocole Diameter sur l'interface I-CSCF – HSS).
- Peut incluse une fonctionnalité de masquage de l'architecture du réseau de l'opérateur par rapport au réseau visité.

- ✓ **S-CSCF : Serving CSCF**

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

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

4.1.3 Serveurs d'applications (AS)

Il y a 3 types de serveur qui agissent comme un serveur SIP du point de vue du réseau IMS.

- Serveur SIP d'application qui effectue des services IP multimédia basé SIP.
- OSA-SCS (Open Service Access – Service Capability Server): C'est une gateway OSA qui implémente l'API Parlay. Elle permet à des serveurs d'application tiers d'accéder au réseau IMS d'une façon sécurisé pour fournir des services aux utilisateurs.
- IMS-SSF (IP Multimedia Service Switching Function) : permet de réutiliser les services CAMEL développer pour les technologies GSM et GPRS. Donc une gsmSCF peut contrôler une session IMS grâce à ce serveur.

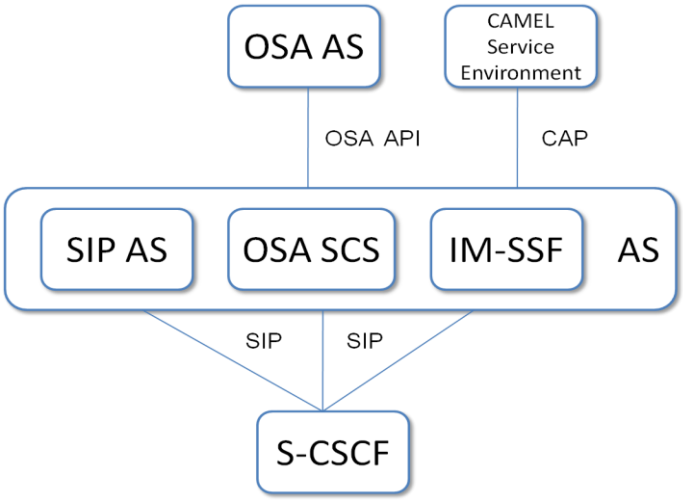

Figure 1.2 - Types de serveurs d'applications dans l'IMS

4.1.4 Le MRF

Le MRF19 offre une source de medias dans le réseau home. Il peut jouer des annonces audio, mixer les flux média (dans un pont de conférence centralisé par exemple), transcoder entre différents codecs, faire des statistiques ou encore analyser tout type de média.

Le MRF est divisé en un nœud dans le plan de signalisation, le MRFC20, et un nœud dans le plan media, le MRFP21. Le MRFC se comporte comme un UA22 SIP et a une interface avec le S-CSCF. Le MRFC contrôle le MRFP via une interface H.248. Le MRFP implémente toutes les fonctionnalités liées aux medias tel que le mixage de différents types de medias.

4.1.5 Le BGCF

Le Breakout Gateway Control Function est essentiellement un serveur SIP qui offre le routage des requêtes en fonction des numéros de téléphone. Le BGCF est utilisé dans le cas où la session initiée par le terminal IMS est destinée à un usager d'un réseau à commutation de circuit tel que le RTC. Les fonctionnalités principales du BGCF sont :

- choisir le bon réseau à commutation de circuit auquel s'interconnecter
- ou bien choisir la bonne passerelle RTC/CS lorsque l'interconnexion a lieu dans le réseau où est situé le BGCF.

4.1.5 L'IMS-ALG et le TrGW :

L'IMS supporte deux versions du protocole IP : IPv4 (RFC 791) et IPv6 (RFC 2640). À un certain moment dans le réseau on peut avoir besoin d'interconnecter ces deux versions. Pour permettre l'interfonctionnement entre ces deux versions sans pour autant imposer au terminal de les supporter tous les deux, l'IMS a introduit deux nouvelles entités qui permettent le passage d'une version à l'autre. Ces deux nouvelles entités sont l'IMS-ALG (IMS Application Layer Gateway) et le TrGW (Transition Gateway). Le premier gère les messages de signalisation (SIP ou SDP) alors que le second s'occupe des media (RTP, RTCP).

4.1.6 ***PSTN/CS Gateway.***

Le PSTN gateway constitue une interface vers les réseaux à commutation de circuit. Cette interface présente plusieurs entités fonctionnelles suivant l'architecture Softswitch :

- **SGW :** Signaling Gateway

C'est la fonction de transcodage de la signalisation, qui permet grâce à SIGTRAN de transporter la signalisation SS7 sur IP, et d'avoir une interface NNI de signalisation avec les réseaux à commutation de circuit. Il effectue les conversions des protocoles dans les couches bas.

- **MGCF :** Elle permet de contrôler les MGW, et elle s'interface avec SIGTAN pour l'échange de la signalisation.
- **MGW :** interface pour le plan de données entre le réseau IMS/IP et les réseaux PSTN à commutation de circuit. D'un côté, elle capable d'envoyer et de recevoir le flux IMS sur le protocole RTP, d'un autre côté il utilise le PCM pour coder la voix et la transmettre sur des times slots au réseau CS. Une autre fonction de transcodage lorsque le terminal ne supporte pas les codes utilisés par le CS.

Le tableau ci-dessous représente les différentes interfaces de l'IMS et leurs caractéristiques :

Interface	Entités IMS	protocole	Description
Gm	UE,P-CSCF	SIP	Utiliser pour l'échange des messages entre UE et CSCFs
Mw	P-CSCF,I -CSCF,S-SCSCF	SIP	Utiliser pour l'échange des messages entre CSCFs
ISC	S-CSCF, I-CSCF,AS	SIP	Utiliser pour l'échange des messages entre CSCF et AS
Mg	MGCF->I-CSCF	SIP	MGCF converts ISUP signaling to SIP signaling and forwards SIP signaling to I-CSCF
Mi	S-CSCF->BGCF	SIP	Utiliser pour l'échange des messages entre S-CSCF et BGCF
Mj	BGCF->MGCF	SIP	Utiliser pour l'échange des messages entre BGCF et MGCF dans le même réseau IMS network
Mk	BGCF->BGCF	SIP	Utiliser pour l'échange des messages entre BGCFs dans les différents réseaux
Mr	MRCF,S-CSCF	SIP	Utiliser pour l'échange des messages entre S-CSCF et MRFC
Cx	I-CSCF,S-CSCF,HSS	Diameter	Utiliser pour communiquer entre I-CSCF/S-CSCF et HSS
Dx	I-CSCF,S-CSCF,SLF	Diameter	Used by I-CSCF/S-CSCF to find a correct HSS in a multi-HSS environment
Sh	SIP AS,OSA,SCF,IM-SSF,HSS	Diameter	Utiliser pour l'échange des informations entre SIP AS/OSA SCS et HSS
Dh	SIP AS,OSA,SCF,IM-SSF,HSS	Diameter	Used by AS to find a correct HSS in a multi-HSS environment
Go	PDF,GGSN	Diameter	Allows operators to control QoS in a user plane and exchange charging correlation information between IMS and GPRS network
Gq	P-CSCF,PDF	Diameter	Used to exchange policy decisions-related information between P-CSCF and PDF

5. Concepts de l'IP Multimedia Subsystem

Dans cette partie, nous allons introduire l'architecture basique et les concepts de base du système l'IMS.

5.1 Session multimedia IP

Les réseaux existant supportent les services voix, vidéo et messages en se basant sur la commutation du paquet. L'IMS garde la continuité des services offerts aux utilisateurs en cas de déplacement d'un réseau à un autre de type différent. Avec l'IMS, les utilisateurs disposent de choix de mixer les services basés IP, par exemple deux utilisateurs en communication peuvent par la suite ajouter d'autres applications, comme les jeux ou la vidéo, à leur session qu'ils ont ouverte initialement pour la voix.

5.2 Connectivité IP

Comme son nom l'indique, L'IMS implique des équipements terminaux supportant l'IP. Avec l'IPv6 les équipements terminaux peuvent se joindre facilement vu la non saturation en terme d'adresses IP. Le terminal obtient son adresse IP soit via le réseau IMS ou via le réseau visité même si ce dernier n'est pas un réseau IMS, mais supportant bien sûr l'IP. Ceci dans le but que l'utilisateur bénéficiera des services IMS dans les zones où ce dernier n'est pas disponible.

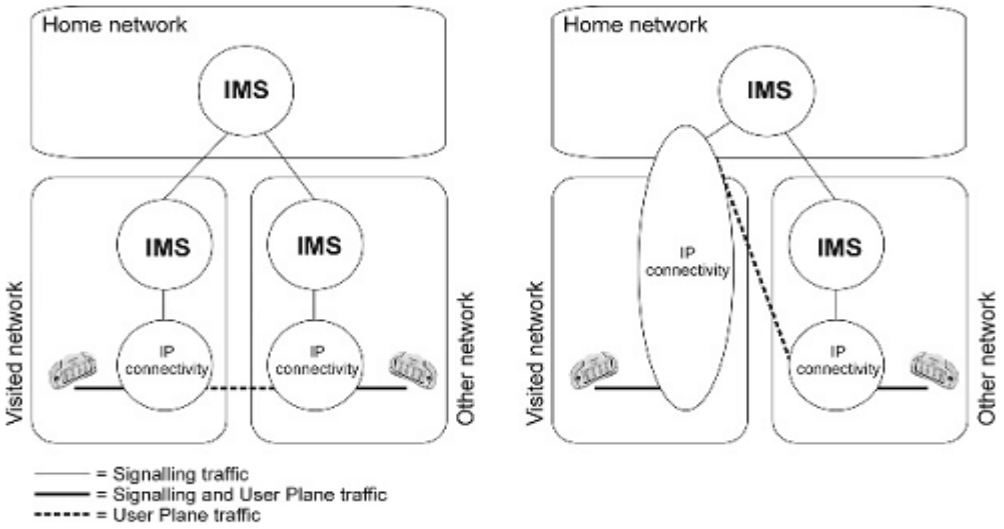

Figure 1.3: connexion IMS en cas de roaming.

5.3 Assurer la QoS des services multimédia IP.

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

- *Type de média, direction du trafic.*
- *Débit binaire, taille du paquet et leur fréquence du transport.*
- *L'usage de la charge RTP pour les types de média.*

- *Adaptation de la bande passante.*

Apres avoir discuté lesdits paramètres au niveau applicatif, l'équipement de l'utilisateur procède à une réservation des ressources qu'il lui faut à partir du réseau d'accès. Maintenant que la QoS de bout en bout est créée, le terminal encapsule ses paquets à l'aide d'un protocole approprié (RTP), ensuite transférés, via l'IP, vers le réseau d'accès et de transport avec l'un des protocoles de la couche transport.

5.4 Politique IP de contrôle de bon usage des ressources.

La politique de contrôle IP signifie le pouvoir à autoriser et à contrôler l'usage des porteuses du trafic destiné à l'IMS comme prévu dans les paramètres de signalisation de la session IMS. Ceci exige une interactivité entre le réseau d'accès IP et le réseau IMS. L'installation de cette interactivité peut se faire selon trois catégories différentes:

- La politique du contrôle peut vérifier est-ce que les valeurs négociées dans la signalisation SIP sont utilisées lors de l'activations des porteuses du trafic. Ce qui permet à l'opérateur de contrôler l'utilisation de ses ressources afin d'éviter tout usage abusif.
- La politique du contrôle peut savoir quand commence et quand se termine le trafic d'une session SIP établie entre deux usagers.
- La politique du contrôle peut recevoir des avis sur toute modification, suspension ou libérations des porteuses engagées dans un service associé à un utilisateur durant l'établissement d'une session. Ce qui dit une bonne gestion des ressources.

5.5 La sécurité des communications.

La sécurité n'est pas un élément propre à l'IMS, mais elle est fondamentale pour tous les systèmes de communication. Le système IMS dispose de ses propres mécanismes de contrôle et d'authentification entre l'UE et le réseau. Dans ce sens l'IMS offre un niveau de sécurité similaire à ceux connus dans le GPRS et les réseaux à commutation du paquet. La figure ci-dessous représente un résumé de la solution sécurité.

Figure 1.1: Aspect de la sécurité IMS.

5.6 Roaming

De point du vu utilisateur, il est important d'avoir accès au services indépendamment de sa localité géographique. L'option de roaming rend possible l'accès aux services même si l'utilisateur ne se trouve pas dans la zone couverte par le réseau nominal.

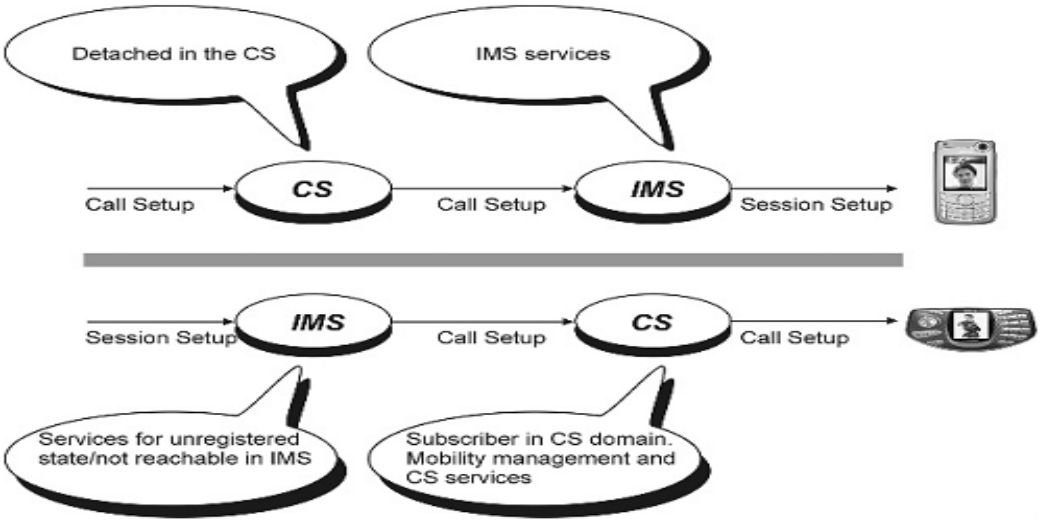

Figure 1.2: IMS/CS alternatives de roaming.

5.7 Interopérabilité avec les autres réseaux.

Il est bien évident que l'architecture IMS n'est pas déployée au même temps partout dans le monde. Ceci ralenti le basculement des utilisateurs d'un terminal à un autre et dans ce cas la difficulté de joindre un utilisateur dépend du terminal utilisé et de sa localité géographique. Pour devenir une technologie de communication réussie, l'IMS doit pouvoir connecter un grand nombre possible d'utilisateurs. Par conséquent l'IMS supporte la communication avec PSTN, ISDN, les utilisateurs mobile et Internet. En plus, il est possible de supporter des sessions avec des applications Internet développées hors la communauté 3GPP.

5.8 Mode de contrôle de services.

Dans les réseaux mobiles de 2ème génération le mode « viseted service control » est pris en charge. Une entité dans le réseau visité fournit les services et contrôle le trafic pour un utilisateur en cas de roaming. Cette entité est appelée « viseted mobile service switching center» pour le cas les réseaux 2G. A partir de la realise 5, à la fois les modes « viseted service control » et « home service contol » sont supportés. Le fait de supporter les deux modes devrait signifier des extensions additionnelles des protocoles de IETF et l'augmentation des efforts à fournir pour l'enregistrement et la supervision des sessions. Le mode « viseted service control » a été annulé vue qu'il s'agissait d'une solution complexe et que sa valeur ajouter était faible vis-à-vis de celle du mode « home service control », il présente aussi des limitations telle que : des rapport multiples et des modèles de roaming entre opérateurs. Par conséquent seul le mode « home service control » été sélectionné : l'entité qui a l'accès aux base de données utilisateur et qui interagit directement avec la plate-forme de service est toujours située dans le réseau nominal de d'utilisateur.

5.9 Structure en couches.

Le 3GPP a décidé d'utiliser une approche en couche pour l'architecture du système IMS. Ceci dit que les services de transport sont séparés de la signalisation IMS et des services de gestion de sessions.

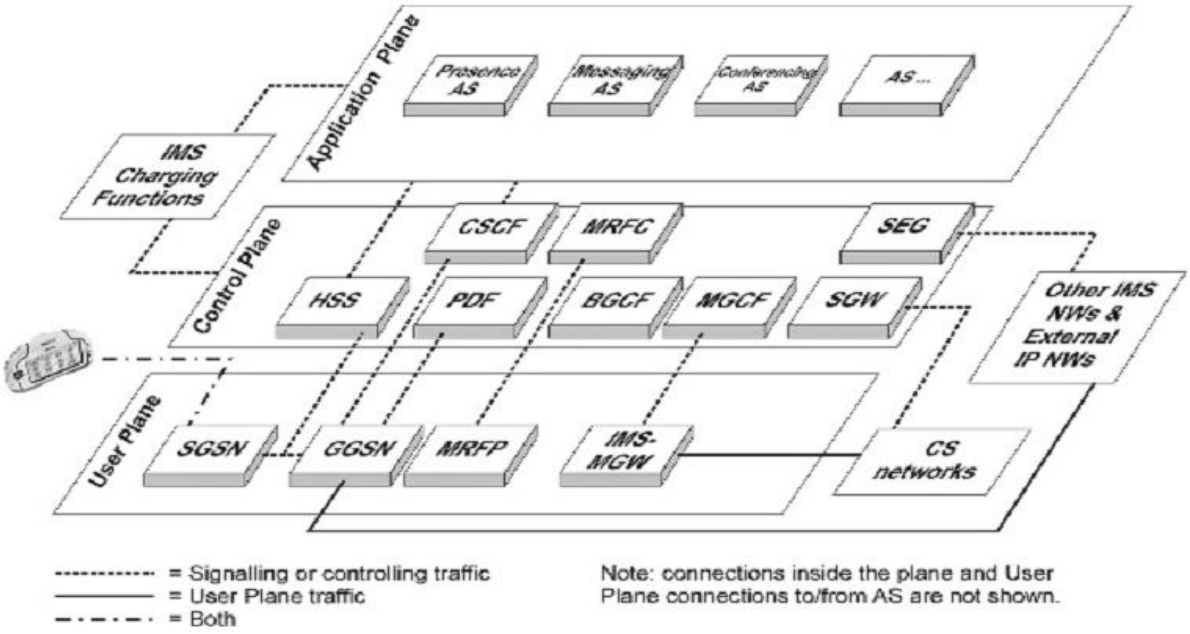

Figure 1.3: Architecture en couche de l'IMS.

Les services se déroulent donc dans la couche située en haut du réseau de signalisation comme montre la figure 6. Cette approche conduit à un minimum de dépendance entre les couches, ce qui facilite l'ajout d'autres réseaux d'accès au système déjà en service à titre d'exemple : WLAN (Wireless Local Area Network) qui a été ajouté dans la release 6 de 3GPP comme réseau d'accès au système IMS.

Ladite approche favorise l'importance de la couche application, vue que les services sont conçus marcher indépendamment du réseau d'accès, l'IMS sert de pont entre eux. Dans le but de communiquer, l'utilisateur peut utiliser soit un mobile soit un PC client et les mêmes fonctions IMS seront utilisées. Les exigences des différents services sont :

- Bande passante
- Latence ;
- Puissance de traitement dans les équipements.

La fonctionnalité multi-accès est introduite dans l'architecture IMS, elle offre aux opérateurs de mobile et de fixe une méthode de délivrer la solution de convergence mobile-fixe. Ceci permet aux fournisseurs de service d'employer les caractéristiques et les possibilités présentes dans l'équipement choisi ainsi que les méthodes disponibles sur son réseau d'accès

6. Identification dans l'IMS:

Dans tout réseau il doit être possible d'identifier de façon unique chaque utilisateur. L'IMS offre la possibilité d'identifier non seulement les utilisateurs mais aussi les services.

6.1 Les identités publiques:

C'est une adresse publique qui permet d'identifier un utilisateur. L'opérateur attribut une ou plusieurs adresse publique pour chaque utilisateur IMS. C'est la grande nouveauté, ce qui

permet à l'utilisateur de séparer son identité personnel, familiale et d'affaire pour générer des services différents. L'identité publique de l'utilisateur est l'équivalent du MSISDN en GSM, donc c'est une adresse de contacte qui permet de joindre un abonné, elle sert à router les messages SIP. La Public User Identity peut être sous deux formats :

- SIP URI : sous la forme « sip : premier.dernier@opérateur.com ». Il est aussi possible d'inclure un numéro de téléphone dans une SIP URI qui sera sous le format :

  « sip: +1-961-007-007@opérateur.com ; user=phone ».

- TEL URL : permet de représenter un numéro de téléphone dans un format international « tel : +1-961-007-007 ». Il est impossible de s'enregistrer avec un TEL URL, il faut toujours une SIP URI pour se faire. Mais le TEL URL est utilisé pour faire des appels entre le monde RTC et le monde IMS. Or en RTC les téléphones sont identifiés par des numéros et ne peuvent composer que des numéros. Donc l'opérateur IMS doit allouer à chaque utilisateur au moins une SIP URI et un TEL URL.

6.2 Les identités privées:

On affecte une identité privée pour chaque utilisateur. Cette identité joue le même rôle que l'IMSI en GSM, elle permet d'authentifier l'abonné et pour l'enregistrement. Elle prend le format d'un « Network Access Identifier » qui est la suivante :
« username@opérateur.com ». L'identité privée est stockée dans la carte à puce.

6.3 Relation entre identités publiques et privées :

Dans le cas GSM/UMTS, la carte à puce stocke l'identité privée et au moins une identité publique. Le HSS contient pour chaque utilisateur son identité privée et la collection d'identité publiques qui lui est attribué. Notons que dans le cas ou l'utilisateur utilise une carte GSM/UMTS qui ne contient pas ces informations, le terminal est capable de les construire à travers l'IMSI (Voire la procédure d'enregistrement par USIM). La relation entre l'utilisateur IMS et ces identités dans la Release 5 est montré par la figure suivante :

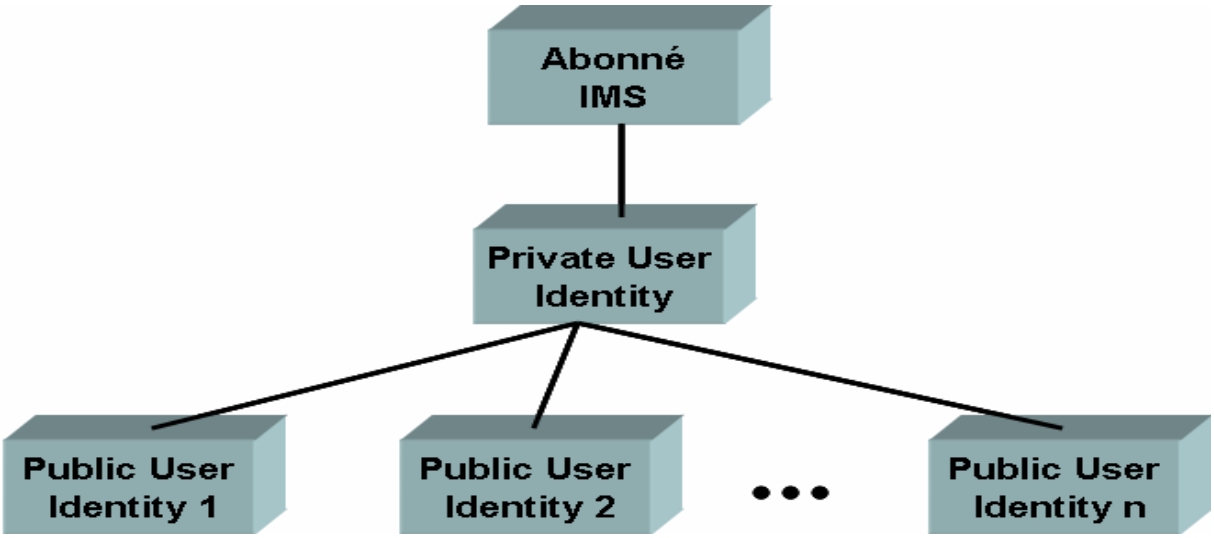

Figure 1.7 : Relation entre l'identité privée et publiques en IMS 3GPP R5.

Dans l'IMS 3GPP Release 6, un abonné peut avoir plusieurs identités privées. Dans le cas de l'UMTS seulement une identité privée peut être contenu dans la carte à puce mais l'utilisateur peu avoir plusieurs cartes contenant chacune une identité privée différente. Il est encore possible d'utiliser simultanément la même identité publique avec plusieurs identités privées (deux cartes insérées dans deux terminaux différents).

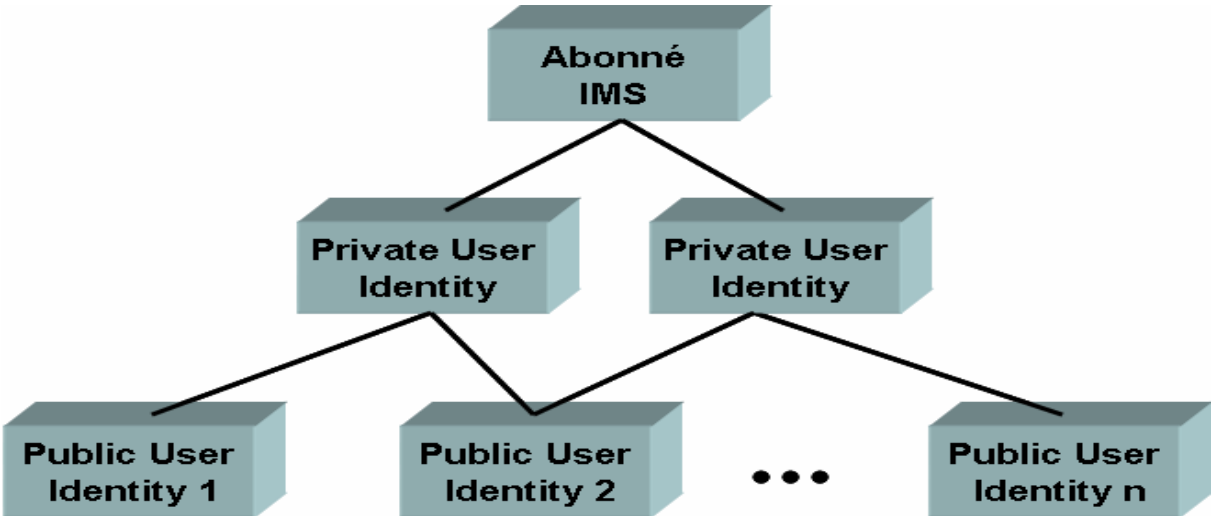

Figure 1.8: Relation entre l'identité privée et publiques en IMS 3GPP R6.

Chapitre 2

La plateforme Open Source IMS

1. Introduction

Open IMS Core est une implémentation des entités « Call Session Control Functions » CSCFs et de la base de données HSS « Home Subscriber Server », qui forment tous les deux la partie cœur de toute architecture IMS/NGN comme spécifié aujourd'hui par le consortium 3GPP et 3GPP2, ETSI TISPAN et PacketCable. Les quatre composant constituant le cœur de IMS sont Open Source (SER : SIP Express Router, MySQL). Ce projet, initié par l'institut de recherche allemand FOKUS a pour but de combler le vide qui existe de nos jours sur l'IMS dans le monde open source. L'idée est de permettre aux utilisateurs de développer des services IMS et de mettre en œuvre les concepts qui entourent l'IMS.

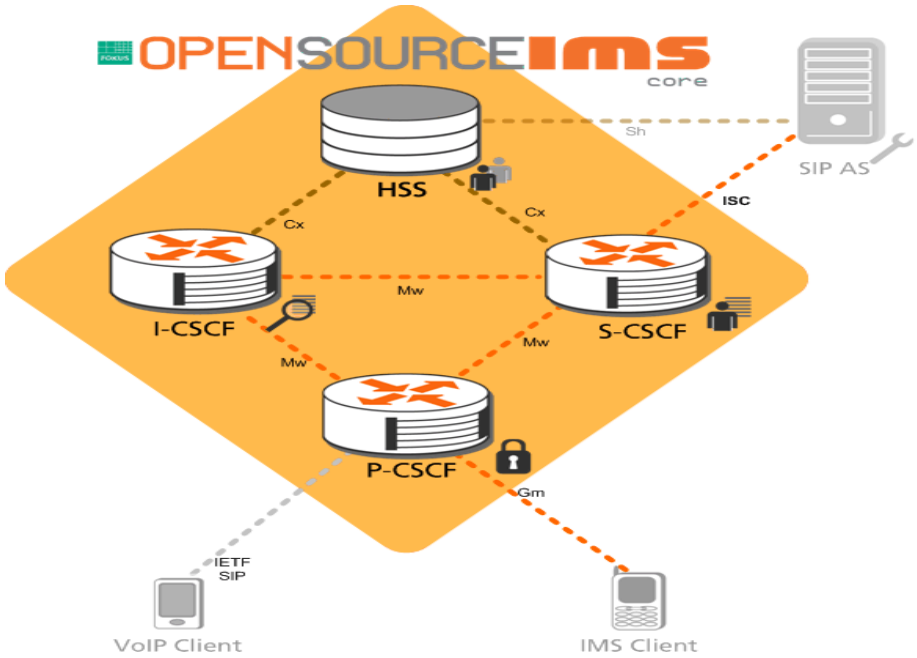

Figure 2.1 : Architecture de la plateforme OpenIMSCore

2. Installation de la plate-forme OpenIMSCore.

L'installation de cette plate-forme demande des requiert des composant matériels et logiciels. Cette phase d'installation passe par plusieurs d'étapes comme sera lister dans les paragraphes à venir.

2.1 Besoins matériels et logiciels.

- une machine Unix/Linux disposant de suffisamment de RAM et de CPU : dans notre cas il s'agit d'un OS Ubuntu 8.04

- Connexion Internet
- Environ 100Mb d'espace disque.
- GCC3/4, JDK1.5, ant.
- MySQL installation et activation.
- libxml2, libmysql - both with development
- Linux kernel 2.6 et ipsec-tools (setkey) si on veut utiliser IPSec security
- Optionnel: openssl pour la sécurité TLS security
- Bind installé et démarré.

Ce sont les module logiciels et matériels nécessaire pour l'installation et pour le bon fonctionnement de la plate-forme OpenIMSCore.

2.2 Comment obtenir le code source.

Le code source de cet outil IMS est disponible sur le site web suivant :

- ✓ *http://svn.berlios.de/svnroot/repos/openimscore* le code est configuré pour travailler avec les chemins suivant : /opt/openIMSCore.

a)

mkdir /opt/OpenIMSCore

cd /opt/OpenIMSCore

b)

mkdir ser_ims

svn checkout http://svn.berlios.de/svnroot/repos/openimscore/ser_ims/trunk ser_ims

c-)

mkdir FHoSS

svn checkout http://svn.berlios.de/svnroot/repos/openimscore/FHoSS/trunk FHoSS

2.1 Compilation du code.

On procède à la compilation du ser_ims dans un premier temps puis suivi de la compilation de FHoSS dans un second temps.

a- Dans le dossier : ser_ims

cd ser_ims

make install-libs all

cd ..

b- Dans le dossier FHoSS :

A cette étape un JDK1.5 est obligatoire, pour vérifier qu'on a une bonne version de JAVA on peut taper la commande suivante :

 # java -version

java version "1.5.0_07"

Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_07-b03)

Java HotSpot(TM) Client VM (build 1.5.0_07-b03, mixed mode)

Une fois qu'on dispose de ladite machine virtuelle java, la compilation est possible avec le code suivat :

cd FHoSS

ant compile

ant deploy

cd..

2.2 Configuration de l'environnement.

La plate-forme est configurer pour travailler en localhost (127.0.0.1) et le nom de domaine est par défaut « open-ims.test ». Pour travailler avec son adresse IP il suffit de remplacer dans les fichiers de configuration l'adresse de loopback 127.0.0.1 par @IP de la machine en question de même pour les mots de passe de la base de données. Le fichier ser_ims/cfg/configurator.sh sert à cette affaire.

- DNS

La configuration de DNS revient à toucher à certains fichiers tels que named.conf, hosts.conf, resolv.conf. Un fichier de configuration est disponible sur ser_ims/cfg/open-ims.dnszone. Une fois la configuration est faite, le redémarrage de DNS se fait par la commande /etc/init.d/named restart. Des pings sur les différentes entités de l'IMS permettent de tester le bon fonctionnement de DNS : *dig @127.0.0.1 pcscf.open-ims.test* ou ping HSS ou CSCF apres avoir donné des alias dans le fichier hosts.conf.

- MySQL

Avant de commencer il faut démarrer le MySQL, afin de pouvoir créer les bases de données nécessaires pour le fonctionnement de l'OpenIMSCore.

mysql -u root -p -h localhost < ser_ims/cfg/icscf.sql

mysql -u root -p -h localhost < FHoSS/scripts/hss_db.sql

mysql -u root -p -h localhost < FHoSS/scripts/userdata.sql

2.3 Configuration de IMS Core

- CSCF

Il s'agit de copier des fichiers de configuration suivant vers le répertoire racine de l'IMS core /opt/OpenIMSCore :

cp ser_ims/cfg/.cfg .*

cp ser_ims/cfg/.xml .*

cp ser_ims/cfg/.sh .*

- FHoSS

Les fichiers de configuration sont disponible après l'étape 3 dans FHoSS/deploy/. Ces fichiers peuvent être édités selon les préférences voulues.

2.4 Lancement des composants.

- le démarrage de CSCF se fait en lançant en parallèle les scripts pcscf.sh, icscf.sh et scscf.sh.
- quant à celui de FHoSS, il demande d'exécuter le script *FHoSS/deploy/startup.sh*. A ce moment une interface graphique sera disponible en localhost *http://localhost:8080/*.

3 Interaction avec le cœur IMS.

Apres avoir résolu les problèmes relatifs à l'installation de la plate-forme Open IMS, nous avons pu grâce à une interface FHoSS sur le localhost *http://localhost:8080/* faire la recherche des utilisateurs enregistrés sur la base de donnée de la plate-forme Open IMS. Deux utilisateurs sont par défaut créés durant l'installation du cœur IMS il s'agit de ***alice*** et ***bob*** dont les SIP-URL sont respectivement :

sip:alice@open-ims.test et *sip:bob@open-ims.test*.

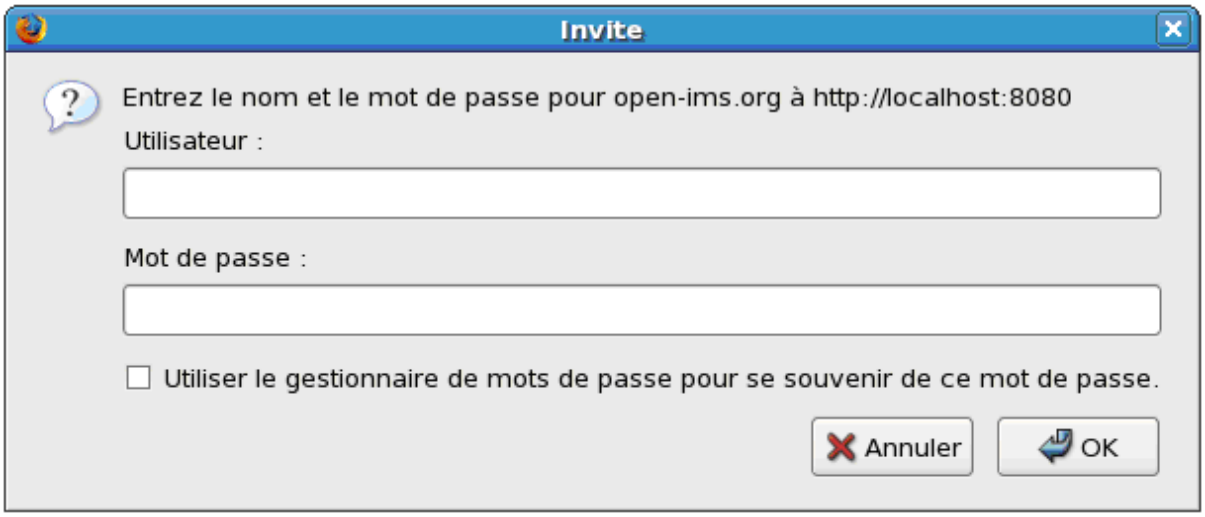

Figure 2.2 : Accès aux comptes.

Il existe deux manières pour accéder aux informations sur les usagers ainsi que sur les services. Ceci est fonction du compte avec lequel on a fait l'accès à l'interface FHoSS:

- Compte client (hss) : il donne la main aux usagers à une recherche des autres utilisateurs. Mais le droit de faire des modifications, suppression ou ajout d'un utilisateur n'est pas permis.
- Compte administrateur (hssAdmin) : Il s'agit d'un compte administrateur qui offre plus de droit qu'un compte client. Il est dans ce cas possible de modifier, d'ajouter et de supprimer les utilisateurs et les services.

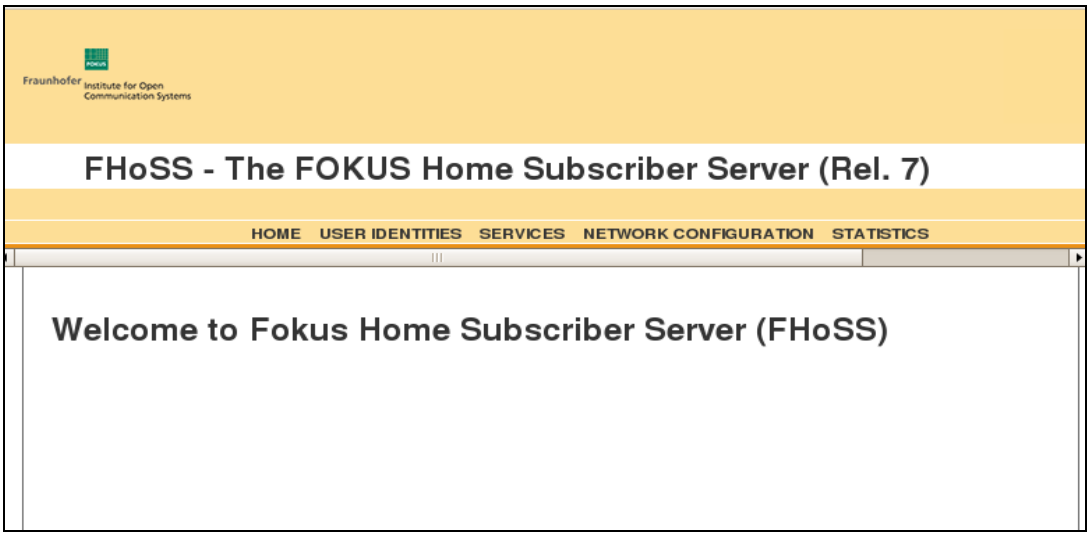

Figure 2.3 : Interface du compte administrateur.

Sur l'outil graphique, existe différents liens permettant de choisir entre plusieurs options dont chacune spécifie des traitements bien déterminés à des paramètres bien déterminés.

- ***User identities :*** un lien vers les informations d'enregistrement des user.

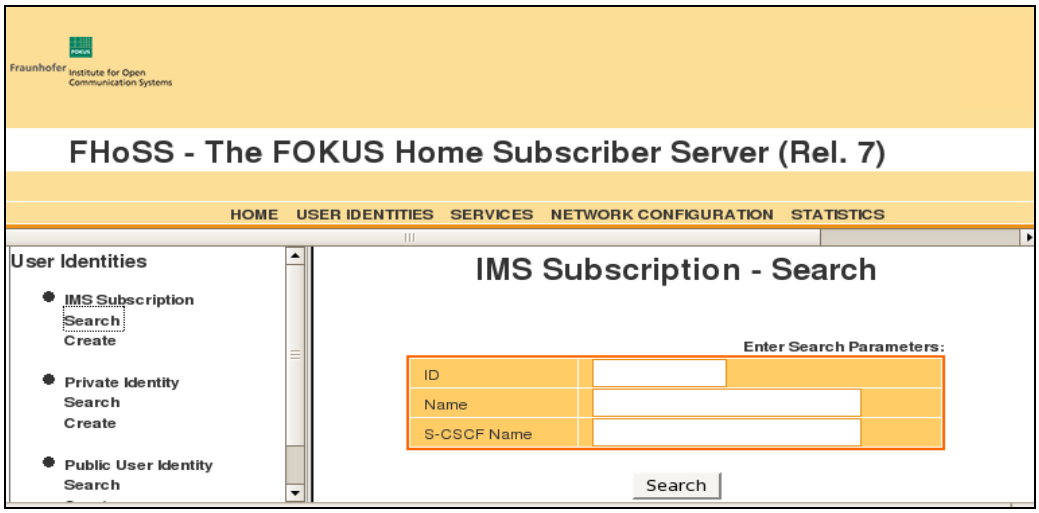

Figure 2.4: Recherche des users.

On retrouve les deux utilisateurs déjà enregistrés sur l'Open IMS. Il s'agit de ***alice*** et ***bob.*** On peut enregistrer d'autres utilisateurs.

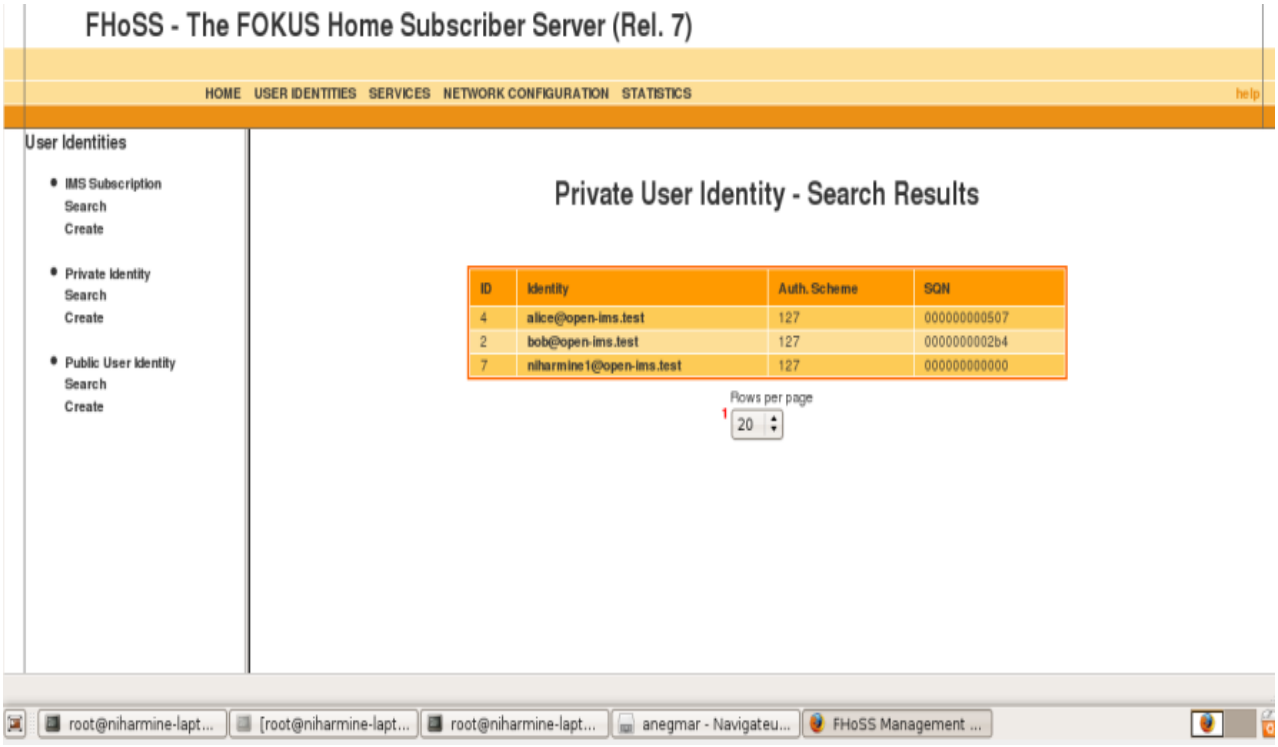

Figure 2.5 : Identités des utilisateurs

Avec ce compte administrateur on peut rechercher les utilisateurs déjà inscrits grâce au lien Search. L'ajout se fait grâce à Create.

- Quant à la partie services, il s'agit de services offerts aux utilisateurs : par défaut c'est le service présence. Il est également possible de créer d'autres services.

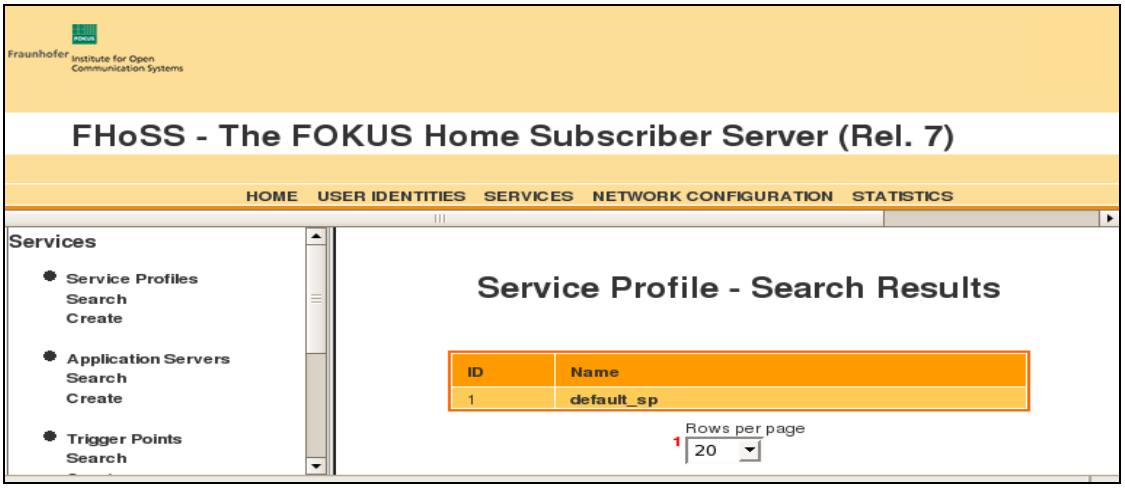

Figure 2.6 : Profile des services.

4. Installation du client IMS

Uctimsclient est un client IMS développé pour fonctionner avec l'Open IMS. Nous avons installé la version v1.0. 12 de ce client IMS :

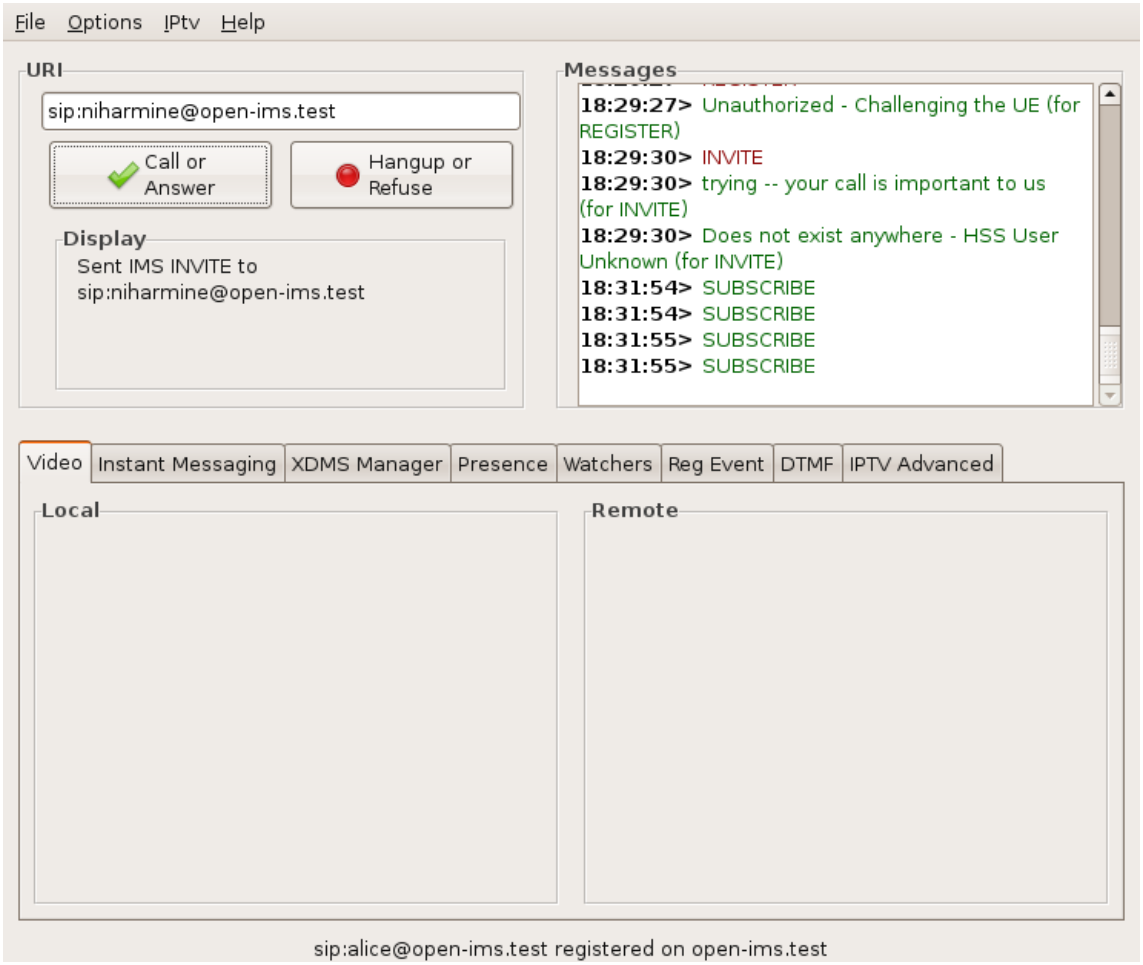

Figure 2.7 : UCT IMS Client.

Sur le menu option, il y'a la possibilité d'enregistrer un utilisateur pour qu'il puisse être reconnu par le system IMS

Chapitre 3

Le service de présence dans l'IMS

1. Introduction :

La présence et la messagerie instantanée changent le paradigme de communications d'entreprise et l'annonce personnelle. La présence augmentera la messagerie aussi bien que présentera un nouveau service (le service de présence lui même) qui peut être utilisé dans beaucoup d'autres applications et services. La présence sera le cœur de toutes les communications et la nouvelle voie pour la téléphonie pour fonctionner. La présence sera aussi une occasion lucrative d'affaires tant pour des opérateurs que pour des prestataires de services. La présence est un profil dynamique de l'utilisateur, qui est visible à d'autres et a eu l'habitude de se représenter, partager des informations et contrôler des services. On peut voir la présence comme le statut d'un utilisateur aussi perçu par d'autres et le statut d'autres que perçu par l'utilisateur. Le statut peut contenir des informations comme l'annonce personnelle et le statut de dispositif, l'emplacement ou le contexte, des capacités terminales, la méthode de contact préférée aussi bien que des services l'utilisateur est enclin à utiliser pour communiquer avec d'autres, y compris la voix, la vidéo, la messagerie instantanée aussi bien que le jeu.

Les informations de présence sont aussi personnelles. Il est toujours lié avec une personne particulière. Il montre la personne introduisant la communication si l'autre personne est disponible et disposée pour communiquer. D'autre part, les informations de présence peuvent être utilisées pour communiquer à d'autres quand une personne est capable et disposée de communiquer aussi bien qu'avec qui et par quels moyens. Cela permettra aux utilisateurs de contrôler leur communication propre plus efficacement.

Le partage d'information de présence soulève de sécurité et de protection de la vie privée. En utilisant le Protocole SIP (Session Initiation Protocol) pour la présence, les utilisateurs peuvent contrôler leurs informations de présence spécifiques propres et avoir le dernier mot comment il est utilisé incluant qui peut et ne pouvoir pas voir de certaines parties, si pas tout, des informations de présence.

1.1 Utilisateurs de service de présence :

Il y aura beaucoup de groupes d'utilisateurs différents, qui utiliseront des informations de présence pour des buts différents. Ces groupes s'étendront d'utilisateurs d'affaires d'entreprise aux adolescents et des enfants. Tandis que la présence va probablement être utilisée plus pour la gestion de disponibilité raisonnable dans l'utilisation d'entreprise, de jeunes consommateurs cherchent constamment les nouvelles façons d'expression eux-mêmes et la construction d'une identité dans une manière visuellement riche. Des services de présence fructueux seront adaptables aux différents besoins de divers groupes d'utilisateur et segments.

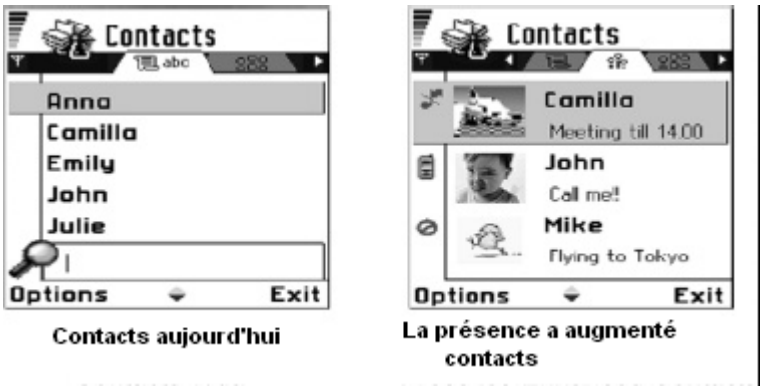

Figure 3.1. : Présence dynamique

1.2 Services Augmentés de présence

La présence peut contribuer aux affaires existantes et créer une activité de son propre. Il y aura des services d'utilisateur de présence de base aussi bien que des nouveaux services permis de présence. Les opérateurs et d'autres prestataires de services ont un rôle majeur dans l'adoption massive de services de présence. Le service de présence mobile de base peut faire partie du portefeuille de service de l'opérateur, puisque d'autres services - c'est-à-dire, les nouveaux services de présence - peuvent utiliser le service de base. Le domaine mobile, étendant maintenant presque un milliard d'abonnés dans le monde entier, est une plate-forme rentable pour des nouveaux services grand public.

L'offre d'un service de présence de base peut donner un avantage compétitif pour un opérateur sur d'autres opérateurs qui ne l'offrent pas en liant leurs informations de présence aux services d'un opérateur particulier, les clients ont des services de valeur haute que d'autres opérateurs ne peuvent pas être capables d'offrir sans cela aux informations. La présence produit le nouveau trafic pour des services existants comme la messagerie instantanée. La présence réduit aussi au minimum des appels incomplets ou des appels étant rejeté due à la partie appelée étant occupé.

Les opérateurs doivent aussi soigneusement considérer à la tarification de présence permettant le peuple de prendre une décision facile de l'adoption du service de présence, sans devoir pour penser pour trop longtemps du coût/bénéfice.

2. C'est quoi La présence? :

La présence est essentiellement deux choses : il implique la fabrication de mon statut disponible à d'autres et les statuts d'entre d'autres disponibles à moi. Les informations de présence peuvent inclure :

- Personne et disponibilité de terminal
- Preferences de communication
- Capacités de terminal
- Activité actuelle
- Emplacement et services actuellement disponibles.

La présence facilitera toute la communication mobile, non seulement la messagerie instantanée, qui a été le conducteur principal pour la présence. La messagerie instantanée a été le service de communication interactif, presque en temps réel principal dans l'Internet et par la présence vous pouvez savoir aussi si un ami est en ligne avant que vous ne commenciez la session achat avec lui. Cependant, dans l'environnement mobile, il est prévu que les informations de présence soutiendront non seulement la messagerie instantanée, elle (la présence) sera aussi utilisé comme un indicateur de la capacité de s'engager à n'importe quelle session, y compris des appels de voix, la vidéo et les jeux : toutes les communications mobiles seront à base de présence.

Des applications spécifiques de présence des services seront disponibles dans un proche avenir. Un exemple typique d'une application spécifique de présence sera un annuaire téléphonique avec des informations de présence incorporées, le faisant dynamique.

La présence dynamique sera les informations initiales. L'utilisateur voit avant l'établissement de la communication. Ces informations affectent le choix de méthode de communication et le chronométrage(le choix du temps).

2.1 SIP pour présence:

Le Protocole *SIP* a été étendu pour la présence par la création d'un paquet d'événement appelé "presence". En signant à un tel événement, un abonné place le signe "presence" en cas l'en-tête.

Quelques définitions ont été conçues pour décrire l'abonné et le notifier pour le but de présence :

- **Presentity** - l'entité de présence, une ressource qui fournit des informations de présence à un service de présence.

- **Observateur** - l'entité qui demande des informations de ressources.

Deux entités SIP sont définies pour la présence dans [RFC3856] :

- L'agent de Présence (PA) - capable de stocker des abonnements et produire des notifications.

- L'agent d'Utilisateur de Présence (PUA) - manipule des informations de présence pour un presentity et publie de telles informations de présence.

Comme mentionné plus tôt, le NOTIFY porte le corps comportant les informations d'état. Dans ce cas, les informations d'état sont l'état de présence d'un presentity. L'extension de Courrier d'Internet Polyvalente (MIME) le type d'un tel contenu est "application/pidf þ Xml" comme défini dans [RFC3863].

2.2 Architecture de service de présence dans IMS :

Les informations de présence d'un utilisateur peuvent être obtenues d'une multiplicité d'entités dans le Sous-système de Multimédia de Protocole d'Internet (IMS) : cela pourrait être un PUA situé dans un réseau étranger, un PUA au terminal ou un PUA situé comme une entité dans le réseau. Le serveur de présence est un exemple d'un serveur IMS d'application. Les observateurs peuvent être dans le même domaine domestique que le presentity ou dans un domaine étranger.

La figure suivante représente une architecture de référence pour supporter un service de présence dans l'IMS.

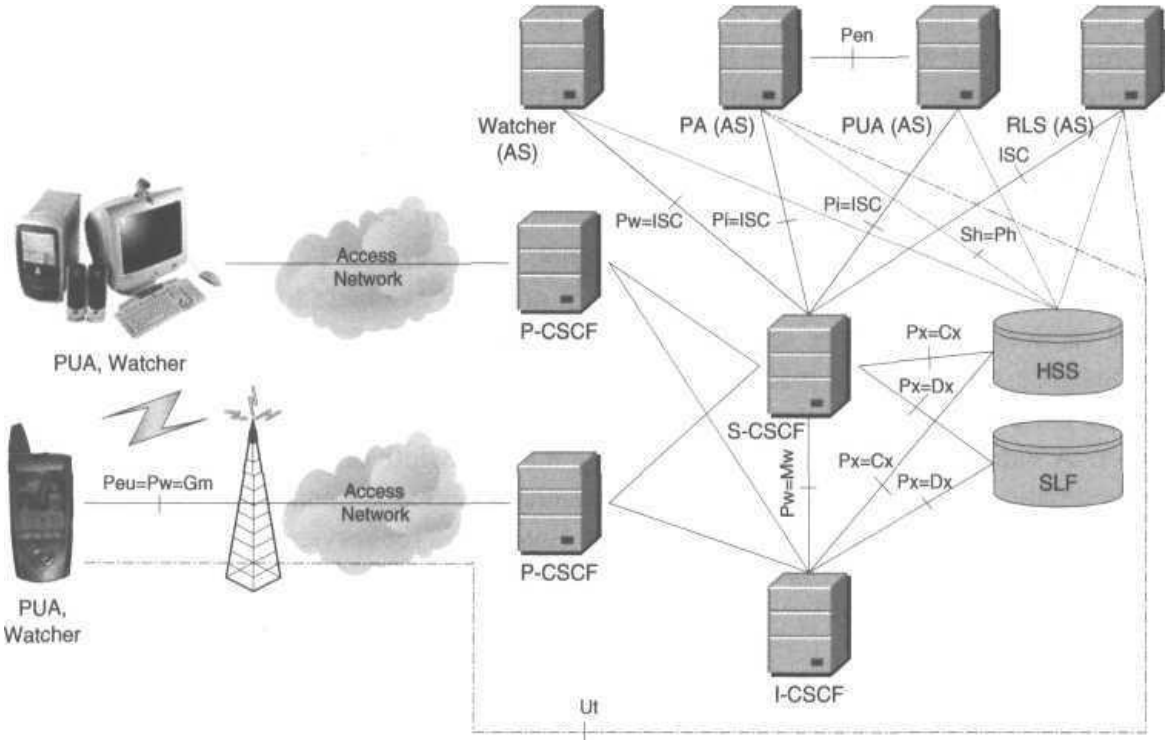

Figure 3.2 : Architecture de référence supportant le service de présence en IMS

Les entités sont définies comme suit :

- Presence Server (PS): gère des informations de présence téléchargées par PUA et traite des demandes d'abonnement de présence

- Watcher presence proxy : Identifie le réseau cible.
- Presentity presence proxy : identifie le serveur de présence assigné à certains presentity.

- PUAs : assemble et fourni les informations de présence au serveur.

2.3 La liste Presentity :

Il est prévu que les utilisateurs auront plusieurs presentities (amis) dont leurs informations de présence les intéressent. Pour le contrôle de la congestion et les limitations de la largeur de la bande il est déconseillé économiquement d'avoir un terminal d'utilisateur qui envoie une multiplicité des demandes de SUBSCRIBE, un pour chaque presentity.
Pour résoudre ce problème Group Management Solutions était crée. La liste de presentity est un type de ressource liste :

- Application Usage ID (AUID) – ‘‘resource-lists’’.
- Contraintes additionnelles-none
- Naming-Convention-none
- Interdépendances de ressource - la liste est représentée par un Identificateur de Ressource Universel (URI). Si le client ne peuple pas l'élément XML portant la valeur d'URI, le Protocole d'Accès de Configuration XML (XCAP) le serveur doit faire ainsi.
- Autorisation des polices.

L'interface Ut dans l'architecture de l'IMS est utilisée pour manipuler les listes des ressources.

2.4 Autorisation des présences :

Les informations de présence peuvent être disponibles aux niveaux différents portées aux observateurs différents. Cela signifie que des observateurs différents peuvent être autorisés à voir les parties différentes des informations de présence d'un presentity. Le choix de ce qui voit ce qui appartient au presentity. Le presentity peut mettre de tels niveaux d'autorisation utilisant une solution XCAP-defined en forme de déclarations de permission.
[Draft-ietf-geopriv-common-policy], [Draft-ietf-simple-presence-rules], [Draft-ietfsimple-common-policy-caps] et [Draft-ietf-simple-pres-policy-caps] Définis le schéma XML avec sa sémantique aussi bien que ces sections qui sont défini pour l'utilisation XCAP.

a. Publication de présence :

Les informations de publication de présence peuvent être achevées en utilisant l'extension de protocole SIP. L'en-tête d'événement d'une demande de PUBLISH porte le signe "presence". Le temps d'expiration par défaut d'une publication est 3,600 secondes. Le corps d'une demande PUBLISH portant des informations de présence a de type de MIME "application/pidf+Xml".

- ***Le paquet modèle des informations d'événement de l'observateur :***

Les utilisateurs souscrivent pour recevoir des informations sur l'état d'une ressource particulière utilisant un paquet d'événement. Ces abonnés peuvent être mentionnés comme "des observateurs". Un paquet de modèle d'informations d'observateur permet à un utilisateur de gagner la connaissance d'observateurs et l'état de leurs abonnements au paquet principal. Un paquet de modèle d'informations d'observateur est identifié avec le signe "winfo".

L'utilisation primaire de ce paquet de modèle est pour la présence. Les utilisateurs souscrivent à ce paquet de modèle pour voir qui souscrit à leurs informations de présence et l'état de cet abonnement.

Les informations portées à l'abonné d'informations d'observateur contiennent deux articles importants : le statut de chaque abonnement fait par les observateurs du paquet principal et l'événement qui a causé la transition du statut précédent au actuel.

Les états du paquet d'informations d'observateur sont décrits dans [RFC3857] comme suit :

- Init : Aucun état n'est alloué (réparti) pour un abonnement.
- Termined : Une police existe qui interdit à un observateur de souscrire au paquet d'événement principal
- Active : Une police existe qui autorise un observateur souscrire au paquet principal.
- Pending : aucune police n'existe pour cet utilisateur.
- Waiting : Semblable à en suspens, mais dit à l'abonné de paquet de modèle qu'un utilisateur a essayé de souscrire au paquet principal et que l'abonnement a expiré avant qu'une police n'ait été créée.

b. Flux des services de présence :

- ***Abonnement réussi au service de présence :***

La figure suivante montre un flux d'exemple d'un observateur qui a avec succès signé aux informations de présence d'un presentity la résidence dans un réseau différent tandis que l'observateur réside dans son réseau domestique. Le flux montre un initial NOTIFY à la demande de SUSCRIBE.

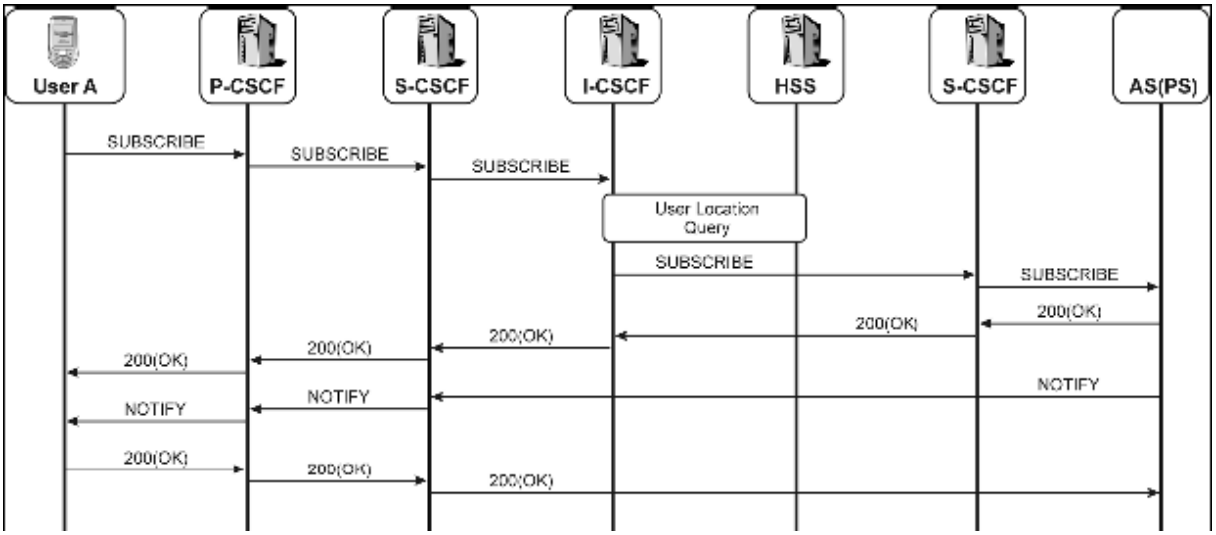

Figure 3.3 : Abonnement réussi au service de présence

- ***Publication réussite des informations de présence :***

La figure montre un flux d'exemple d'un presentity qui a avec succès publié des informations de présence. Dans ce scénario l'Équipement Usager (UE) se comporte comme un PUA. Cela aboutit typiquement le Commuté de paquet (PS) au domaine produisant des notifications aux observateurs.

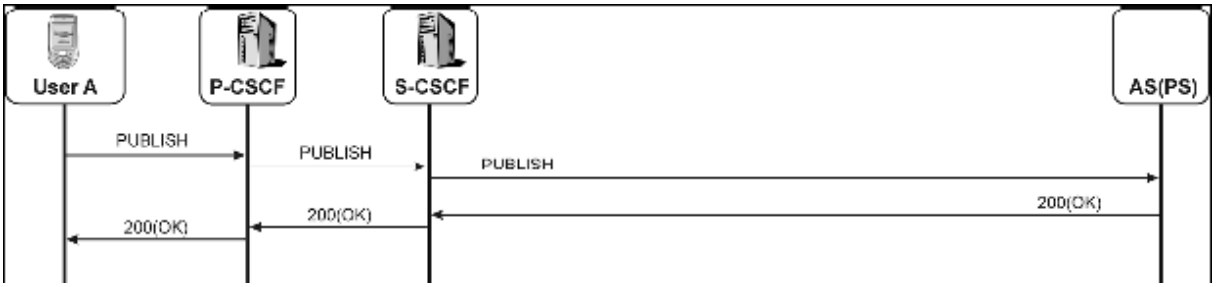

Figure 3.4 : Publication réussi

- ***Abonnement à une liste de ressource :***

La figure montre un flux d'exemple d'un observateur qui souscrit aux informations de présence d'une liste de ressource qui a été crée plus tôt (utilisant probablement XCAP). La liste des ressources est faite référence en utilisant une SIP. Le flux montre l'immédiat NOTIFY la demande qui est envoyée après la réception de la demande SUBSCRIBE. Si le Serveur de Liste de Ressource (RLS) ne tient pas d'informations de présence sur les ressources dans la liste, donc la demande NOTIFY peut porter un corps vide.

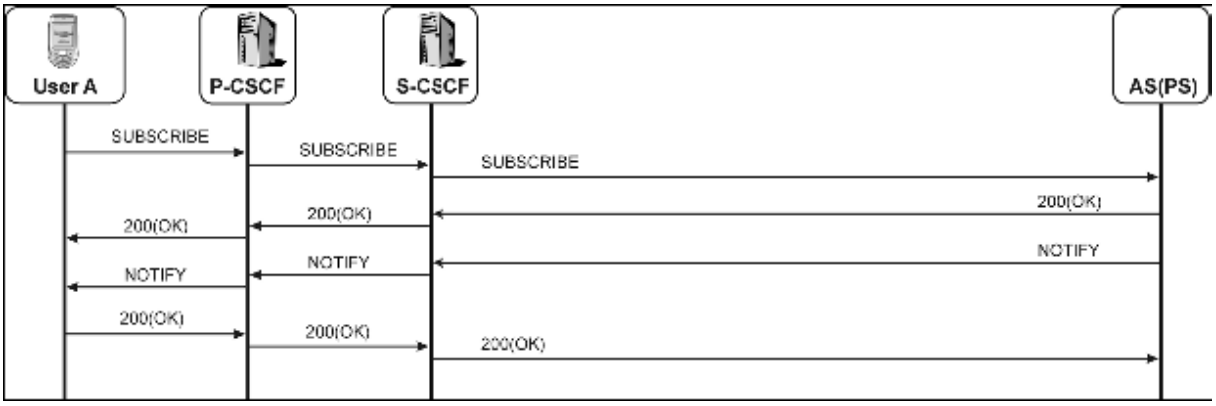

Figure 3.5 : Abonnement à une liste de ressource

- ***Abonnement aux informations d'observateur :***

La figure décrit comment le message coule en réalité entre le PUA et le domaine PS quand un utilisateur souscrit pour recevoir des notifications des changements d'état des observateurs. Le chemin des messages est le même comme celui de la demande PUBLISH.

Le flux montre la notification immédiate après une demande réussie d'abonnement. La figure récapitule les interactions entre le serveur de présence, l'observateur et presentity.

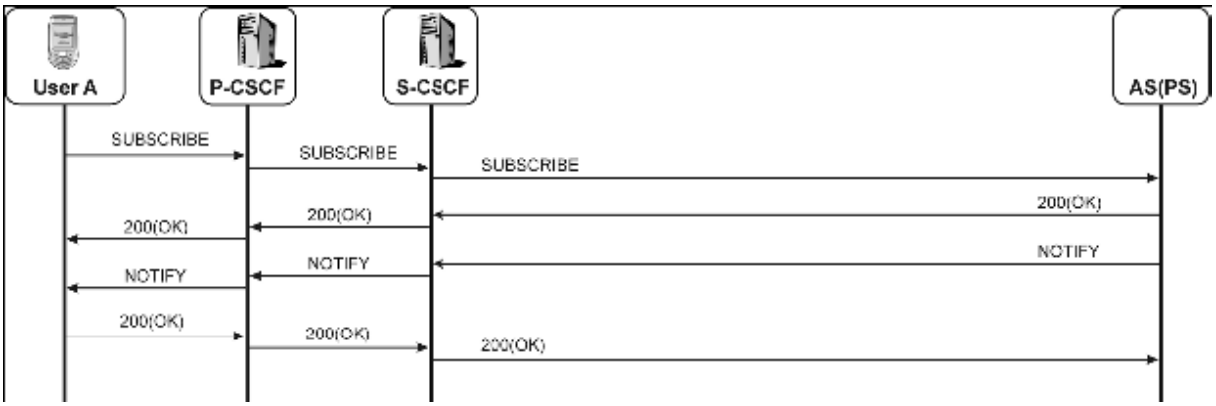

Figure 3.6 : Abonnement aux informations d'observateur.

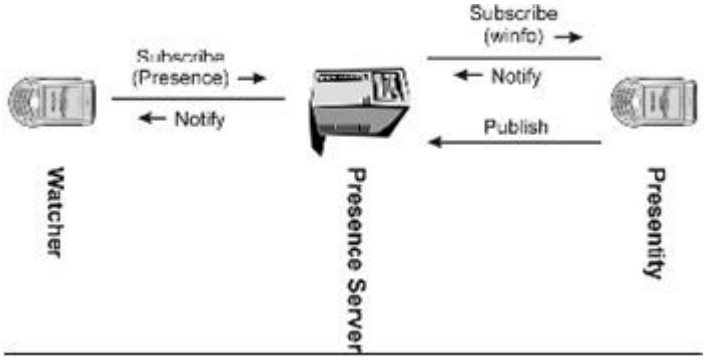

Figure 3.7 : Interaction entre serveur de présence, observateur et presentity

Conclusion

Dans ce projet, on a analysé deux aspects fondamentaux de cette nouvelle technologie qui tend à remplacer l'infrastructure de contrôle dans les réseaux mobile. L'apport principal de l'IMS est le faite de pouvoir établir des sessions multimédia avec la fourniture de nouveaux services comme le service de présence qui permet à l'operateur de donner plus de qualité a son service et de fidéliser ses clients, la messagerie instantanée jusqu'aux jeux vidéo…Mais pour faire des services très riche il faut que les réseaux d'accès IP assurent un débit élevé par utilisateur et une bonne réactivité. Actuellement les réseaux mobiles de troisième génération, telle que l'UMTS, ne fournissent pas un débit très élevé par utilisateur, donc pour vraiment faire des services multimédia d'une haute qualité il faut attendre l'émergence d'une nouvelle technologie radio. En plus le réseau IP de transport qui pourra être l'Internet doit fournir une qualité de service minimum pour véhiculer le trafic IMS. Là, on voit plusieurs problématiques qui apparaissent au niveau accès transport et même au niveau de la gestion de la mobilité de l'utilisateur quand il change de technologie d'accès.

Et Face au déclin des services existants et à l'augmentation de la concurrence, les opérateurs de réseau doivent actuellement relever un défi sans précédent. Comment augmenter le revenu moyen par client, réduire les taux de désabonnement et fournir une expérience de service convergente à l'utilisateur final ? La réduction des coûts, l'innovation en termes de services et le respect de l'environnement sont les nouvelles stratégies clés des opérateurs de réseau.

Références

- www.openimscore.com
- www.uctimsclient.com
- **The IMS ,Ip Multimedia Subsystem: Concepts and Services**, Miikka Poikselka : Nokia, Finland
- CAMARA El Hadj Mory Ismael , PFE 2008 INPT: **Développement de services conversationnels pour la VoIP sur un serveur d'application SIP open source dans une architecture IMS,** France Télécom

Annexe
Configuration de Serveur de présence OpenSER (OpenSIPS)

I- OpenSER (OpenSIPS) :

1- Qu'est ce que OpenSIPS:

OpenSIPS (Open SIP Server) est une mise en oeuvre Source Ouverte mûre d'un serveur SIP. OpenSIPS est plus qu'un mandataire/routeur de SIP comme il inclut des fonctionnalités de niveau d'application. OpenSIPS, comme un serveur de SIP, est le composant principal de n'importe quelle solution VoIP à base SIP. Avec un moteur de cheminement très flexible et adaptable, OpenSIPS unifie la voix, la vidéo, IM et des services de présence d'une façon fortement efficace, des remerciements à sa conception évolutive.

Dans quoi OpenSIPS doit offrir, entre une fiable et très performante OpenSIPS est un des serveurs de SIP les plus rapides, avec une sortie qui le confirme comme une solution jusqu'à la classe de catégorie de transporteur

2- Vision OpenSIPS :

OpenSIPS est une suite du projet d'OpenSER. L'héritage de l'esprit OpenSER de franchise à la communauté et la volonté de progrès ; un travail continu pour se développer, pour augmenter et prolonger le code, OpenSIPS continue et prolonge la vision OpenSER par un processus fort de consolidation.

3- Quand/où utiliser OpenSIPS

OpenSIPS peut être utilisé comme :

- Fournisseur de services VoIP
- SIP raccordemant au réseau
- SIP load-balancing
- SIP front-end
- SIP NAT traversal unit
- SIP application serveur
- Services aux entreprises
- SIP router

4- Caractéristiques principales :

- Serveur SIP d'enregistrement
- Redirection serveur SIP
- SIP présence agent
- SIP serveur de messagerie instantanée
- SIP à la passerelle SMS (bidirectionnel)

- SIP à XMPP passerelle de la présence et de messagerie instantanée (bidirectionnel)
- SIP répartiteur de charge ou de l'expéditeur
- SIP avant de passerelles / astérisque
- SIP NAT traversal unité
- Serveur d'applications SIP

II- Comment installer un serveur de présence dans votre réseau IMS :

1- installer OpenSIPS :

Le serveur OpenSER de présence est très rapide et facile à installer. Télécharger OpenSER et MySQL.

Puisque on utilise Ubuntu une distribution à base vous pouvez simplement utiliser dpkg-i sur la deb. On aura besoin du serveur MySQL et du client, et la libmysqlclient-dev libxml et les bibliothèques. Une fois OpenSER et la présence des modules sont installés, vous devez exécuter le script:

```
openser_mysql create
```

Ce script permet de configurer la base mySQL de la présence du serveur.

2- Configurer OpenSIPS (OpenSER) :

Modifier le fichier **/ etc / openser.cfg** présence à l'appui. N'oubliez pas de redémarrer OpenSER.

3- Configurer le FHoSS de l'interface Web :

Définissez votre IMPUs (identités public) à utiliser par défaut le profil de service (default_sp). Ce profil avant de publier et de tous les ABONNEZ messages au serveur d'applications par défaut (localhost: 8080).

4- Démarrage du Client :

UCT démarrage, le client et le SGI dans les préférences son tour sur la présence. Cela Inscrivez-vous à tous vos contacts dès que vous Inscrivez-vous à l'IMS de base. Il va également publier votre statut qui est fixé par défaut à **Available.**

En présence onglet ajouter l'URI de statut que vous souhaitez regarder. Ajouter vos propres URI si vous souhaitez surveiller votre propre statut.

Le serveur de présence devrait vous informer à chaque fois de votre statut.