UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

Année : **2020** N° d'ordre : **151**

THESE DE DOCTORAT UNIQUE

Présentée pour obtenir le grade de Docteur de l'Université Cheikh Anta DIOP de Dakar

Mention : Informatique et Télécommunications

Spécialité : Télécommunications

Par :

Ngartabé KAG-TEUBE

Titre : **ETUDE DE LA FIABILITE DES SYSTEMES CONVERGENTS DE TELECOMMUNICATION ET LEURS APPLICATIONS**

Soutenue le 20 juillet 2020 devant le jury composé de :

Président	Hamidou	DATHE	Professeur Titulaire	UCAD, Sénégal
Rapporteurs	Cheikh	SARR	Professeur Titulaire	Université Thiès, Sénégal
	Michel	BABRI	Professeur Titulaire	INPHB, Côte d'Ivoire
Examinateurs	Abdourahmane	RAIMY	Maître de Conférences (CAMES)	UCAD, Sénégal
	Gervais	MENDY	Maître de Conférences (CAMES)	UCAD, Sénégal
Directeur de Thèse	Samuel	OUYA	Maître de Conférences (CAMES)	UCAD, Sénégal

Dedicaces

Je dedie cet humble travail :

A Dieu soit la Gloire,

A tous ceux qui me sont les plus chers : mon père Joseph MAYO Ngartabé, ma mère Marie MOBANE Djembonbé, mes sœurs : Josephine DANDE, Béatrice DENNEBEYE, Grâce DEBBO et mes frères : Joél DAREM, Josué DAHINBE, Désiré MAOUG-NDOU.

A mon épouse NOUDJIKWAMBAYE Naomie et mes enfants MAMADJIBEYE Mbaidjé Eveline, MADJIDENE KAG-TEUBE Marina, NENODJI KAG-TEUBE Marielle, Roland MBAIDIGUIM, Romaniel NGUEMNODJI et MBAIGUEDOUMMADJI Justin.

A tous mes parents : François DAGOTO TEUBE, Alexis NGARMADJIBE TEUBE, Keinome TEUBE, Sianleyo TEUBE, René NAINBANE, Michel OUSMANE, Simon KOULADJE.

A tous mes grands parents et parents de NDOU et BELADJA au Tchad.

A tous mes compatriotes : Yena RASSEMNGAR, Jorim Ngonnbé NGANAN, Zenias DJEKO MEUGRE, Dabé YOSSANGUEM, Dillah DOUMAYE, Pr. Bhen TOGUEBAYE, Jude DJINDIL, Rebnodji MIARO, Kaltouma BOURKOU, Djerang KOBE.

A tous ceux qui oeuvrent inlassablement pour le developpement de l''Afrique.

Remerciements

Après avoir enduré sur ce parcours académique universitaire, je mřétais armé de patience et de courage avec abnégation pour atteindre lřobjectif que je mřétais fixé dans le cadre de mes études. Venu le moment où je présente ce travail, il convient de rendre hommage à tous ceux et celles qui mřont apporté un soutien de loin ou de près à lřaccomplissement de cette thèse.

Ma profonde gratitude :

- ✓ A Monsieur **Mohamed MOUSSA**, Directeur Général de lřASECNA ;
- ✓ Aux Directeurs, chefs de Départements, chefs de Services de lřASECNA ;
- ✓ A lřensemble des collaborateurs de lřASECNA.

Je salue les efforts de lřAgence dans sa politique de formation de longue durée et le souici dřavoir un personnel de qualité. Et ce cadre me donne lřopportunité de réaliser mon rêve aujourdřhui. Quřils soient remerciés de leur confiance.

Je remercie le Professeur **Pape Alioune NDIAYE**, Directeur de lřEcole Supérieure Polytechnique (ESP) de lřUCAD, de mřavoir accepté dans son établissement de référence.

Aux membres du jury qui mřont accordé lřhonneur par leur présence afin dřévaluer ce travail :

Toute ma reconnaissance au **Professeur DATHE**, Directeur de lřEcole Doctorale Mathématiques et Informatiques (EDMI), **Président du jury** de cette soutenance de thèse pour lřaccompagnement quřil a manifesté depuis notre première année jusquřaujourdřhui. Le travail administratif quřil a mené à lřécole doctorale pour que les soutenances de thèse se tiennent dans de bonnes conditions. Il appuie fortement lřécole doctorale et le laboratoire LIRT car en ce début dřannée 2020, LIRT a déjà enregistré trois docteurs, cřest très encourageant. Je vous en remercie infiniment.

Toute ma reconnaissance aux deux rapporteurs ; le professeur **Michel BABRI** de lřINPHB en Côte dřIvoire et le professeur **Cheikh SARR** de lřuniversité de Thiès au Sénégal qui ont consacré leur temps à faire des analyses pertinentes, à apporter des critiques constructives et à faire de propositions à lřamélioration de la version finale de la thèse, je vous en remercie infiniment.

Toute ma reconnaissance aux deux examinateurs ; le professeur **Abdourahmane RAIMY** et le professeur **Gervais MENDY** qui ont pris leur temps de lire la thèse et aussi être membre du jury pour lřexaminer, je vous en remercie infiniment.

Mes pensées vont vers mes défunts parents qui mřont élevé dans la dignité et inculqué lřamour du travail bien fait. Merci mon Père, Merci ma Mère.

Au terme de ce travail, je tiens à remercier le Professeur **Samuel OUYA**, mon Directeur de thèse, pour avoir accepté dřen assurer la direction. Lřexpression de ma profonde gratitude et reconnaissance au Professeur **Samuel OUYA**, Directeur du Laboratoire Informatique, Réseaux et Télécommunications (LIRT) de lřESP. Il nřa ménagé aucun effort pour la réalisation de cette thèse à travers son implication, son soutien, ses encouragements, ses conseils précieux et orientations.

Mes remerciements vont à lřendroit de **Yvan Paillard KALIA-SYA DODOAGNEN** et **Kéba GUEYE** qui ont contribué dans la simulation de ce travail.

Je remercie tous les Docteurs et Doctorants du LIRT pour mřavoir accueilli et aidé à différents niveaux de la recherche.

Je garde une place toute particulière pour toute ma famille. Je la remercie pour son soutien de tous les instants.

Mes remerciements vont à ma chère épouse **Naomie KAG-TEUBE**. Comment pourrais-je suffisamment la remercier pour son amour sans limites, pour sa grande confiance, pour son constant encouragement, pour ses précieux conseils, pour ses remarques pertinentes, pour sa patience.

Mes remerciements du fond du coeur à ma fille **Marielle NENODJI KAG-TEUBE**, qui mřa encouragé tout au long de ce travail de recherche, en ayant la patience dřattendre la fin des longs mois de rédaction pour en partager le succès.

Enfin, que les TIC, objets de cette recherche, soient aussi remerciées. Sans leurs usages, ce travail nřaurait pu aboutir. En ligne, elles ont été indispensables à ma recherche dřinformations. Une mine à portée de clic ! De quoi rêver à un futur encore meilleur, où les chercheurs auraient accès à des données brutes, ouvertes et directement exploitables.

Table des matières

Liste des figures

CHAPITRE 1 : L'EVOLUTION DES RESEAUX DE MOBILES

CHAPITRE 2 : L'EVOLUTION DES SYSTEMES DE SIGNALISATION ET DE GESTION DES PROFILS UTILISATEURS DANS LES RESEAUX DE TELECOMMUNICATIONS

CHAPITRE 3 : ETUDE DE L'ARCHITECTURE DE L'IMS ET DE L'INTEGRATION AVEC LE WEBRTC

CHAPITRE 4 : PRESENTATION DE L'ENVIRONNEMENT ET OUTILS DE RECHERCHE

CHAPITRE 5 : PROPOSITIONS DE SOLUTION D'AMELIORATION DE FIABILITE DES RESEAUX CONVERGENTS

CHAPITRE 6 : PROPOSITION DE SOLUTIONS DE E-SANTE BASEES SUR LES RESEAUX CONVERGENTS

Liste des tableaux

Liste des abreviations, sigles et acronymes

AAA : Authentication Authorization Account (Authentification Autorisation Traçabilité)
ADIE : Agence de lřinformatique de lřEtat
ADSL : Asymmetric Digital Subscriber Line (ligne d'abonné numérique à débit asymétrique)
AES : Advanced Encryption Standard (Système de cryptage ou de chiffrement)
AMR : Adaptative MultiRate (Codec de voix utilisé dans les téléphones mobiles de 3G)
AMQP : Advanced Message Queing Protocol (Protocole avancé de Message Queuing)
AN : Access Network (Résea dřaccès)
ANDSF : Access Network Discovery and Selection Function (Fonction de découverte et de sélection de réseau d'accès)
ANGW : Access Network GateWay (Passerelle dřaccès au réseau)
AOR: Address-O-Record (Adresse dřenregistrement)
API : Application Programming Interface ((Interface Applicative de Programmation).
APSVR : Application Server (Serveur dřapplication)
AS : Application Server (IMS)
ATM : Asynchronous Transfer Mode (Mode de transfert asynchrone)
AuC : Authentication Center (Centre dřauthentification)
AUTN : AUthentication TokeN (Jeton dřauthentification)
AVP : Attribute Value Pairs (Paires de valeurs dřattribut)

BDR : Base de Données Relationnelle
BFCP : Binary Floor Control Protocol (Protocole de contrôle utilisé pour le partage de contenu dans le cadre de conférences de type SIP)
BG : Breakout Gateway (Passerelle de sortie)
BGCF : Breakout Gateway Control Function (Passerelle controle compatibilité des équipements en sortie)
BICC : Bearer Independant Call Control (gestion de la communication entre serveurs d'appel, indépendamment du type de support, permettant aux opérateurs de réaliser une migration de leurs réseaux RTC/RNIS vers des réseaux en mode paquet)
BSC : Base Station Controller (Contrôleur de station de base)
BSD : Berkeley Software Distribution
BSS : Base Station Sub-system (Sous-système des stations de base)
BTS : Base Transceiver Station (Station de Transmission de Base)

CAMEL : Customized Applications for Mobile network Enhanced Logic (Réseau Intelligent Mobile)
CAN : Connectivity Access Network (Réseau dřaccès de connectivité)
CAP : CAMEL Application Part
CAPEX : CAPital EXpenditure (budget dřinvestissement)
CAS: Channel Associated Signalling
CCS: Common Channel Signalling
CDMA : Code Division Multiple Access (Accès multiple par répartition en code)
CDP: Continuous data protection (Cisco Discovery Protocol)
CG : Charging Gateway (Passerelle de chargement)
CK : Ciphering Key (Clé de Chiffrement)
CN : Core Network (Réseau Cœur)
COPS : Common Open Policy Service (Service des politiques ouvert commun)
CRF : Connection Related Functions (Fonctions liées à la connexion)
CS : Circuit Service (Service Circuit)
CSCF : Call/Session Control Functions (Fonctions de contrôle des appels/sessions)
CTI : Couplage Téléphonie Informatique

DiffServ : Differentiated Services (Services différenciés)

DISC : DIAMETER Server Client (Client serveur Diameter)
DNS : Domaine Name System (Système de nom de domaine)
DPI : Deep Packet Inspection (Inspection approfondie de paquets)
DRNC : Drift RNC
DSL : Digital Subscriber Line (Ligne dřabonné numérique)
DTLS : Datagram Transport Layer Security (Sécurité de la couche de transport Datagram)
DTMF : Dual Tone Multi Frequency (Système de signalisation utilisé pour transmettre la numérotation en commutation analogique)
EAP : Extensible Authentication Protocol Application (Application de protocole dřauthentification extensible)
ECG : ElectroCardioGramme
ECSD : Enhanced Circuit Switched Data (Données à communtation de circuits améliorées)
E-CSCF: Emergency-CSCF (Urgence ŘCSCF)
EDGE : Enhanced Data for GSM Evolution (Données améliorées par GSM Evolution)
ePDG : Packet Data Gateway (Passerelle de données par paquets)
EGPRS: Enhanced GPRS (GPRS amélioré)
eIMS-AGW: IMS Access GateWay (Passerelle dřaccès IMS)
EIR: Equipment Identity Register (Registre dřidentité de lřéquipement)
EPC: Evolved Packet Core (Coeur de paquet amélioré)
EPS: Evolved Packet System (Système de paquets évolué)
ESP : Ecole Supérieure Polytechnique
ETSI : European Telecommunications Standards Institute (Institut Européen des Normes de Télécommunications)
E-UTRAN: Evolved UTRAN (UTRAN évolué)

FO : Fibre Optique
FTTH : Fiber To The Home (Fibre à la maison)

3GPP : 3th Generation Partnership Project (Projet de parténariat de 3ème génération)
GGSN : Gateway GPRS Support Node (Noeud de support GPRS de la passerelle)
GMSC: Gateway MSC (Passerelle MSC)
GMSK : Gaussian Minimum-Shift Keying (Gausienne à décalage minimum)
GNU : GNUřs Not Unix
GPRS : General Packet Radio Service (Service général de radio par paquets)
GSM : Global System for Mobile communications (Système global pour les communications mobiles)
GSS : GPRS Sub-System (Sous-Système GPRS)

HLR : Home Location Register (Base de données locale)
HSCSD : High Speed Circuit Switched Data (Données à commutation de circuits à haute vitesse)
HSDPA : High Speed Downlink Packet Access (Accès par paquets de liaison descendente haute vitesse)
HSL : High Speed Signalings Links (Liens de signalisation haute Vitesse)
HSPA : High Speed Packet Access (Accès Haut débit par paquets)
HSS : Home Subscriber Server (Serveur dřabonne local)
HSUPA : High Speed Uplink Packet Access (Accès haut debit par paquets en liaison montante)
HTA : HyperTension Arterielle
HTML : Hyper Text Markup Language (Langage signalétique Hyper texte)
HTTP : Hyper Text Transfer Protocol (Protocole de transfert hypertexte)
HTTPS : Hyper Text Transfer Protocol Security (Sécurité du protocole de transfert hypertexte)

IAM: Initial Address Message (Message dřadresse initiale)
IAX: Inter Asterisk eXchange (Echange inter Axterisk)
ICE : Interactive Connectivity Establishment (Etablissement de connectivité interactive)
I-CSCF : Interrogating-CSCF (Interrogation ŘCSCF)

IEEE : Institute of Electrical and Electronic Engineers (Institut des ingénieurs électriciens et électroniciens)
IETF : Internet Engineering Task Force (Groupe de travail sur lřingénierie Internet)
IFC : Initial Filter Criteria (Critères de filtrage initiaux)
IK : Integrity Key (Clé dřintégrité)
IMEI : International Mobile Equipment Identity (Identité Internationale de lřéquipement mobile)
IMPI : IP Multimédia Private Identity (Identité privée IP Multimédia)
IMPU : IMS Public User identity (Identité de lřutilisateur public IMS)
IMS : IP Multimedia Subsystem (Sous-Système Multimédia IP)
IMSI : International Mobile Subscriber Identity (Identité Internationale des abonnés mobiles)
IM-SSF : IP Multimedia Service Switching Function (Fonction de commutation de service multimedia IP)
IMSU : IMS Subscription User (Utilisateur dřabonnement IMS)
INAP : Intelligent Network Application Part (Partie dřapplication de réseau intelligent)
IP : Internet Protocol (Protocole Internet)
IP-CAN : IP Connectivity Access Network (Réseau dřaccès de connectivité IP)
IP-PBX : IP-Private Branch eXchange (Echange IP privés)
IPv4 : Internet Protocol version 4 (Protocole dřInternet version 4)
IPv6 : Internet Protocol version 6 (Protocole dřInternet version 6)

IPTV : Internet Protocol TéléVision (Protocole Internet de télévision)
ISC : IP Multimedia Service Control (Contrôle de service multimedia IP)
ISDN : Integrated Services Digital Network (Réseau numérique à intégration de services)
ISIM : IP Multimedia Service Identity Module (Module dřidentité de service multimédia IP)
ISUP : ISDN User Part (Partie utilisateur RNIS)
ITU : International Telecommunication Union (Union Internationale des Télécommunications)
IVR : Interactive Voice Response (Serveur Vocal Interactif)

LAI : Location Area Identification (Identification de la zone de localisation)
LAN: Local Area Network (Réseau Local)
LDAP : Ligthweight Directory Access Protocol (Protocole dřaccès à lřannuaire)
LER : Label Edge Router (Routeur dřétiquette)
LIRT : Laboratoire dřInformatique et réseaux de télécommunications
LNP : Local number portability (Portabilité du numéro local)
LSL : Low Speed Signalings Links (Liens de signalization basse Vitesse)
LSR : Label Switch Router (Router Commutateur dřétiquette)
LTE : Long Term Evolution (Evolution à long terme)

M3UA : MTP 3 User Adaptation (Adaptation utilisateur MTP 3)
MAA : Multimedia-Auth-Answer (Réponse dřauthentification multimédia)
MAC : Medium Access Control (Contrôle dřaccès moyen)
MAR : Multimedia-Auth-Request (Demande dřauthentification multimedia)
M2M : Mobil To Mobil (Mobil à Mobil)
MGCF : Media Gateway Control Function (Fonction de contrôle de la passerelle multimédia)
MGW : Multimédia Gateway (Passerelle multimédia)
MIC : Modulation Impulsion Codée
MME : Mobility Management Entity (Entité de gestion de mobilité)
MMS : Multimedia Messaging Service (Service de messagérie multimédia)
MOM: Message-Oriented Middleware (Middleware orienté message)
MPLS : Multi Protocol Label Switching (Commutation dřétiquette multiprotocole)
MRF : Multimedia Resource Function (Fonction de ressource multimedia)
MRFC : Multimedia Resource Function controller (Controleur de fonction de ressource multimédia)
MRFP : Multimedia Resource Function Processor (Processeur de fonction de ressource multimédia)
MS : Mobile Station (Station Mobile)

MSC : Mobile-services Switching Center (Centre de commutation des services mobiles)
MSISDN : Mobile Station ISDN Number (Numéro RNIS de la station mobile)
MSRP : Message Session Relay Protocol (Protocole de relais de session de message)

NAT : Network Address Translation (Réseau de translation dřadresse IP (RFC 1631))
NGMN : Next Generation Mobil Network (Réseau mobile de nouvelle génération)
NGN : Next Generation Network (Réseau de nouvelle génération)
NSS : Network Sub-System (Sous-Système Réseau)

OPEX: Operating EXpenditure (budget dřexploitation)
OSA : Open Service Access (Accè au service ouvert)
OSA- SCS : Open Service Access Service Capability Server (Serveur de capacité de service dřaccès au service ouvert)
OSS : Operating Sub-System (Sous-Système dřexploitation)
OTT : Over The Top (Sur le dessus)

PABX : Private Automatic Branch eXchange (Autocommutateur privé automatique)
PBX: Private Branch eXchange
PC: Personal Computer (Ordinateur personnel)
PCEF: Policy and Charging Enforcement Function
PCI : Peripheral Component Interconnect (RFC7143) (Interconnexion des composants périphériques)
PCRF : Policy and Charging Rules Function (Fonction politique et règles de facturation)
P-CSCF : Proxy-CSCF
PCU : Packet Control Unit (Unité de contrôle de paquets)
P2P : Peer To Peer (Dřégal à égal)
PDA : Personal Digital Assistant (Agenda électronique personnel)
PDF : Policy Decision Function (Fonction de decision politique)
PDN : Packet Data Network (Réseau de données par paquets)
PDP : Policy Decision Point (Point de decision politique)
PEP : Policy Enforcement Point (Point dřapplication de politique)
PGW: PDN Gateway (Passerelle PDN)
PHP : Personal Home Page (scripts) (Page dřaccueil personnel)
PLMN : Public Land Mobile Network (Réseau mobile terrestre public)
POTS : Plain Ordinary/Old Telephone Service (service téléphonique de base)
PPR : Push profile Request (Demande de profil Push)
PS: Packet Switched (Paquet commuté)
PS : Point Sémaphore
PSK : Phase Shift Keying (Clé de changement de phase à commutation de paquets)
PSTN : Public Switched Telephone Network (Réseau téléphonique commute)
PTS : Points de Transfert Sémaphores (Points de transfert sémaphores)
PUA : Presence User Agent (Agent utilisateur de présence)
PUI : Public User Identity (Identité de lřutilisateur public)

QoS : Quality Of Service (Qualité de service)

RADIUS. : Remote Authentication Dial In User Service (Authentification à distance dans le service utilisateur)
RAND : Nombre aléatoire émis par le réseau vers la MS pour l'authentification et le chiffrement
RCS : Rich Communication Services (Riches services de communication)
RFC : Request For Comments (Demande pour des commentaires)
RI : Réseau Intelligent
RLC : Radio Link Control (Contrôle de liaison radio)
RNC : Radio Network Controller (Contrôleur de réseau radio)

RNIS : Réseau Numérique à Intégration de service
RPC : Remote Procedure Call (Appel de procédure à distance)
RTC : Réseau Téléphonique Commuté
RTCP : Réseau Téléphonique Commuté Public
RTP : Real-Time Transport Protocol (Protocole de transport en temps réel)
RSVP : Ressource Reservation Protocol (Protocole de réservation de ressources)
SAA : Server Assignment Answer (Réponse d'affectation de serveur)
SAE : System Architecture Evolution (Évolution de l'architecture du système)
SAR : Server-Assignment-Request (Demande d'attribution de serveur)
SBC : Session Border Controller (Contrôleur de session)
S-CSCF : Serving-CSCF
SCP : Service Control Point (Point de contrôle de service)
SCTP : Stream Control Transmission Protocol (Protocole de transmission de contrôle de flux)
SDH : Synchronous Digital Hierarchy (Hiérarchie numérique synchrone)
SDP : Session Description Protocol (Protocole de description de session)
SEMS: SIP Express Media Server (Serveur multimédia SIP Express)
SER : SIP Express Router (Routeur SIP Express)
SGSN : Service GPRS Support Node (Noeud de support GPRS de service)
SGW : Serving Gateway (Passerelle de service)
SIGTRAN : Signalling Transport over IP (Transport de signalisation sur IP)
SIM : Subscriber Identity Module (Module d'identité d'abonné)
SIP : Session Initiation Protocol (Protocole de signalisation)
SIP-AS : SIP Application Server (Serveur d'applications SIP)
SLF : Subscriber Location Function (Fonction de localisation d'abonné)
SMS : Short Message Service (Service de messages courts)
SMTP : Simple Mail Transport Protocole (Protocole de transport de courrier simple)
SNA : Subscribe-Notification-Answer (S'abonner-Notification-Réponse)
SNR : Subscribe-Notification-Request (nscription-Notification-Demande)
SOAP : Simple Object Access Protocol (Protocole d'accès aux objets simple)
SONATEL : SOcieté NAtionale des TELecommunications
SQL : Structured Query Language (Langage de requête structure)
SRNC : Serving RNC
SRVCC : Single Radio Voice Call Continuity (Continuité des appels vocaux radio unique)
SS7 : Signalling System 7 (Système de signalisation 7)
SSP : Service Switching Point (Point de commutation de service)
STP : Signalling Transfer Point (Point de transfert de signalisation)
STUN : Session Traversal Utilities for NAT (Utilitaires de traversée de session pour NAT)
SVP : SerVice Profile (Profil de Service)

TCH : Traffic Channel (Canal de trafic)
TCP : Transport Control Protocol (Protocole de contrôle de transport)
TDM : Time Division Multiplexing (Multiplexage par répartition dans le temps)
TIC : Technologies de lřInformation et de la Communication
TLS : Transport Layer Security (Sécurité de la couche de transport)
TRAU : Transcoder/Rate Adaptor Unit (ranscodeur / adaptateur de debit)
TS : Time Slot (Créneau horaire)
TSC : Tandem Switching Center (Centre de commutation tandem)
TURN : Traversal Using Relays around NAT (Traversée à l'aide de relais autour de NAT)

UA : User Agent (Agent utilisateur)
UAA : User Authorization Answer (Réponse d'autorisation utilisateur)
UAC : User Agent Client (Client de l'agent utilisateur)
UAR : User Authorization Request (Demande d'autorisation utilisateur)

UAS : User Agent Server (Serveur Agent utilisateur)
UCAD : Université Cheikh Anta Diop
UDA : User-Data-Answer (données utilisateur-réponse)
UDP : User Datagram Protocol (Protocole de datagramme utilisateur)
UDR : User-Data-Request (Demande de données utilisateur)
UE : User Equipment (Équipement utilisateur)
UHF : Ultra Haute Frequence
UICC : Universal Integrated Circuit Card (Carte de circuit intégré universelle)
UIT : Union Internationale des Télécommunications
UMTS : Universal Mobile Telecommunications System (ystème universel de télécommunications mobiles)
URI : Uniform Resource Identifier (Identificateur de ressource uniforme)
URL : Uniform Resource Locator (Localisateur de ressources uniforme)
USIM : Universal Subscriber identity Module (Module d'identité d'abonné universel)
UTRAN : Universal Terrestrial Radio Access (Accès radio terrestre universel)

VCC : Voice Call Continuity (Continuité des appels vocaux)
VLR : Visitor Location Register (Registre de localisation des visiteurs)
VoIP : Voice over IP (Voix sur IP)
VPN: Virtual Private Network (Virtual Private Network)

W3C: World Wide Web Consortium (Consortium WWW)
WAC : WebRTC Application Controller (Contrôleur d'application WebRTC)
WebRTC: Web Real-Time Communications (Communications Web en temps reel)
WIC: WebRTC IMS Client (Client WebRTC IMS)
Wi-Fi: Wireless Fidelity (Fidélité sans fil)
WLAN : Wireless Local Area Network (Réseau local sans fil)
WiMAX: Worldwide Interoperability for Microwave Access (nteropérabilité mondiale pour l'accès aux micro-ondes)
WS: WebSocket
WSS: WebSocket Secure (Websocket sécurisé)
WWSF : WebRTC Web Server Function (Fonction de serveur Web WebRTC

XHR : XLM HTTP Request (Requête HTTP XLM)
XML : eXtensible Markup Language (Langage de balisage extensible).
XRES : eXpected RESponse (réponse attendue)

Résumé

Lřévolution rapide des TIC (*Technologies de l''Information et de la Communication*), a conduit vers les réseaux de nouvelle génération. Elle sřexplique par le fort pouvoir intégrateur de lřIP qui a facilité la convergence des systèmes de télécommunications existants. LřIMS est le système révolutionnaire pour les réseaux de nouvelle génération. Il est basé sur une architecture standardisée et fournissant une variété de services multimédias qui sont : la téléphonie, la messagerie, les vidéos, lřinternet, la présence dřun abonné, la visioconférence etc... La fourniture des services IMS est assurée par le protocole de signalisation SIP. Les échanges dřinformations dřauthentification et de facturation sont basés sur le protocole DIAMETER. LřIMS demeure un système fédérateur des technologies. Il a permis :

- La première convergence des systèmes de télécommunications, dřaudiovisuel et dřinformatique ;
- La deuxième convergence des systèmes de communications sur le Web ;
- Enfin, la convergence de ces deux grandes familles ci-dessus.

LřIMS demeure le socle de la plateforme de télécommunications, **gage d'émergence numérique**.

Nous assistons aussi à lřémergence de la technologie WebRTC permettant à des utilisateurs dřInternet dřutiliser de simples navigateurs pour accéder à des services multimédias à partir de leurs ordinateurs ou de leurs terminaux mobiles tels que smartphones ou tablettes sans avoir besoin dřinstaller des greffons. Le WebRTC utilise les mêmes services que lřIMS.

Lřobjectif de la thèse est dřaméliorer la fiabilité de lřIMS. Le HSS (*Home Subscriber Server*) est lřélément central de lřIMS. Cřest une base de données qui stocke les profils propres à chaque abonné. Lors de notre expérience, un dysfonctionnement a été constaté au niveau du HSS qui fait que ce dernier nřenvoie pas de réponse au serveur S-CSCF (*Serving-Call/Session Control Functions*). Malgré ce manque de réponse de la part du HSS, on constate sur lřinterface du téléphone du client un message reçu du serveur S-CSCF quřil est connecté. Pour se faire, dans notre première contribution, nous avons proposé une solution dřamélioration de la fiabilité des données du HSS, en intégrant un gestionnaire de file dřattente (*Rabbitmq*) dans le circuit de téléchargement du profil de lřabonné afin que lřentité HSS notifie à lřabonné quřil est bien enregistré.

Dans notre seconde contribution, la problématique dřaccès aux soins de santé dans les zones rurales est dřactualité. Grâce à lřIMS, une solution de suivi et surveillance des paramètres physiologiques vitaux des patients en zones rurales, est proposée pour avoir un accès universel à des soins de qualité et abordables. Une troisième contribution basée sur lřIMS, le WebRTC et les objets connectés, propose une solution pour les plus jeunes gens dans le domaine de la pédiatrie. Ces applications de e-santé vont contribuer largement à aider nos populations dans lřaccès aux soins de bonne qualité et à garantir leur santé. Le facteur humain est une ressource très importante et non négligeable dans le développement dřun pays. Il est urgent dřagir pour avoir une population en très bonne santé et valide pour booster lřéconomie de nos Etats en vue de sortir du sous-développement.

Cřest un apport tangible de propositions de solution pour améliorer la fiabilité de nos systèmes convergents ainsi que les conditions de vie de nos populations.

Mot-clés : TIC, IMS, HSS, DIAMETER, SURVEILLANCE, ACCES UNIVERSEL, E-SANTE, WebRTC, IoT, FIABILITE, CONVERGENCE.

Abstract

The rapid evolution of ICT (*Information and Communication Technologies*) has led to new generation networks. It is explained by the strong integrative power of IP which has facilitated the convergence of existing telecommunications systems. IMS is the revolutionary system for next generation networks. It is based on a standardized architecture and providing a variety of multimedia services which are: telephony, messaging, videos, internet, presence of a subscriber, videoconferencing etc ... The provision of IMS services is ensured by the protocol of SIP signaling. The exchange of authentication and billing information is based on the DIAMETER protocol. The IMS remains a unifying system of technologies. He allowed:

- The first convergence of telecommunications, audiovisual and IT systems;
- The second convergence of communication systems on the Web;
- Finally, the convergence of these two large families above.

IMS remains the backbone of the telecommunications platform, a guarantee of digital emergence.

We are also witnessing the emergence of WebRTC technology allowing Internet users to use simple browsers to access multimedia services from their computers or mobile devices such as smartphones or tablets without the need for install plugins. The WebRTC uses the same services as the IMS.

The objective of the thesis is to improve the reliability of the IMS. The HSS (*Home Subscriber Server*) is the central element of the IMS. It is a database that stores the profiles specific to each subscriber. In our experience, a malfunction has been observed with the HSS which means that the latter does not send a response to the S-CSCF (*Serving-Call / Session Control Functions*) server. Despite this lack of response from HSS, there is a message on the customer's phone interface from the S-CSCF server that he is connected. To do so, in our first contribution, we proposed a solution to improve the reliability of HSS data, by integrating a queue manager (*Rabbitmq*) in the subscriber profile download circuit so that the HSS entity notifies the subscriber that it is well registered.

In our second contribution, the issue of access to health care in rural areas is topical. Thanks to IMS, a solution for monitoring and surveillance of vital physiological parameters of patients in rural areas, is offered to have universal access to quality and affordable care. A third contribution based on IMS, WebRTC and connected objects, offers a solution for the youngest people in the field of pediatrics. These e-health applications will make a major contribution to helping our populations access good quality care and guarantee their health. The human factor is a very important and significant resource in the development of a country. It is urgent to act to have a population in very good health and able to boost the economy of our States in order to emerge from underdevelopment.

This is a tangible contribution of proposed solutions to improve the reliability of our converging systems as well as the living conditions of our populations.

Keywords: TIC, IMS, HSS, DIAMETER, SURVEILLANCE, UNIVERSAL ACCESS, E-HEALTH, WebRTC, IoT, RELIABILITY, CONVERGENCE.

Introduction générale

Aujourd'hui, le domaine des télécommunications et des réseaux est en pleine expansion. La libéralisation du secteur de télécommunications avec lřévolution rapide des technologies de lřinformation et de la communication (*TIC*), la téléphonie mobile est devenue la locomotive du secteur des télécommunications. LřInternet sřest positionné comme un vecteur de développement mondial. Nous constatons aussi lřévolution de lřinternet en général et de lřavènement de lřInternet des objets (*IoT*) en particulier, pourrait engendrer de milliards dřobjets connectés en 2020 selon Cisco Visual Networking Index. Ainsi, plus le trafic va croissant et important, plus la charge des équipements réseaux augmentera. Ceci va avoir un impact non négligeable sur la qualité de service (*QoS*) lors de la transmission des flux malgré les différentes solutions proposées jusquřici dans les réseaux de télécommunications.

Ainsi, les opérateurs sont dans le processus dřamélioration continue de leurs architectures afin de les adapter au nouveau concept. La difficulté du processus de déploiement des services se manifeste aussi avec une lourde charge des CAPEX (*CAPital EXpenditure ou budget d'ìnvestissemnt*) et OPEX (*Operating EXpenditure ou budget d'ëxploitation*). Face aux demandes croissantes des nouveaux services, lřexplosion du trafic numérique avec lřutilisation de lřinternet, les opérateurs avaient pour objectif dřoptimiser leurs infrastructures afin de les rendre flexibles à toute modification avec un coût minimum (réduction de CAPEX et OPEX). Des architectures basées essentiellement sur le protocole IP, permettent la mutualisation des ressources réseaux et services. Elles ont donné naissance aux réseaux de nouvelle génération (*NGN*). Les caractéristiques communes des réseaux de nouvelle génération, globalement agréées sont : la généralisation des réseaux à commutation des paquets et la convergence vers « **Tout IP** », la séparation nette entre les fonctions de contrôle et les fonctions de transport, le découplage service/transport, lřubiquité, la flexibilité et la convergence des fonctions de gestion. Les réseaux de nouvelle génération vont permettre dřaugmenter la productivité en créant des nouveaux usages en fonction de besoins exprimés par lřutilisateur. Le choix du réseau est soumis aux politiques des fournisseurs ainsi quřaux préférences des utilisateurs. Dans cet environnement, lřutilisateur peut choisir le réseau le plus adapté pour effectuer sa communication.

LřIMS (*IP Multimedia Subsystem*) constitue le standard des réseaux NGN et offre aux opérateurs une architecture de services multimédias. Il a pour objectif le traitement des flux et services multimédias dans une optique de convergence, quel que soit le réseau dřaccès utilisé

(GSM, Wi-Fi, Ethernet, UMTS, WiMAX, etc.), quelle que soit sa nature (Fixe, Mobile ou Internet), et quel que soit le type de terminal considéré (ordinateur, smartphone, téléphone, etc…). Il fournit du haut débit en mobilité pour les données et les services téléphoniques de qualité. Il intègre différents services tout en offrant une plateforme commune, facilitant leur déploiement et centralisant les fonctionnalités comme la gestion de session, les fonctions dřauthentification, dřautorisation et de traçabilité comme sous le sigle AAA (*Authentication, Authorization, Accounting/Auditing*) ou encore la gestion de la qualité de service. Il est basé sur le protocole IP pour le transport de données et le protocole SIP (*Session Initiation Protocole*) pour la signalisation et le contrôle de session. Dans cette convergence, lřIMS permet dřinterconnecter les systèmes basés sur les technologies des opérateurs des télécommunications et les systèmes de communication basés sur les technologies Internet. Il nřy a plus de limites entre les télécommunications et lřinformatique. LřIMS demeure un réseau fédérateur des systèmes de communication. Voilà pourquoi, il est important de faire une étude de sa fiabilité. Un système fiable est un système auquel nous pouvons lui faire entièrement confiance et lřutiliser avec beaucoup de satisfaction.

En effet, nous montrons lřimportance de lřIMS dans les réseaux mobiles, fixes et Internet. Une étude détaillée de son architecture va nous permettre de montrer son utilité dans les systèmes convergents. Les technologies de télécommunications sur le Web prennent aussi une importance capitale grâce à la technologie WebRTC. Le WebRTC fournit les mêmes services que lřIMS. Une passerelle est prévue dans lřIMS pour une interconnexion avec le WebRTC.

Dans le cadre de nos travaux, nous notons que lřOpen IMS est le coeur de réseau IMS basé sur la solution open source SIP Express Router (*SER*). Il a été développé par lřinstitut Fraunhofer FOKUS en Allemagne et les premières versions sont apparues à partir de 2006 et sont destinées à des plateformes du monde Linux. OpenIMSCore est une implémentation Open Source de la norme 3GPP IMS. Ce projet a été lancé pour promouvoir lřadoption de la technologie IMS dans les réseaux de télécommunications de prochaine génération, et amener le développement de nouveaux services basés sur IMS. OpenIMSCore implémente les différentes fonctions qui forment ensemble les éléments de base dřune architecture IMS/NGN. Il sřagit des fonctions de contrôle de session dřun coeur de réseau IMS (serveurs CSCF - P-CSCF, I-CSCF et S-CSCF), de fonction HSS permettant donc de provisionner un certain nombre dřutilisateurs et de leur associer un profil de service permettant la mise en oeuvre de lřinvocation de services si chers à lřarchitecture IMS. Tous les composants sont basés sur des logiciels open source, tels que SER (*SIP Express Router*) ou MySQL. Le projet

OpenIMSCore est avant tout conçu pour la recherche et le développement (fournisseurs de matériel de télécommunications, opérateurs de réseaux, projets de recherche universitaire).
Grâce aux outils de recherche basés sur les logiciels libres qui ont fait leur preuve, nous avons implémenté une plateforme Kamailio qui respecte toutes les normes de lřarchitecture IMS et présente des avantages suivants :

- Aucune dépendance vis à vis dřun fournisseur de matériel ou de logiciel et le coût de mise en œuvre est negligeable, à portée des mains, car aucune acquisition dřéquipement de télécommunications ou de licence de logiciel propriétaire ;
- La plateforme va permettre aux chercheurs de faire des simulations concrètes sur de nouvelles approches, de nouveaux concepts ainsi que de nouveaux services et protocoles sans le moindre coût et dřen tirer des résultats probants.

Cřest dans ce contexte que nous menons ce travail de recherche qui sřintéresse, entre autres, aux problématiques liées dřune part à lřauthentification des abonnés qui va impacter la fiabilité de la base de données HSS de lřIMS et dřautre part à lřaccès difficile aux soins de santé des populations rurales pour les cas de maladies telles que le diabète, lřhypertension, etc… et au cas des plus petits dans le domaine de la pédiatrie entrainant de taux de mortalité infantile et juvénile dans les zones rurales.
Lřobjectif de cette thèse est de contribuer à lřamélioration de la fiabilité du réseau IMS. Pour se faire, la gestion des utilisateurs est un des aspects importants dans le système IMS. Ainsi, lřIMS dispose dřun élément central appelé HSS. Lřentité HSS est une base de données qui stocke les données propres à chaque utilisateur, les paramètres dřaccès, les règles dřinvocation de service ainsi que les données de facturation. Un dysfonctionnement de lřentité HSS peut impacter négativement sur la qualité de service (QoS) et les profits des opérateurs. Lřétude de ce dysfonctionnement a permis de proposer lřintégration dřun gestionnaire de file dřattente pour améliorer la fiabilité du HSS.
Grâce à lřIMS et le WebRTC, une première proposition dřapplication de e-santé offre un accès universel à la santé à moindre coût aux zones rurales.
Une deuxième proposition dřapplication basée sur les technologies, lřIMS, le WebRTC et les objets connectés, a été faite par le groupe de travail du laboratoire LIRT dans le domaine de e-santé pour que les plus jeunes enfants du monde rural puissent être consultés à distance par les meilleurs spécialistes. Cřest une contribution pour réduire le taux de mortalité infantile et juvénile.

Ce document qui présente nos travaux de recherche sur « ***l'étude de la fiabilité des systèmes convergents de télécommunications et leurs applications*** », sřorganise en six (6) chapitres répartis comme suit :

- **Chapitre 1** : « **l'évolution des réseaux de mobiles** ». Ce chapitre présente les six (6) étapes de lřévolution des réseaux de mobiles portant sur lřétat de lřart relatif à leurs différentes architectures. La convergence des réseaux de télécommunications est abordée ;
- **Chapitre 2 :** « **l'évolution des systèmes de signalisation et de gestion des profils utilisateurs dans les réseaux de télécommunications** ». Ce chapitre est consacré à lřévolution de la signalisation depuis la SS7 jusqřau SIP en passant par SIGITRAN ainsi que le protocole DIAMETER. Il met en exergue lřimportance de lřIMS dans les réseaux fixes et mobiles ;
- **Chapitre 3 :** « **l'étude de l'architecture de l'IMS et de l'intégration avec le WebRTC** ». Ce chapitre présente lřétat de lřart du réseau IMS sur lequel sřappuie cette thèse ainsi que lřintégration de lřIMS avec le WebRTC ;
- **Chapitre 4 :** « **l'environnement et les outils de recherche** ». Ce chapitre présente les logiciels libres qui ont aidé à la conception de la plateforme déployée et utilisée pour mettre en évidence certains dysfonctionnements de lřIMS lors de lřenregistrement dřun abonné. Ils constituent un atout pour les chercheurs africains afin de contribuer efficacement à lřamélioration des systèmes de télécommunications ;
- **Chapitre 5 :** « **la proposition de solutions d'amélioration de fiabilité des réseaux convergents** ». Ce chapitre soulève la problématique du non-enregistrement dřun abonné dans la base HSS. Lřabonné nřa pas reçu lřinformation « statut connecté » du système sur son terminal. Il décrit la solution à la suite des différents tests pour montrer lřimportance de la fiabilité dřun système convergent tel que lřIMS. LřIMS constitue le point dřancrage pour ces deux réseaux : fixe et mobile puis permet de réaliser leur convergence. Voilà pourquoi, il est important de regarder son architecture en détail puis dřétudier la fiabilité des informations échangées dans le réseau IMS notamment lřenregistrement dřun abonné. Il faut un système fiable en vue dřexploiter les services à valeur ajoutée mis à la disposition de la clintèle pour lřépanouissement de nos populations dans les domaines suivants : lřaccès aux soins de la santé à distance, lřéducation, lřagriculture etc...

- **Chapitre 6 :** « **la proposition de solutions d'e-santé basée sur les réseaux convergents** ». Ce chapitre présente une contribution dřapplications pour lřaccès universel à la santé aux populations adultes des zones rurales ainsi quřà la population la plus jeune (les bébés) ;
- **La conclusion** présente les résultats des travaux réalisés et suggestions ou perspectives pour les prochains travaux de recherche.

Chapitre 1 : L'évolution des réseaux mobiles

Les systèmes de communications mobiles ont considérablement évolué durant ces dernières années. Plusieurs systèmes ou réseaux cellulaires ont été déployés pour repondre à la demande de la clientèle. Un réseau peut être vu comme un ensemble de ressources mises en place pour offrir un ensemble de services. Le service téléphonique et la transmission des données constituent les deux principaux services rendus par les réseaux mobiles. Les évolutions technologiques ont augmenté progressivement les capacités et les fonctionnalités des ressources réseaux afin de garantir lřoffre des services aux usagers. Lřaugmentation des débits de la transmission des données améliore encore lřaccessibilité aux services de lřInternet. La migration des services de lřInternet vers les réseaux mobiles, constitue un enjeu majeur de recherche en télécommunications. La qualité de service (*QoS*) offerte aux utilisateurs mobiles sřaméliore dřun système à lřautre. Les différentes étapes dřévolution des réseaux mobiles vont conduire au standard des réseaux NGN qui est lřIMS. L'IMS offre aux opérateurs la possibilité de construire une infrastructure de services ouverte basée sur IP avec un déploiement facile de nouveaux services, et sur le protocole SIP (*Session Initiation Protocol*) pour le contrôle de session. LřIMS constitue le socle des systèmes convergents et son importance dans les réseaux mobiles, fixes et Internet est démontrée dans les chapitres qui suivent. Les réseaux mobiles ont connu plusieurs évolutions ; nous avons enregistrés six (6) étapes dřévolutions que nous traitons dans le cadre de cette thèse. Enfin, nous terminerons chaque étape par une synthèse.

1.1. Première étape de l'évolution de réseaux mobiles

Cette première étape de réseaux mobiles est marquée par le réseau GSM (*Global System for Mobile communications*), premier système de téléphonie mobile, répondant aux exigences dřinterconnexion et de mobilité du monde contemporain. Il offre des services de données avec de la messagerie texte (SMS). De plus, le GSM ne propose quřun **débit de 9,6 kbits/s.** Il permet de gérer les communications des réseaux de mobiles **PLMN** (*Public Land Mobile Network*) et réseaux fixes téléphoniques **PSTN** (*Public Switched Telephone Network*). Il est constitué dans son architecture de base (figure 1.1) : dřun réseau dřaccès **BSS** (*Base Station*

Sub-system), dřun cœur de réseau **NSS** (*Network Sub-System*) et dřun mobile **MS** (*Mobile Station*).

Figure 1.1. Achitecture de base du réseau GSM

Ce réseau se raccorde aux PSTN et aux PLMN dřautres opérateurs grâce aux passerelles ; elles sont aussi spécifiées dans le standard GSM. Lřarchitecture physique détaillée du réseau GSM est décrite à la figure 1.2 ci-dessous [1] [6].

1.1.1. Les composants de l'architecture physique détaillée du réseau GSM

Le réseau de mobiles GSM est constitué de deux sous-systèmes : le **BSS** et le **NSS** (figure 1.2). Ils sont décrits ci-dessous.

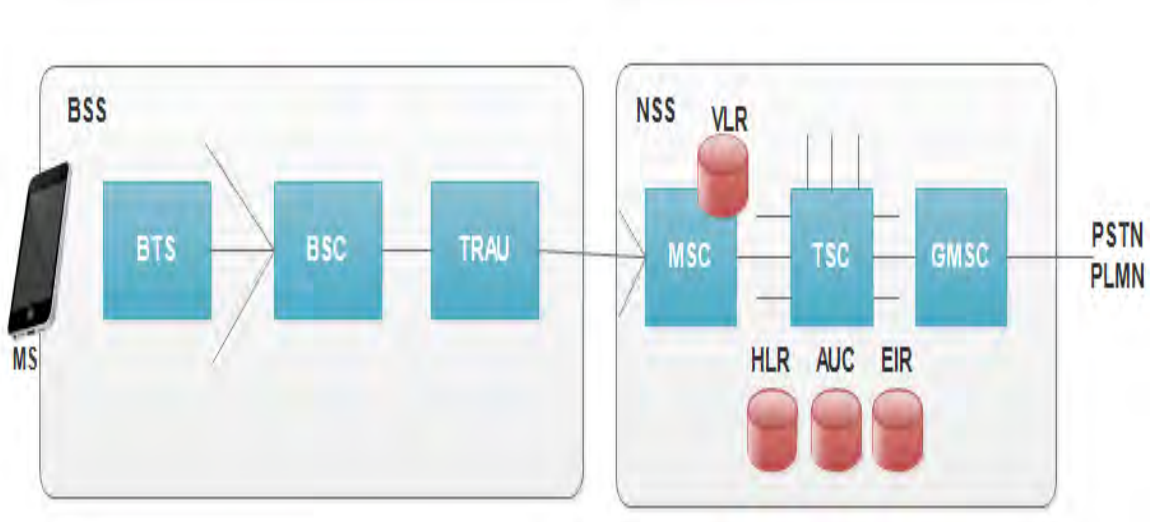


Figure 1.2. Composants de l'architecture physique détaillée du réseau GSM

1.1.1.1. Le sous-système radio BSS (*Base Station Sub-System*)

Il assure la transmission radioélectrique avec le mobile, gère les ressources radioélectriques et permet la mobilité du mobile. Il est constitué de :

- **Terminaux mobiles :** ce sont des supports utilisés pour la voix et les données ou lřéchange de message SMS. Chaque terminal a une carte **SIM** (*Subscriber Identity Module*) avec un numéro **IMSI** (*International Mobile Subscriber Identity*). Un numéro **IMEI** unique (*International Mobile Equipment Identity*) attribué par le constructeur.
- **Stations radioélectriques BTS** (*Base Transceiver Station*) : ce sont des points dřaccès au réseau. Un BTS est associé à une cellule et est située au centre de celle-ci.
- **Contrôleurs de stations radioélectriques BSC** (*Base Station Controller*) : ils gèrent les ressources radio dřune ou de plusieurs BTS.
- **Équipements de transcodage TRAU** (*Transcoder/Rate Adaptor Unit*) : il réalise le transcodage de la parole et permet la conversion du format G711 à 64 kbit/s. Pour le service de transmission de données, le TRAU effectue la conversion de rythme (< 14 400 kbit/s) afin de lřadapter au circuit à 64 kbit/s commuté par le NSS [1] [3].

Les entités du sous-système NSS sont décrites dans le paragraphe qui suit.

1.1.1.2. Le sous-système réseau NSS (*Network Sub-System*)

Il sřoccupe de lřinterconnexion avec les réseaux fixes, publics ou privés, auxquels est rattaché le réseau mobile. Le **NSS** est constitué des entités suivantes :

- Commutateurs téléphoniques **MSC** (*Mobile-services Switching Center*) : ils font la gestion des appels et de tout ce qui est lié à lřidentité des abonnés, à leur enregistrement et à leur localisation. Il existe des passerelles appelées **GMSC** (*Gateway MSC*), assurant lřinterface avec le réseau téléphonique fixe **PSTN** ou le réseau des mobiles **PLMN**. Le **TSC** (*Tandem Switching Center*) est un commutateur temporel à 64 kbits/s, effectuant le transit entre deux MSC.
- Base de données **HLR** (*Home Location Register*) : elle contient les informations sur les abonnés dřune région desservie par le MSC et possède leur position courante. Les caractéristiques enregistrées de chaque abonné sont les suivantes : **l'identité IMSI**, le

numéro dřannuaire **MSISDN** (*Mobile Station ISDN Number*) et le profil de lřabonnement ou lřautorisation dřappel international.

- **VLR** (*Visitor Location Register*) : une base de données contenant temporairement des informations sur les abonnés qui visitent une région desservie par un MSC autre que celui auquel ils sont abonnés. Ces informations proviennent du HLR auquel lřabonné est enregistré et indiquent les services auxquels lřabonné a droit. Ce transfert dřinformations se fait une seule fois et nřest effacé que lorsque lřabonné ferme son appareil ou quitte la région du MSC courant. Il est à noter que le VLR est toujours associé à un MSC.
- **AuC** (*Authentication Center*) : elle est une base de données protégée qui contient une copie de la clé secrète inscrite sur la SIM de chaque abonné. Cette clé est utilisée pour vérifier lřauthenticité de lřabonné et lřencryptage des données envoyées.
- **EIR** (*Equipment Identity Register*) : elle est une base de données qui contient la liste de tous les terminaux validés (IMEI). Elle est consultée lors des demandes de connexion dřun abonné et permet de refuser lřaccès au réseau à un terminal qui a été déclaré perdu ou volé.

A cela, nous ajoutons un sous-système dřexploitation et maintenance **OSS** (*Operating Sub-System*) qui permet à lřexploitant dřadministrer le réseau et dřen effectuer la maintenance.

La couverture du territoire est assurée par le réseau de mobiles GSM. Le réseau doit enregistrer la zone de localisation **LAI** (*Location Area Identification*) où se situe le mobile, appelée itinérance ou roaming. Le mobile peut passer dřune cellule à une autre, sa liaison avec le réseau doit être maintenue : **c'est la notion de mobilité ou de handhover** [1] [3].

1.1.2. Synthèse de l'étape 1

Le réseau GSM a permis de rendre les services de la voix, des données avec un débit de 9,6 kbits/s. Néanmoins, les limites les plus connues de cette première étape sont les suivantes : la plus importante est dřordre capacitaire, impliquant le rejet dřappels aux heures les plus chargées. Et la seconde est que le réseau GSM utilise un cœur de réseau à commutation par circuit où le service des données est particulièrement lent.

Ainsi, les réseaux à commutation de circuits sont inefficaces pour gérer les transmissions de données fréquentes. Pour repousser toutes ces limites et développer des services Internet mobile, des efforts ont été consentis pour améliorer le système GSM.

1.2. Deuxième étape de l'évolution de réseaux mobiles

Avec le développement de lřinternet, le réseau à commutation par paquets, les terminaux mobiles reposant sur les services GSM ne pouvaient y accéder qu'avec de faibles débits ***(9,6 kbit/s)*** utilisant la commutation en mode circuit, capacité en débits limitée. Une entité nouvelle sřest rajoutée dans lřarchitecture de base du GSM de la figure 1.1 : cřest le sous-système **GSS (***GPRS Sub-System*) (figure 1.3). Ainsi, les trois (3) sous-systèmes : **BSS**, **NSS** et **GSS** constituent le réseau GPRS (*General Packet Radio Service*), réseau qui utilise la commutation par paquets pour le monde de lřInternet mobile.

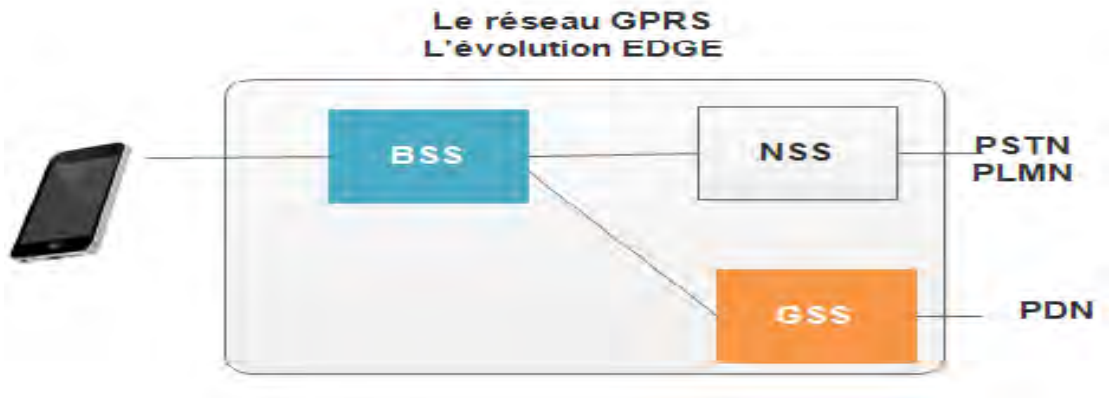


Figure 1.3. Réseau GPRS, l'évolution EDGE

1.2.1. Le réseau GPRS (General Packet Radio Service)

Le **GPRS** sřintègre convenablement au GSM. Ils ont en commun plusieurs entités représentées sur la figure 1.4.

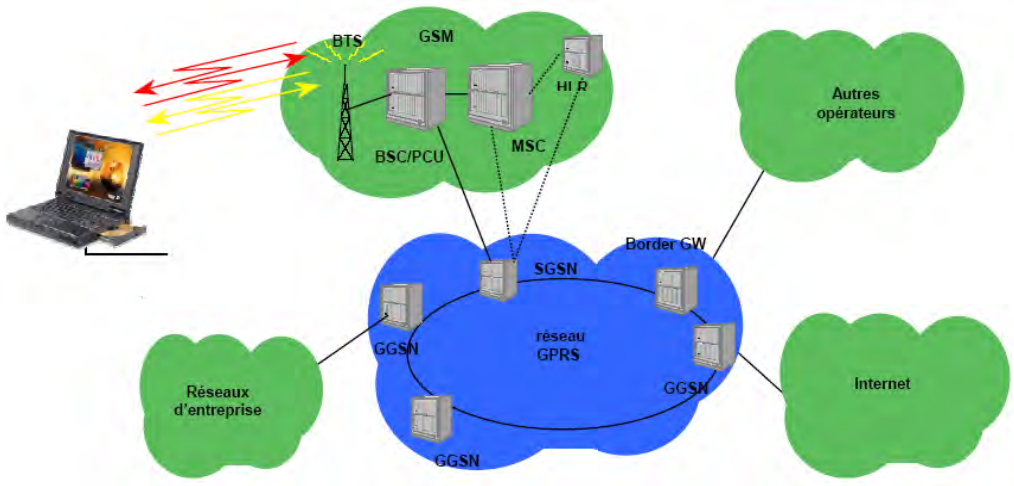


Figure 1.4. Réseau GPRS, couche supplémentaire au GSM [4]

Lřarchitecture physique détaillée de la figure 1.5 montre bien le GSS rajouté et est constitué des entités suivantes : le **SGSN** (*Service GPRS Support Node*) et le **GGSN** (*Gateway GPRS Support Node*) qui constituent le réseau GSS et qui assurent le routage des paquets. La fonction **PCU** (*Packet Control Unit*) introduite dans le BSS qui assure lřattribution de la ressource radioélectrique au mobile et lřinterface avec le SGSN.

- ✓ **SGSN** : cřest un serveur dřaccès au service GPRS (équivalent au MSC), gère les MS (Mobile Station) en délivrant des paquets ;
- ✓ **GGSN** : cřest un routeur connectant le réseau GPRS aux réseaux externes IP ou X25. Il sert de passerelle entre les SGSN et les autres réseaux de données ;
- ✓ **PCU** : il gère les fonctions de couches basses, les protocoles RLC (Radio Link Control), MAC (*Medium Access Control*), le contrôle de puissance, lřadaptation des débits, …. Il gère aussi les fonctions de transmissions et dřacquittements [1].

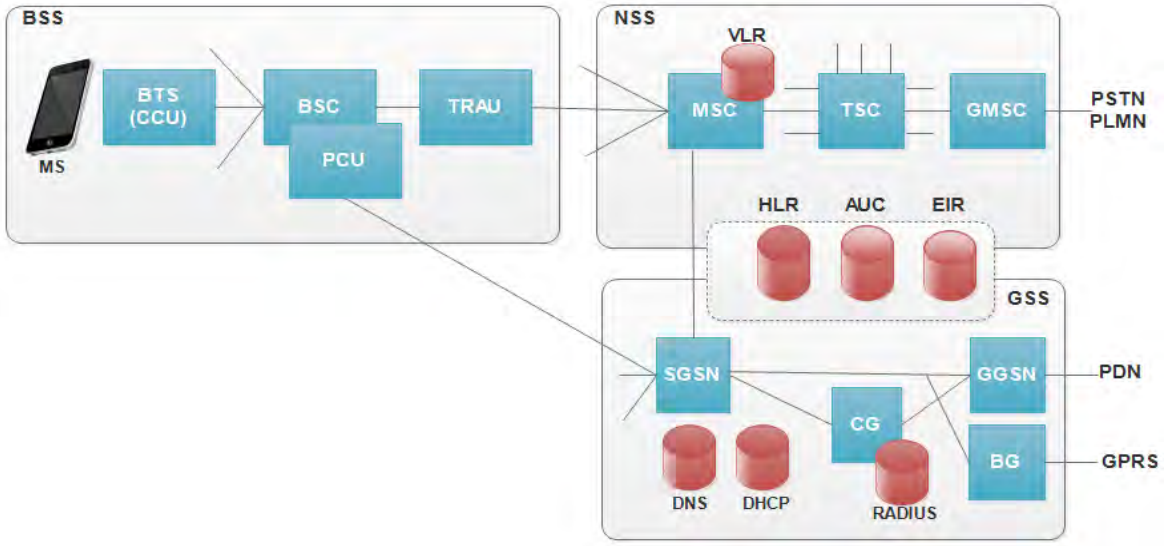


Figure 1.5. Architecture physique détaillée du réseau GPRS

Dans le but dřaccroitre les débits, le réseau dřaccès GSM est connecté au cœur de réseau GPRS. Cette nouvelle étape améliore la prise en charge des services de données. Avec le service GPRS, ces données sont transmises par paquets avec un débit élevé ***(jusqu'à 171,2 kbit/s*** quand les conditions de propagations sont optimales), ce qui diminue le temps de téléchargement pour les pages Web. Cependant, les débits uplink restaient faibles au départ du fait de la limitation des mobiles à un time slot, bien quřune certaine volonté des opérateurs a permis dřobtenir des terminaux capables notamment de transmettre jusquřà 4TS (Time Slot)

sur la liaison montante. Avec le GPRS, le réseau sřadapte à la communication de paquets de données. LřEDGE (*Enhanced Data for GSM Evolution*) suit le GPRS et renouvelle lřinterface radio pour offrir des débits plus élevés. Ainsi, GSM offre un débit **au maximum égal à 14,4 kbit/s**. Le service de transmission de données en mode circuit nommé **HSCSD** (*High Speed Circuit Switched Data*), peut être utilisé par un seul utilisateur lui permettant dřoccuper jusqřà quatre (4) canaux logiques **TCH** (*Traffic Channel*) dřune porteuse radioélectrique. Lřutilisateur peut disposer dřun débit allant jusqřà **57,6 kbit/s (4 x 14,4 kbit/s)**. Ce service de données est compatible avec le débit 64 kbit/s commuté par MSC (*Mobile-services Switching Center*). **Le GPRS** et **EDGE** sont de standard de transition entre le GSM et lřUMTS [1].

1.2.2. Le réseau EDGE et son évolution

Le **réseau EDGE** (*Enhanced Data for Global Evolution*) est introduit dans les réseaux GSM et GPRS pour offrir soit un service en mode circuit **ECSD** (*Enhanced Circuit Switch Data),* soit un service en mode paquet **EGPRS** (*Enhanced General Packet Radio Service*) [1] [3]. Le standard EDGE utilise une modulation **8-PSK** (Phase Shift Keying à 8 états de phase) différente de celle du GSM. Lřobjectif de ce réseau EDGE est lřaugmentation du débit sur lřinterface radioélectrique en conservant la même largeur du canal radioélectrique (**200 KHz**). Dans la théorie, lřEDGE permet d'atteindre des débits allant jusqřà ***384 kbit/s*** pour les stations fixes (piétons et véhicules lents) et jusqřà ***144 kbit/s*** pour les stations mobiles (véhicules rapides) [1]. LřEDGE est une extension du réseau GPRS pour le service Internet avec un débit élevé, meilleur qřen GSM. Il est aussi important de parler de la qualité de service.

1.1.3. La qualité de service

La qualité de service associée aux services déployés, comprend plusieurs critères comme le taux de perte et le délai (tableau 1.1 et tableau 1.2). La situation de congestion du réseau est gérée en écartant le trafic le moins prioritaire grâce aux trois classes de service offertes. Les niveaux de taux de perte correspondant à des garanties différentes sur la probabilité de perte, de duplication et de séquencement des données. Différentes classes de délai sont aussi définies en fonction de la taille des paquets. La probabilité de perte fait allusion au temps

maximal (dépend des protocoles utilisés : TCP/IP) de séjour du paquet dans le réseau GPRS, temps au-delà duquel le paquet est supprimé. Les applications de classe 1 ne doivent généralement avoir aucune contrainte de temps réel, car elles nřacceptent aucune erreur. En revanche, les applications tolérant des erreurs peuvent être de classe 3 et avoir des contraintes temps réel. Quatre classes de délai sont définies. Dans un premier temps, les réseaux GPRS offrent seulement le service de classe 4 (best effort), qui correspond à la classe assurée par les réseaux IP actuels. Le délai comprend le temps dřaccès au canal ŕ niveau RLC-MAC ŕ , le temps de transmission sur lřinterface air, le temps de transit dans le réseau GPRS ŕ entre les différents nœuds du réseau ŕ mais ne comprend pas les délais dus aux autres réseaux. Le débit moyen inclut les périodes de silence pour les services dont le trafic est sporadique. Les classes de débit moyen sont recensées au tableau 1.2.

Tableau 1.1. Les classes de service – Le taux de perte

Classe	Probabilité de perte	Probabilité de duplication	Probabilité de déséquencement
1	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-2}

Tableau 1.2. Les classes de service – Le délai

Classe	Taille 128 octets		Taille de 1024 octets	
	Délai moyen	Délai à 95%	Délai moyen	Délai à 95%
1	< 0,5s	<1,5s	< 2s	< 7s
2	< 5s	< 25s	< 15s	< 75s
3	< 50s	< 250s	< 75s	< 375s

1.2.4. Synthèse de l’étape 2

Lřarchitecture **GSM** fournit les services voix, tandis que lřarchitecture **GPRS** fournit les services de données par paquets avec un débit élevé. Le réseau GPRS est le premier à utiliser la commutation par paquets dans le monde de lřInternet mobile grâce à lřentité GSS rajoutée. Il permet de faire découvrir aux utilisateurs ce que lřon peut avoir avec son terminal mobile, les possibilités en matière de services, etc… Le réseau **EDGE** fait partie de GPRS et ouvre

enfin le GSM aux systèmes de troisième génération des réseaux mobiles (UMTS). Lřintroduction du EDGE dans le réseau GSM/GPRS a permis aux opérateurs dřaméliorer les services et les capacités à la demande des utilisateurs [1] [4]. La troisième étape dřévolution des réseaux mobiles va être déterminante.

1.3. Troisième étape de l'évolution de réseaux mobiles

Cette troisième étape a été marquée par **le réseau UMTS** (*Universal Mobile Telecommunications System*) (figure 1.6). Il a une structure comparable à celle des réseaux GSM et GPRS. Il faut remarquer que lřélément nouveau qui est rajouté à lřarchitecture de base du GPRS (figure 1.5) est le **réseau d'accès UTRAN** (*UMTS TRAnsport Network*). Le réseau UMTS est constitué dřun :

- ✓ sous-système **NSS :** il est commun aux réseaux GSM et à lřUMTS pour les services orientés circuits ;
- ✓ sous-système **GSS :** il est commun aux réseaux GPRS et à lřUMTS pour les services orientés paquets ;
- ✓ réseau dřaccès **UTRAN** qui est identique à celui du BSS des réseaux GSM et GPRS ;
- ✓ mobile **UE** (*User Equipment*).

Lřinterconnexion des machines de lřentité NSS est assurée par le réseau de transmission **SDH** (*Synchronous Digital Hierarchy*).

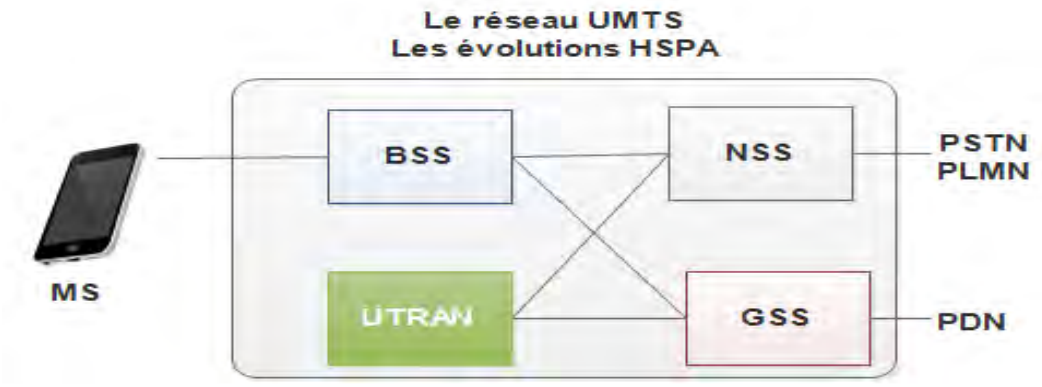


Figure 1.6. Réseau UMTS, évolutions HSPA

Le réseau UMTS a des taux de transfert plus élevés que celui du GSM/GPRS, a été le premier à permettre des **appels vidéo**. Les objectifs de lřUMTS définis dans le tableau 1.3 :

Tableau 1.3. Les objectifs de l'UMTS

	Services temps réel		Services non-temps réel	
Environnement	**Débit Max**	**BER Retard**	**Débit Max**	**BER Retard**
Rural (v<500km/h)	144 kbits/s	10^{E}-3/10^{E}-7 20-300 ms	144 kbits/s	10^{E}-5/10^{E}-8 150 ms (95%)
Urbain (v<120 km/h	384 kbits/s		384 kbits/s	
Indoor ou courte portée	2 Mbits/s		2 Mbits/s	

Les services temps réel : VoIP, Vidéo.Webcam, messagérie instantanée, radio amateur bidirectionnelle ou multidirectionnelle, chat, visioconférence en direct, téléconférence en direct, téléprésence robotique.

Les services non-temps réel : SMS, MMS, messagérie vocale, le courrier électronique (e-mail), navigation sur Internet.

Un des buts de lřUMTS est de fournir des services temps réel au moins jusquřà **144 kbits/s** pour les données et, éventuellement dans certains cas, de monter le débit pour certains utilisateurs jusquřà **2 Mbits/s** tout en continuant à fournir des services de voix performants en adaptant par exemple comme en GSM, un ensemble de dispositifs de codage de la parole aux conditions radio du canal (**AMR** : *Adaptive Multi-Rate*) [1]. Les services supports du réseau UMTS sont définis ci-dessous.

1.3.1. Les services

LřUMTS offre une gamme de services supports qui permet le transfert de trois types de téléservices suivant le tableau 1.4 :

Tableau 1.4. Les services UMTS

Téléservice	Classe de service	Mode CS/PS	Débit maximal en kbit/s	
			Sens montant	Sens montant
Parole AMR (300Hz-3400Hz)	Conversationnel	CS	12,2	12,2
Signal numérique UDI	Conversationnel	CS	64	64
Paquet IP	Interactive Arrière plan	PS	64/128/384	64/128/384
			8	8

Il existe des classes de service qui sont énumérées ci-dessous :
La **classe de service conversationnelle** est utilisée pour les signaux bidirectionnels en temps réel tels que la téléphonie ou la vidéoconférence. Les applications en temps réel ont des contraintes sévères sur les trois paramètres de la qualité de service : **la perte**, **le retard** et la **gigue.**

La **classe de service Streaming** est utilisée pour les signaux unidirectionnels en temps réel, comme la vidéo en temps réel ou lřaudio. Cette classe de service présente des contraintes moins importantes en ce qui concerne le **retard**.

La **classe de service interactive** est utilisée pour les applications (dialogue entre un abonné et un serveur). Les applications interactives utilisent généralement le protocole TCP qui effectue une reprise en cas de perte. Lřinteractivité impose une **clause sur le retard**.

La **classe de service d'arrière-plan** est utilisée pour les applications de lřInternet (messagerie électronique, transfert de fichiers) peu sensibles à la dégradation des paramètres de la qualité de service [1].
Lřoffre de ces services sřappuie sur une architecture avec ces différentes composantes décrites ci-dessous.

1.3.2. Les composantes de l'architecture du réseau UMTS

Lřarchitecture physique détaillée du réseau UMTS est représentée par la figure 1.7, constituée des éléments suivants :

- ✓ la station de base ou **Node B** effectue des fonctions semblables à celles des BTS des réseaux GSM et GPRS. Elle assure lřinterface radioélectrique avec le mobile et se raccorde au RNC.
- ✓ le **RNC** (*Radio Network Controller*) assure les fonctions semblables à celles du BSC des réseaux GSM et GPRS. Il gère les ressources radioélectriques de la zone dont il a le contrôle. Il se raccorde au MSC et au SGSN. Deux RNC peuvent se raccorder directement entre eux.

Le **SRNC** (*Serving RNC*) gère la connexion avec le cœur de réseau, le protocole de signalisation avec le mobile et lřallocation des ressources radioélectriques. Le **DRNC** (Drift

RNC) effectue le transfert des données de façon transparente et assure le contrôle des cellules. Le handover entre deux RNC se réalise sans avoir recours au MSC ou au SGSN.

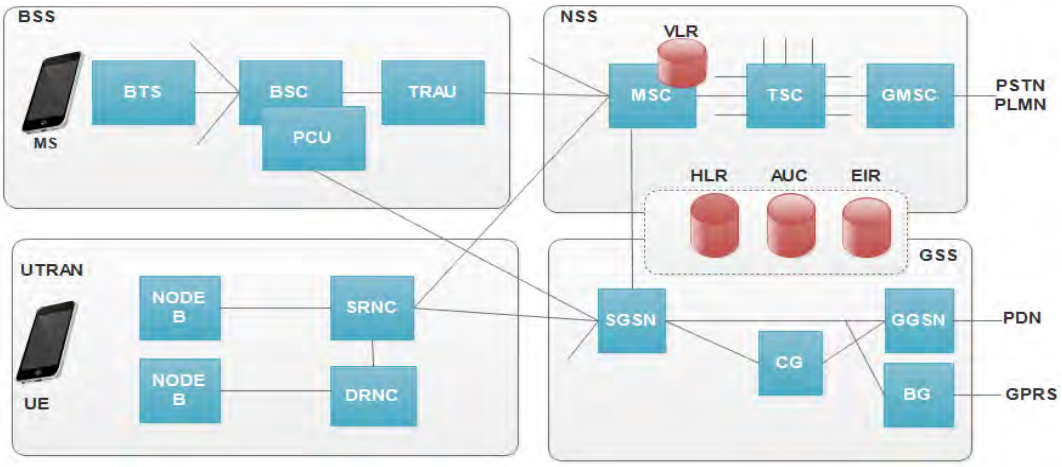


Figure 1.7 Architecture physique détaillée du réseau UMTS

1.3.3. Synthèse de l'étape 3

Dans cette troisième étape des réseaux mobiles, le réseau **UMTS** ouvre la voie à la vidéo. En plus de la transmission de la voix et des données, elle permet dřeffectuer la visiophonie et la diffusion de contenus vidéo sur des terminaux compatibles et mobiles. LřUMTS a ouvert la porte aux applications mobiles multimédias. La quatrième étape des réseaux mobiles est décrite ci-dessous

1.4. Quatrième étape de l'évolution de réseaux mobiles

Lřévolution du cœur de réseau NSS de lřUMTS vers une architecture **NGN (***Next Generation Network***)** (voir figure 1.8) a marqué cette quatrième étape. Lřarchitecture NGN permet une séparation des fonctions de transport du trafic téléphonique et de traitement de la signalisation. Lřinterconnexion des machines de lřentité NSS est assurée par le réseau SDH. Cependant, lřinterconnexion des équipements du **réseau NGN** est mise en œuvre par **un réseau de données IP** qui est identique à celui du sous-système GSS capable : de gérer tous les types de flux (Data, Vidéo, Voix …), dřoffrir une qualité de service spécifique à la demande, dřoptimiser les ressources disponibles, dřavoir une gestion et une maintenance

uniforme du réseau, dřassurer lřinterconnexion avec les réseaux existants et dřajouter des services sophistiqués (Multimédia, Interactif, …).

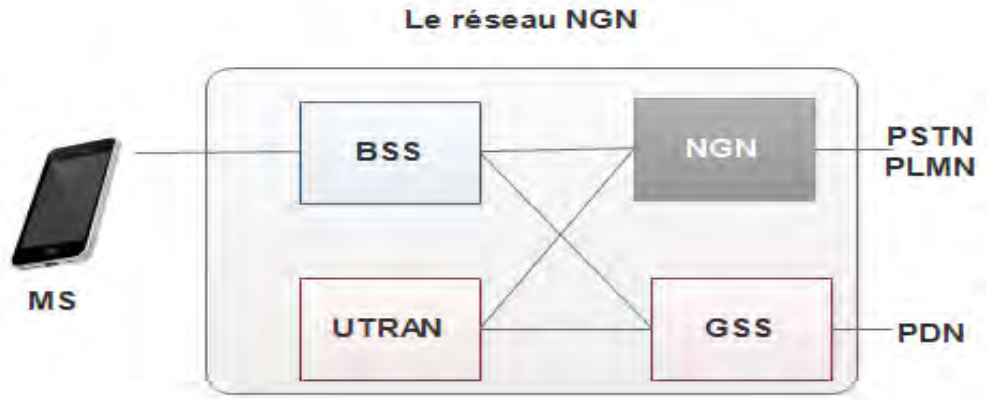


Figure 1.8. Réseau NGN

Cette séparation des fonctions ci-dessus permet dřassurer la fourniture de services auxquels lřutilisateur peut souscrire chez lřopérateur afin dřêtre servi lors de lřétablissement dřune communication. Les composantes de lřarchitecture du réseau NGN sont détaillées ci-dessous.

1.4.1. Les composants de lřarchitecture du réseau NGN

Les nœuds MSC et GMSC (*Gateway MSC*) sont décomposés en deux entités : le **MSC Server** ou le **GMSC Server** et les passerelles **MGW** (*Multimédia Gateway*). Lřarchitecture physique du réseau NGN est détaillée ci-dessous (figure 1.9) :

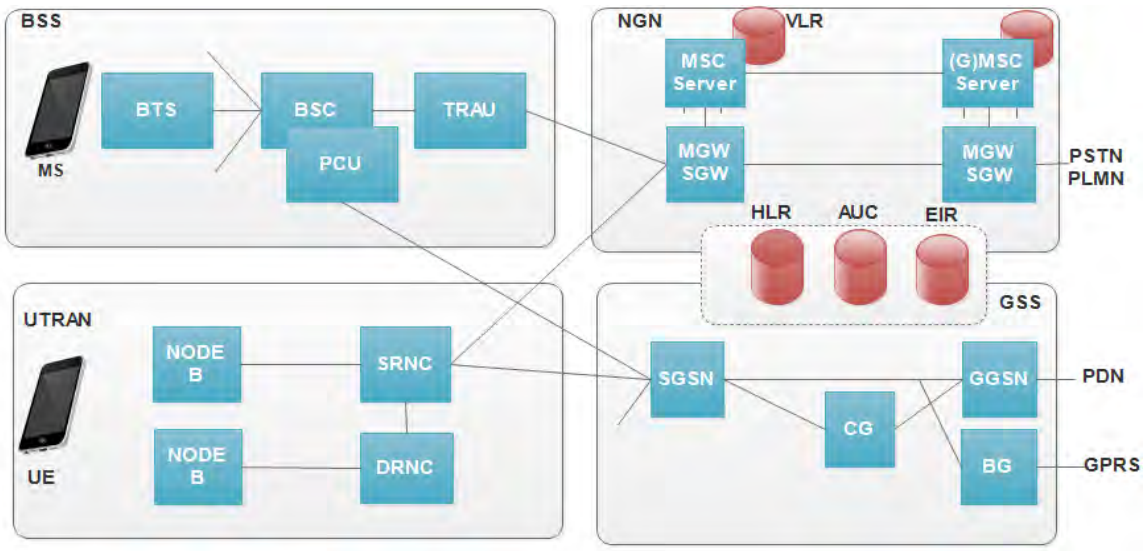


Figure 1.9. Architecture physique détaillée du réseau NGN

Le MSC Server assure le traitement des fonctions de gestion de la communication et de la mobilité. Comme le MSC, il est associé à la base de données **VLR** afin de prendre en compte les données des mobiles stockées dans la base de données **HLR**. Le MSC Server peut contrôler plusieurs **MGW/SGW**. Il nřeffectue uniquement que le traitement de la signalisation.

Le GMSC Server assure la fonction particulière correspondant au traitement dřun appel entrant. Le MSC Server assure lřétablissement, le maintien et la libération des connexions dans le MGW. Une connexion représente une association entre une terminaison en entrée (par exemple lřinterface avec les réseaux dřaccès ou les réseaux tiers) et une terminaison en sortie (par exemple lřinterface avec le réseau de données IP) et inversement. La passerelle MGW effectue la conversion de protocoles relatifs aux flux multimédia entre les deux terminaisons. Il contient les traitements effectués sur les flux média, comme le transcodage (modification du type de codec entre les deux terminaisons), lřannulation dřécho, lřémission des tonalités et des annonces. La passerelle SGW effectue la conversion de protocoles de transport relatifs à la signalisation échangée entre, dřune part le MSC Server et dřautre part les réseaux dřaccès et les réseaux tiers [1]. Un certain nombre de services déployés dans le réseau NGN est décrit ci-dessous.

1.4.2. Les services

Lřévolution vers les réseaux NGN, fondés sur des technologies de transmission haut débit avec des garanties en matière de QoS, a permis de supporter des types variés de services tels que **la voix, la vidéo et les données**. La variété des services envisageables dans les réseaux de nouvelle génération est due aux multiples possibilités quřils offrent en termes de média, de mode de communication, de mobilité, de réseaux dřaccès et de terminaux. Ces services incluent les **services IP traditionnels** comme **le mail** et **le web**, mais aussi des services émergents comme : la **voix sur IP** (VoIP : *Voice over IP*), la **diffusion de la télévision sur IP** (*IPTV*), et les applications fondées sur **la présence** tels que la **messagerie instantanée** (*Instant Messaging*) et les **services de localisation** (*Location-Based Services*).

1.4.3. Synthèse de l'étape 4

LřUMTS est le premier système qui inclut dans ses spécifications une évolution vers lřarchitecture du futur : le **NGN**. Il constitue une évolution du cœur du réseau NSS. Le protocole unificateur IP dans le réseau NGN, a facilité lřinteropérabilité et ouvert le système aux services à valeur ajoutée. La cinquième étape des réseaux mobiles est décrite ci-dessous.

1.5. Cinquième étape de l'évolution de réseaux mobiles

La cinquième étape est marquée par le **réseau EPS** (*Evolved Packet System*). Son architecture de base est constituée de deux sous-systèmes : le **réseau d'accès eUTRAN** (*Evolved UTRAN*), le **cœur de réseau EPC** (*Evolved Packet Core*) et des mobiles **UE** (*User Equipment*) (figure 1.10).

Figure 1.10. Réseau de base EPS

Les composantes de son architecture physique détaillée sont décrites ci-dessous.

1.5.1. Les composants de l'architecture du réseau EPS

Le réseau EPS est constitué dřun cœur de réseau EPC et dřun réseau dřaccès eUTRAN.

Le cœur de réseau EPC :

Il comprend lřentité de traitement de la signalisation **MME** (*Mobility Management Entity*), les entités de transfert des données **SGW** (*Serving Gateway*) et **PGW** [*PDN (Packet Data Network) Gateway*], les bases des données du mobile **HSS** (*Home Subscriber Server*) et **EIR** (*Equipment Identity Register*), puis lřentité **PCRF** (*Policy and Charging Rules Function*)

définissant les règles de qualité de service et de taxation (figure 1.11) [1] [7]. Le cœur de réseau EPC présente les différences suivantes par rapport au cœur de réseau GSS des réseaux de mobiles 2G et 3G :

- une entité spécifique **MME** est responsable de lřéchange de la signalisation avec le mobile et avec le réseau dřaccès. Dans le cas des réseaux 2G et 3G, ces fonctions sont réalisées par le **SGSN** (*Service GPRS Support Node*) ;
- deux points dřancrage (**SGW** et **PDW**) sont créés. Dans les réseaux 2G et 3G, le seul point dřancrage est assuré par le **GGSN** (*Gateway GPRS Support Node*).

Le réseau d'accès eUTRAN :

Il est simplifié et comprend un seul type dřentité, la station radioélectrique **eNode B. eNode B** intègre les fonctions précédemment dévolues aux contrôleurs de stations BSC des réseaux 2G et RNC des réseaux 3G (figure 1.11). Lřentité eNode B est responsable de la gestion des ressources radioélectriques, du contrôle de lřallocation du support au mobile, et de sa mobilité. Elle effectue la compression et le chiffrement des données sur lřinterface radioélectrique. Elle route aussi les données du mobile vers lřentité SGW et effectue pour les données sortantes, le marquage des paquets IP en fonction de la qualité de service affectée au support [1] [7] [8].

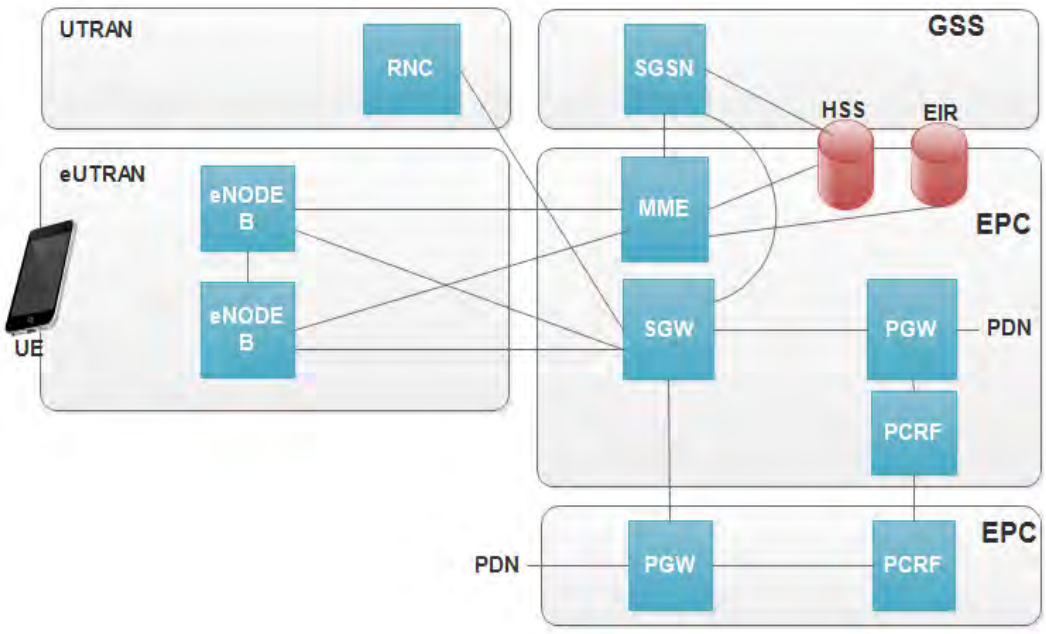


Figure 1.11. Architecture physique détaillée du réseau EPS

Cette architecture permet la mise en œuvre des services décrits ci-dessous.

1.5.2. Les services

Le réseau EPS présente la particularité par rapport aux réseaux GSM/GPRS et UMTS de ne proposer quřun **service de transmission de données en mode paquet PS** (*Packet Service*), dont la caractéristique principale est lřaugmentation du débit maximal [1].
Pour la fourniture dřun **service téléphonique**, le réseau EPS ne produit que le transport de la voix et de la signalisation, considérées comme des données. Le traitement de la signalisation et de la voix est effectué par le réseau IMS (*IP Multimedia Subsystem*), externe au réseau de mobiles. Le réseau EPS transfère seulement les paquets IP contenant de la **voix** ou de la **vidéo** (flux RTP, *Real Time Protocol*) ou de la signalisation téléphonique (flux SIP, *Session Initiation Protocol*). Le service téléphonique ou visiophonique est fourni par le réseau IMS qui assure les fonctions suivantes : le routage de lřappel, les compléments de service téléphonique ou visiophonique et lřinterconnexion vers les réseaux tiers, téléphoniques ou visiophoniques.

1.5.3. Synthèse de l'étape 5

La cinquième étape a été dominée par lřaccès au réseau par E-UTRAN et le cœur de réseau assuré par lřEPC. Lřintroduction du réseau IMS, externe aux réseaux mobiles, permet dřinterconnecter le réseau EPS aux réseaux tiers. Manifestement, cette favorable transition va nous conduire à la sixième étape décrite ci-dessous.

1.6. Sixième étape de l'évolution de réseaux mobiles

Dans la sixième étape, la tendance tire vers les RCS (*services de riches communications*). Les RCS définissent un ensemble de services que les opérateurs de réseau peuvent fournir grâce à lřarchitecture IMS, notamment les appels vocaux et vidéo, la messagerie instantanée, etc…Lřentité nouvelle qui a été rajoutée par rapport au réseau EPS (*4G*) (figure 1.10) est : lř**IMS** (figure 1.12). Lřarchitecture de base des réseaux mobiles de la sixième étape est présentée par la figure 1.12 :

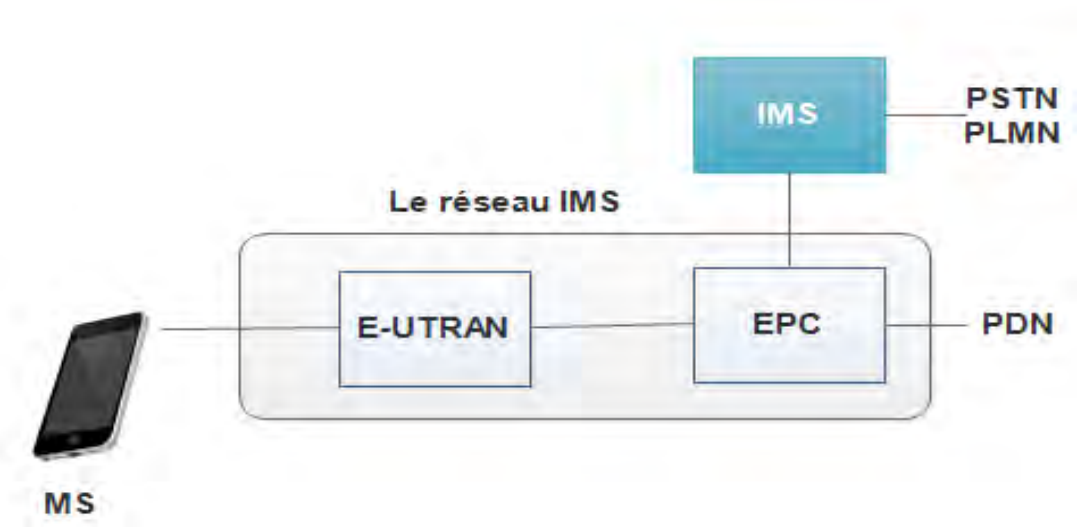


Figure 1.12. Réseau IMS

L'IMS est une partie structurée de l'architecture des réseaux de nouvelle génération (*NGN*) qui permet l'introduction progressive des applications voix et données multimédia dans les réseaux fixes et mobiles. L'IMS inter-fonctionne avec tous types de réseaux (fixe, mobile ou sans fil), incluant les fonctions de commutations de paquets, comme le GPRS, lřUMTS, CDMA 2000, WLAN, WiMAX, DSL, le câble… Les plus anciens systèmes de commutation de circuit (POTS, GSM) sont aussi supportés par lřIMS grâce à des passerelles (*Gateways*). Des interfaces ouvertes entre les couches de contrôle et les couches de service, permettent de mélanger les appels/sessions de différents réseaux dřaccès [9]. LřIMS utilise les technologies cellulaires pour fournir un accès en tout lieu, et les technologies Internet pour fournir les services.

L'architecture IMS est constituée par un ensemble d'équipements et de protocoles dont les fonctions et les rôles se complètent. Les interfaces sur les différentes liaisons internes et externes à cette architecture font également l'objet des spécifications évolutives. Le principe de l'IMS consiste, d'une part à séparer nettement la couche transport de la couche des services et d'autre part à utiliser la couche transport pour des fonctions de contrôle et de signalisation afin d'assurer la qualité de service souhaitée pour l'application désirée. L'IMS a pour ambition de constituer une **plate-forme unique** pour toute une gamme de services et d'être en mesure **d'offrir de nouvelles applications en un temps minimum**. LřIMS vise, à faire du réseau une sorte de **couche middleware** entre les applications et l'accès. Les applications sont soit SIP, soit non SIP, elles passent alors par une passerelle avant la connexion au contrôleur de sessions [1] [14]. Le réseau de la sixième étape, assure le transport du trafic téléphonique,

assimilé à des données. Le traitement de la signalisation qui administre le service téléphonique est pourvu par lřIMS qui est une entité externe au réseau de mobiles. IMS est indépendante du réseau qui effectue le transport de données.

1.6.1. Les composantes de l'architecture du réseau IMS

A partir du réseau EPS représenté par la figure 1.10, une entité nouvelle a été rajoutée : **le réseau IMS** (voir figure 1.12). Le réseau IMS permet dřinterconnecter le réseau EPS vu ci-dessus aux réseaux téléphoniques fixes PSTN (*Public Switched Telephone Network*) ou aux réseaux mobiles PLMN (*Public Land Mobile Network*). Il permet de faire converger le réseau EPS (4G), les réseaux téléphoniques fixes PSTN et les réseaux mobiles PLMN. Son architecture détaillée est présentée par la figure 1.13 et sera développée dans le chapitre 4, vu son importance dans les systèmes de communication actuels.

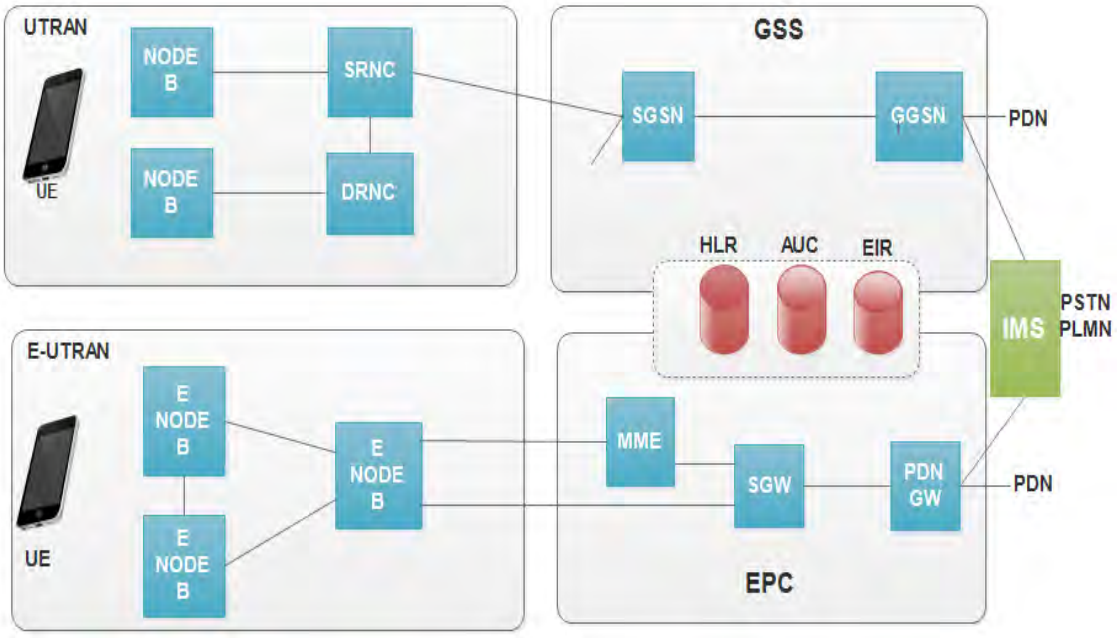


Figure 1.13. Architecture physique détaillée du réseau IMS

1.6.2. Les services

En effet, lřIMS est considéré aujourdřhui comme le socle de la sixième étape pour fournir de nouveaux services et de faire converger tous les moyens de communication existants : réseaux mobiles, réseaux fixes et Internet. Les réseaux mobiles fonctionnant en mode paquet PS (Packet Service) effectuent uniquement le transport de paquet IP. De ce fait, il transfère seulement les paquets IP contenant de la voix ou de la signalisation téléphonique.

En revanche, le traitement de la signalisation qui offre le service téléphonique, est fourni par **l'IMS (***IP Multimedia Subsystem***)**, une entité externe au réseau de mobiles (figure 1.12). LřIMS fournit les **services multimédias (téléphonie, visiophonie, données)**. Son architecture est constituée dřun ensemble de fonction en charge de traitement de la signalisation SIP/SDP et du média. Le traitement du flux média concerne les fonctions indisponibles dans le réseau des mobiles comme la conférence et les passerelles vers les réseaux téléphoniques fixes PSTN et les réseaux mobiles PLMN [1].

Ainsi, la convergence voix, données et images est devenue une réalité technique et commerciale. Les deux piliers de cette convergence sont dřune part le protocole Internet (*IP*) et dřautre part le très haut débit. IP sřimpose comme protocole unificateur des réseaux de nouvelle génération (*NGN*). Les entreprises et les opérateurs migrent à marche forcée vers de réseaux de nouvelle génération. Cette migration est destinée à procurer des gains de performances ; elle prend en compte les possibilités offertes par cette nouvelle plateforme unifiée, capable de diffuser aux consommateurs des services plus puissants, plus riches, mais aussi plus rapides à mettre en place et plus facile à gérer. Le très haut débit notamment sur fibre optique sřimpose partout car lui seul peut offrir de nouveaux services convergents avec une qualité requise. Après sřêtre définitivement imposée dans les cœurs de réseaux, le très haut débit est parti à la conquête de lřaccès. Les déploiements se multiplient (*FTTH*) et les nouveaux acteurs contribuent largement à ce succès.

LřIMS est le véritable relais de croissance de lřunivers IP. Cřest une architecture normalisée, définie par des instances internationales réunissant les opérateurs, les équipementiers et les représentants de la communauté IP, apte à favoriser les applications commerciales dřIP. LřIMS superpose une intelligence à IP, en permettant la création, le contrôle et lřexécution de nouveaux services multimédias enrichis. Quřil sřagisse de services dřutilisateur à utilisateur, dřutilisateur à serveur ou multi-utilisateurs, **IMS est la solution**.

LřIMS révolutionne la création de services car son adoption implique de désassembler les éléments des réseaux traditionnels pour les réassembler dans une architecture différente, plus efficace, bâtie autour dřun ensemble de technologies à base de standards. De plus, la 4G est la génération des standards pour la téléphonie mobile. Le **WiMAX (IEEE802.16e)** permet dřélargir la couverture cellulaire tout en offrant un débit supérieur. Il fournit un accès Internet à très haut débit pour les appareils mobiles.

Les deux (2) tableaux ci-dessous résument les six (6) étapes de lřévolution des réseaux mobiles (générations, caractéristiques et débits etc..) :

Tableau 1.5. Les six (6) étapes des réseaux mobiles

LES SIX (6) ETAPES DE L'EVOLUTION DES RESEAUX MOBILES										
Etapes	**1ère étape**	**2ème étape**		**3ème étape**				**4ème étape**	**5ème étape**	**6ème étape**
Réseau	**2G**			**3G**				**4G**		
	GSM	**GPRS**	**EDGE**	**UMTS**	**HSDPA**	**HSUPA**	**HSPA+**	**NGN**	**EPS**	**IMS**
CN	NSS	GSS	GSS	NSS et GSS	GSS	GSS	GSS	NGN	EPC	IMS
AN	BSS	BSS (évolution)	BSS (évolution)	UTRAN	UTRAN (évolution)	UTRAN (évolution)	UTRAN (évolution)	UTRAN (évolution)	E-UTRAN	E-UTRAN

Légende

CN : Core Network	**UTRAN** : UMTS TRAnsport Network
AN : Access Network	**NGN** : Next Generation Network
BSS : Base Station Sub-system	**EPS** : Evolved Packet System
NSS : Network Sub-System	**EPC** : Evolved Packet Core
GSS : GPRS Sub-System	**IMS** : IP Multimedia Subsystem

Le tableau 1.5 montre le résumé des six (6) différentes étapes de lřévolution des réseaux mobiles depuis la 2G à la 4G. Il fait référence aussi à lřévolution du réseau dřaccès et le cœur de réseau depuis la 2G jusqřà la 4G.

Tableau 1.6. Recapitulatif des architectures des réseaux mobiles : Débits et services

Générations	**Réseau**	**Sous-ensembles réseaux**		**Mode**	**Débit**	**Observations sur le Débit**	**Services**
		CN : Cœur du réseau	**AN : Réseau d'accès**				
2G	GSM	NSS	BSS	CS	14,4kbits/s		Digital voice SMS Grande Capacité en paquet de données
	GPRS	GSS	BSS (Evolution du BSS)	PS	171,2kbits/s		
	EDGE	GSS	BSS (Evolution du BSS)	PS (CS peu utilisé)	473,6kbits/s	Débit utilisé par PS	

3G	UMTS	NSS	UTRAN	CS	64kbits/s		Haute Qualité audio Vidéo et data intégrés
		GSS		PS	384kbits/s		
	HSDPA	GSS	UTRAN (Evolution dřUTRAN)	PS	14,4Mbits/s	Débit sens descendant	
	HSUPA	GSS	UTRAN (Evolution dřUTRAN)	PS	5,76Mbits/s	Débit sens montant	
	HSPA+	GSS	UTRAN (Evolution dřUTRAN)	PS	43,2Mbits/s	Débit sens descendant	
					11,5Mbits/s	Débit sens montant	
4G	EPS	EPC	E-UTRAN	PS	302Mbits/s	Débit sens descendant	Accès dynamique à lřinformation, Objets connectés
					75Mbits/s	Débit sens montant	

Le tableau 1.6 montre le récapitulatif des architectures des réseaux mobiles : Débits et services. Le tableau présente les différentes générations de réseaux mobiles qui se sont succédées, les réseaux et sous-ensemble réseaux (réseaux dřaccès et cœur de réseau) déployés, le mode de circuit utilisé (commutation de circuit et commutation de paquet) et les trois (3) dernières colonnes du tableau indiquent lřévolution de différents débits requis pour écouler normalement le trafic souhaité en fonction de différents services à offrir.

1.6.3. Synthèse de l'étape 6

Les réseaux de télécommunications mobiles ont connu une rapide évolution à cause des exigences des utilisateurs en matière de service et aussi de la croissance rapide du nombre dřutilisateurs qui découvrent ces services quřoffrent les opérateurs de téléphonie

Depuis la première étape jusquřà la sixième étape, le réseau GSM était le premier réseau mobile avec les entités BSS et NSS qui ont permis dřoffrir les services de voix et de données avec un débit relativement faible pour les données. Cřest ce qui a montré les limites de GSM en commutation de circuits.

A la deuxième étape, une nouvelle entité le GSS sřest rajoutée au réseau GSM pour réaliser le réseau GPRS afin de rendre possible lřaccès à Internet par le mobile.

A la troisième étape le réseau dřaccès UTRAN sřest rajouté au réseau GPRS pour permettre en plus de services de voix, de données, de fournir des appels vidéo avec des débits allant de 144 kbits/s à 2 Mbits/s, cřest le réseau UMTS.

A la quatrième étape, lřévolution du cœur de réseau NSS vers une architecture NGN dont lřinterconnexion des équipements du réseau NGN est mise en œuvre par un réseau des données IP pour offrir des services voix, vidéo, données, IPTV, applications sur la présence (*messagerie instantanée*) et services de localisation.

A la cinquième et sixième étape, toute lřarchitecture a été révolutionnée, le réseau dřaccès devient lřE-UTRAN et le cœur de réseau est lřEPC. Le réseau EPS offre uniquement un service de transmission de données en mode paquets PS. Lřintroduction du réseau IMS qui est externe aux réseaux mobiles, interconnecte le réseau EPS (*4G*) aux réseaux tiers. LřIMS est lřancrage pour la convergence des réseaux existants de télécommunications.

Ces évolutions sřorientent vers la transmission de données avec des débits de plus en plus élevés et du Tout-IP. La migration vers le Tout-IP, lřinteropérabilité entre les réseaux fixes, mobiles et même Internet a été possible. Les terminaux mobiles sont de plus en plus performants, donnant plus de fonctionnalités aux usagers, alors que le réseau deviendra de plus en plus intelligent et simple pour satisfaire aux besoins pressants des utilisateurs. Les réseaux de nouvelle génération offrent une connectivité mondiale transparente indépendamment du type de réseau, du dispositif utilisé, à tout moment et en tout lieu. Le passage dřune architecture traditionnelle basée essentiellement sur la commutation de circuits vers une nouvelle architecture basée sur IP constitue un changement majeur dans le secteur de technologies dřinformation et de communication (*TIC*), gage de lřémergence numérique.

Le but principal du système IMS est dřoffrir aux opérateurs une architecture de service multimédia standard. Il est basé sur le protocole IP pour le transport de données et le protocole SIP (*Session Initiation Protocol*) pour la signalisation et le contrôle de session. LřIMS constitue le socle des systèmes convergents de télécommunications, ce qui justifie **son importance dans les réseaux mobiles, fixes et Internet.** Les efforts fournis durant les six (6) différentes étapes démontrent lřévolution des réseaux mobiles vers le réseau IMS, un véritable réseau de convergence.

Le chapitre 2 qui suit montre lřévolution des systèmes de signalisation (**SS7**, **SIGITRAN**, **SIP**) utilisés dans les réseaux de télécommunications et leur importance ; lřexemple dřinterconnexion du réseau fixe de la SONATEL nous édifie.

Chapitre 2 : L'évolution des systèmes de signalisation et de gestion des profils utilisateurs dans les réseaux de télécommunications

La signalisation est lřune des plus importantes fonctions dans lřinfrastructure des télécommunications puisquřelle permet aux composants du réseau de communiquer entre eux pour établir et terminer des appels. Elle permet le transfert des informations concernant la gestion du réseau et les ressources, la taxation, etc…

Dans le réseau téléphonique classique, le fonctionnement du réseau sřappuie sur le protocole **SS7** (*Signalisation System 7)*. Lors de la modernisation du réseau téléphonique en réseau numérique, la signalisation était toujours assurée par le protocole SS7. Il a migré vers le protocole IP nommé **SIGTRAN**.

Dans le nouveau contexte, le service de télécommunications est devenu une application informatique sřexécutant dans un environnement et sur des composants hétérogènes. Ainsi, les nœuds du réseau PSTN sont répartis et échangent entre eux, au moyen de SS7. Au niveau informatique, deux grandes approches de la VoIP sont standardisées : **H323** issue de lř**ITU** (*International Telecommunication Union*) et **SIP** proposée par la communauté Internet au travers de lř**IETF** (*Internet Engineering Task Force*). Elles ont en commun la définition dřune procédure de signalisation permettant lřétablissement, le contrôle et la terminaison dřappels téléphoniques. Elles facilitent lřintégration des communications de type téléphonique au sein des services variés en émergeant lřInternet comme réseau de transport de données multimédia, comme plateforme de développement dřapplications et de services de télécommunication. H323 a été abandonné au profit du SIP à cause des avantages de SIP pour les systèmes convergents. Ce chapitre va décrire les différentes signalisations qui ont existé depuis la SS7 jusquřà SIP en passant par SIGTRAN et enfin, nous terminerons ce chapitre par une synthèse.

2.1. Le principe de base de la signalisation

Pour réaliser le transfert des données, il est nécessaire dřétablir une liaison, de la superviser durant lřéchange et enfin de libérer les ressources monopolisées en fin de communication. La signalisation au sein dřun réseau de télécommunications fait référence à lřensemble des échanges dřinformation entre les équipements du réseau, indispensables pour fournir et

maintenir le service. Les informations de la signalisation sont acheminées sous forme des paquets de données à débit élevé. La signalisation peut être transmise de deux manières : **la signalisation dans la bande (*in band*)** et **la signalisation hors-bande ou canal dédié (*out band*)**.

La signalisation dans la bande : les signaux dřétablissement dřun appel entre deux commutateurs sřeffectuaient toujours dans le même canal que le transport de la voix (réseau téléphonique traditionnel).

La signalisation hors bande : La conversation et la signalisation ne prennent pas le même canal. Ce type de signalisation nécessite lřétablissement dřun canal numérique appelé canal sémaphore. Les canaux sémaphores de signalisation véhiculent les informations avec de débits de 56 kbits/s aux Etats Unis ou 64 kbits/s pour les autres pays. La signalisation hors-bande a plusieurs avantages qui la rendent préférable à la signalisation dans la bande.

Dans ce système, on distingue différents types de signalisation :

- ✓ **La signalisation entre usager et le réseau** : chargée de lřétablissement de la liaison usager/réseau et de sa supervision ;
- ✓ **La signalisation entre les nœuds du réseau** : permet lřétablissement dřune liaison à travers le réseau (routage ou acheminement) et de la contrôler durant lřéchange ;
- ✓ **La signalisation entre les usagers du réseau** : dite de bout en bout, cette signalisation permet aux entités distantes de sřéchanger des informations hors protocoles de transmission.

La signalisation des différentes communications sur un support est acheminée par un canal dédié appelé **signalisation voie par voie** ou **CAS** (*Channel Associated Signalling*). Elle peut aussi être acheminée dans un canal commun à toutes les voies de communication : cřest la **signalisation par canal sémaphore** ou **CCS** (*Common Channel Signalling*). Ainsi, le réseau téléphonique commuté (***RTCP***) utilise une signalisation de **type CAS**, alors que le réseau téléphonique à intégration de service (***RNIS***) met en œuvre une signalisation de **type CCS** [6] [18].

2.2. Signalisation SS7 et son architecture

La **SS7** est un standard global de télécommunication définie par lřUIT. Elle définit les procédures et protocoles par lesquels les éléments du réseau à commutations de circuits,

sřéchangent des informations de contrôle et de routage sur un réseau digital de signalisation. Elle est utilisée pour : lřétablissement et la gestion des appels, les services mobiles comme le roaming, la portabilité des numéros, les services intelligents (0800, 0900…), les services de transfert (call forwarding).

Son **architecture** est décrite ci-dessous :

Le réseau SS7 fonctionne en mode paquets ; les terminaux sémaphores sont appelés **PS** (*Point Sémaphores*) et les commutateurs de paquets **PTS** (*Points de Transfert Sémaphores*). Le **PLMN (***Public Land Mobile Network***)** comporte deux réseaux : le réseau sémaphore pour la signalisation (mode paquet) et le réseau de transmission de la parole (mode circuit). En effet, dans le réseau SS7, les centraux téléphoniques qui génèrent et interprètent les messages de signalisation sont appelés Points Sémaphores (**PS**). Les nœuds dřacheminement sont le cœur du réseau SS7 qui est lřensemble des Points de Transfert Sémaphore (**PTS**). Chaque point de signalisation a un numéro unique appelé « **Point Code** ». Ces numéros sont utilisés pour connaître les destinataires et émetteurs des messages. Il existe des tables de routage qui permettent un choix du meilleur chemin pour émettre les messages, pour joindre la destination. Il existe trois types de point de signalisation [6] [18] :

Les **SSP** (*Service Switching Point*) sont des commutateurs qui envoient des messages de signalisation à dřautres SSP pour démarrer, gérer et arrêter un circuit vocal. Ils lancent des requêtes vers les bases de données centralisées comme les SCP pour déterminer comment router un appel. Le trafic réseau entre les points de signalisation peut être routé via des commutateurs STP. Un **STP** (*Signalling Transfer Point*) route chaque message entrant vers un lien de signalisation sortant, sur la base de lřinformation de routage contenue dans le message.

Les **SCP** (*Service Control Point*) sont les bases de données qui fournissent lřinformation nécessaire aux fonctions avancées de traitement des appels (voir figure 2.1). Il existe six (6) différents types de canaux sémaphores qui sont catalogués dřA à F [6] [18].

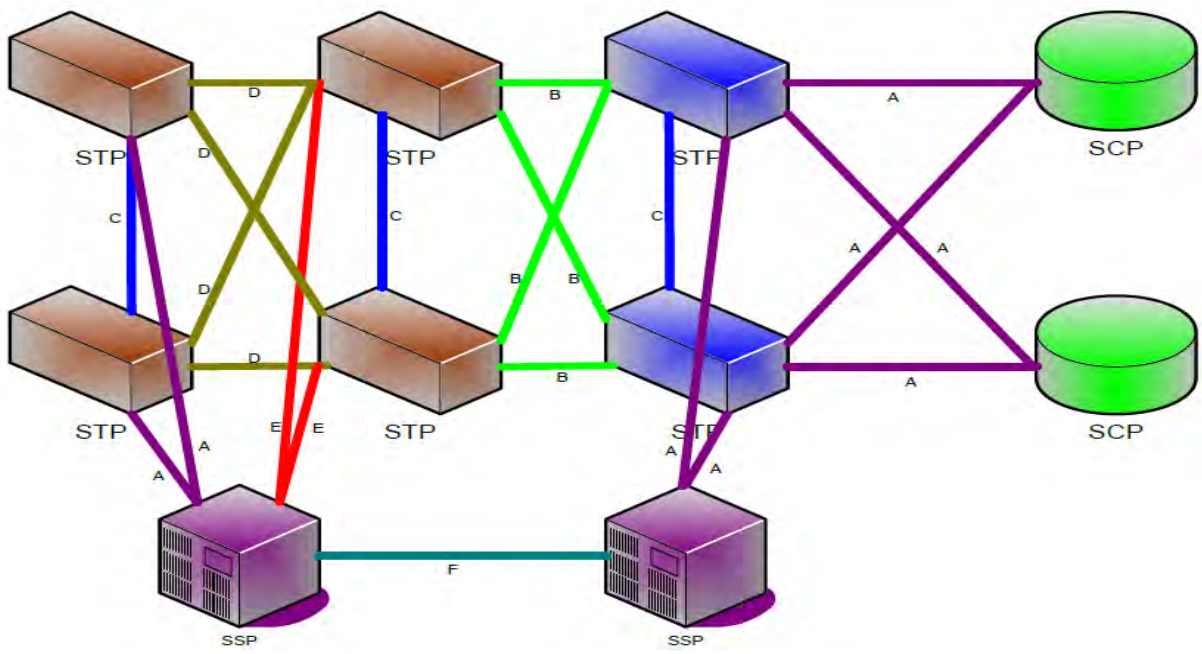


Figure 2.1. Architecture : Points et liens de Signalisation SS7, cas du GSM [18]

Les applications courantes de SS7 sont : la gestion des appels de base (*établissement, maintenance, rupture*), la gestion de la mobilité dans les réseaux GSM (*roaming, identification, authentification et localisation des usagers mobiles*), lřacheminement de messages courts (SMS), les applications RI (Réseau Intelligent), la gestion de numéros spéciaux (toll-free (800/888) & toll (900), les services complémentaires (transfert dřappels, conférence à 3, …), la gestion de réseaux privés virtuels (*VPN*), la portabilité de numéros (local number portability - LNP) et la gestion de cartes prépayées.

2.3. Réseaux intelligent

Le concept de RI (***Réseau Intelligent)*** consiste à séparer, dřune part, les fonctions propres à chacune des applications ou services et, dřautre part, les traitements communs à toutes les applications (décroché, attente de numérotation), gérés par les centraux téléphoniques (*SSP*). Les traitements spécifiques aux services sont intégrés dans des SCP qui sont des ordinateurs capables dřéchanger des messages de signalisation avec les SSP. Le concept de réseau intelligent permet de définir et développer des services, indépendamment des particularités des différents commutateurs du réseau. La conception de nouveaux services est plus rapide et moins coûteuse. Lorsque lřutilisateur demande un service de type RI, le SSP et le SCP

échangent, en temps réel, des messages de signalisation non liés à un circuit. Les réseaux intelligents sřappuient donc naturellement sur SS7. La SS7 est appliquée aux interfaces avec le réseau dřaccès BSS, ainsi quřaux interfaces avec les réseaux tiers. SIGTRAN est utilisé sur les interfaces internes au réseau NGN, entre les entités SGW et MSC Server. La conversion entre la SS7 et le SIGTRAN est effectuée par lřentité SGW. Dans le paragraphe qui suit, nous verrons la migration de SS7 vers IP (SIGTRAN).

2.4. Migration de la signalisation SS7 vers la signalisation sur IP : SIGTRAN

Le **SIGTRAN** (**SIG**naling **TRAN**sport) est un groupe de Travail de lřIETF ayant comme objectif de définir une architecture pour le transport des données de signalisation en temps réel à travers les réseaux IP. Cřest une partie des réseaux de la nouvelle génération basée sur le protocole IP (figure 2.3). Il a été conçu pour lřacheminement du trafic de signalisation tel que SS7, RNIS, et tous les réseaux NGNs utilisant les avantages du SS7, à travers les réseaux IP. La **signalisation SS7 sur IP** appelée **SIGTRAN,** définit un protocole de transport fiable **SCTP** (*Stream Control Transmission Protocol*) et une couche dřadaptation des utilisateurs UA (*User Adaptation*) permettant de transporter des protocoles de signalisation téléphonique sur IP. La pile de protocole SIGTRAN est définie dans la référence **RFC 2719**. Le SCTP est un protocole TCP de la nouvelle génération. Il permet de remédier aux problèmes liés à lřutilisation du protocole TCP puisque ce dernier est un protocole orienté octets et nřest pas capable de fournir la vitesse et la fiabilité requises par la signalisation. En effet, le SCTP est un protocole orienté message permettant de définir des trames de données structurées alors que TCP nřimpose aucune structure des octets transmises. Le nom Stream Control Transmission Protocol découle de la fonction **multi-streaming** fournie par le SCTP. Un stream (flot) est un canal logique unidirectionnel permettant lřéchange de messages entre terminaisons SCTP. Lors de lřétablissement dřune association SCTP, il est nécessaire de spécifier le nombre de streams que comportera cette association. La fonction multi-streaming permet de partitionner les données dans différents streams de telle sorte que la perte dřun message dans un des streams nřait dřimpact sur le transport des données que sur ce stream. Une des fonctionnalités principales du protocole SCTP est le **multi-homing**, cřest à dire la capacité pour un endpoint SCTP de supporter plusieurs adresses IP. Ceci est un avantage comparé à TCP. Une connexion TCP est définie par une paire dřadresses de transport

(Adresse IP + numéro de port TCP). Chaque endpoint dřune association SCTP fournit à lřautre extrémité une liste dřadresses IP avec un unique numéro de port SCTP. Lřendpoint est donc lřextrémité logique du protocole de transport SCTP [6] [7] [18].

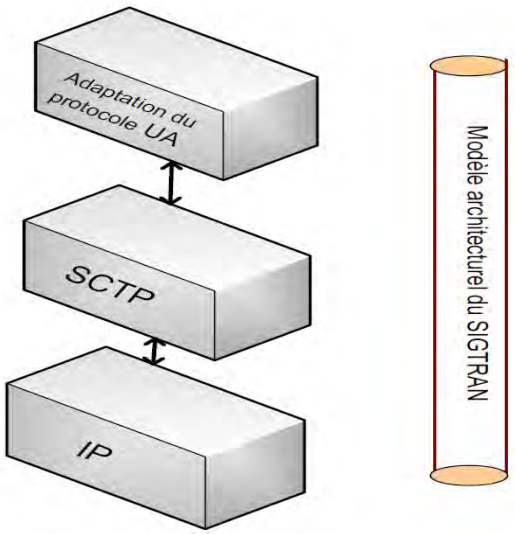


Figure 2.2. Composants de SIGTRAN [18]

2.4.1. Les couches d'adaptation SIGTRAN

Les couches dřadaptation définies par SIGTRAN ont toutes des objectifs communs : le transport des protocoles de signalisation des couches supérieures, basé sur un transport IP fiable. La garantie dřune offre de services est équivalente à celle proposée par les interfaces des réseaux RTC et la transparence du transport de la signalisation sur un réseau IP : lřutilisateur final ne se rend pas compte de la nature du réseau de transport [6] [7] [18]. Les différentes couches dřadaptation SIGTRAN sont montrées sur la figure 2.3.

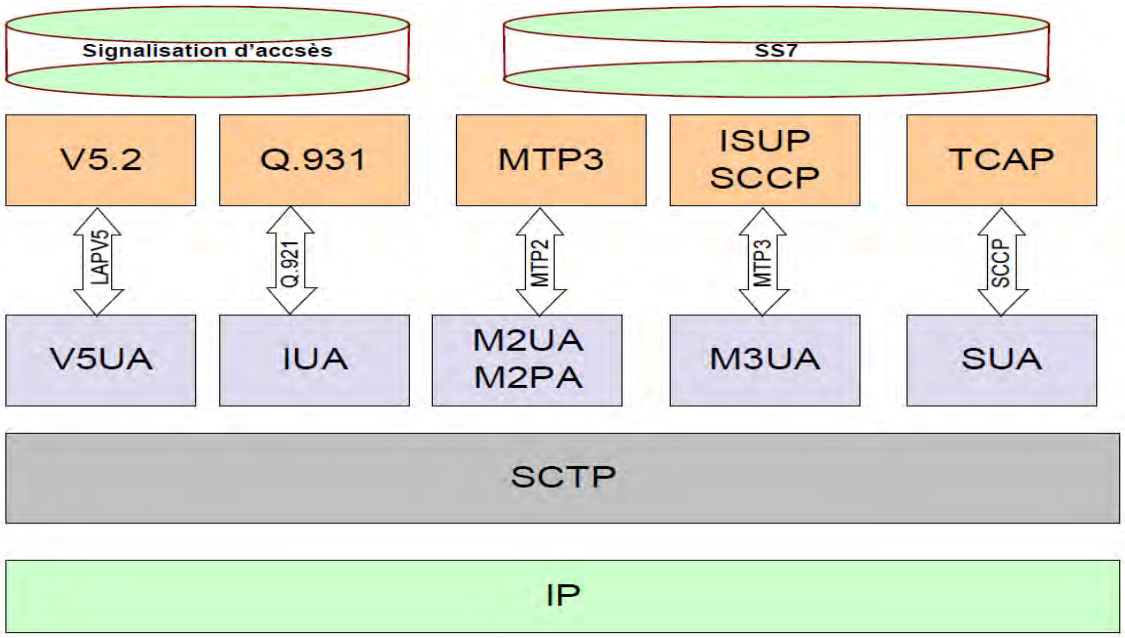


Figure 2.3. Les couches d'adaptation SIGITRAN [18]

2.4.2. Architecture SS7 d'interconnexion de la SONATEL

Lřexemple dřinterconnexion utilisée par lřarchitecture SS7 de la SONATEL (figure 2.4) montre trois types dřinterfaces de liaisons disponibles pour relier les PTS avec les différents équipements du réseau à savoir : les liaisons de type **LSL** (*Low Speed Signalings Links*), avec un débit de 64 kbit/s, interconnectent le réseau international et les équipements du réseau national aux PTS, les liaisons de type **HSL** (*High Speed Signalings Links*) avec un débit théorique de 2 Mbits/s chacune, permettent dřinterconnecter des équipements comme le HLR, les bases de données du réseau intelligent aux PTS, enfin la liaison **SIGTRAN** permet de relier le MSC aux PTS via le réseau IP de la SONATEL.

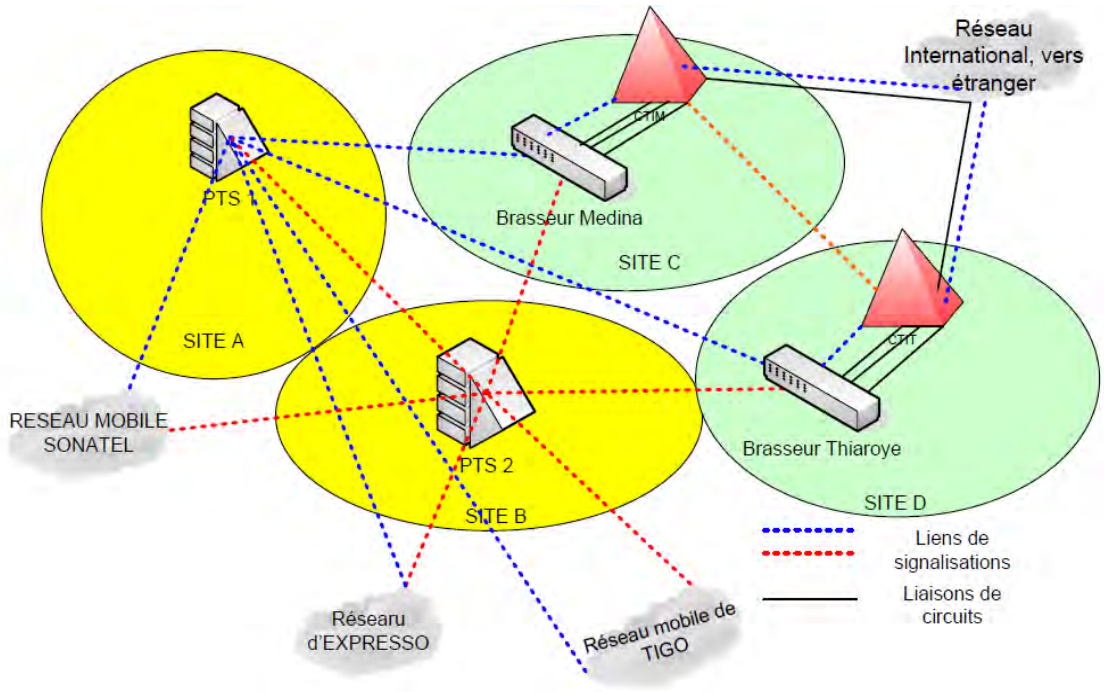


Figure 2.4. Architecture SS7 de l'interconnexion [18]

Ainsi, la SS7 a migré vers IP (SIGTRAN) où IP est devenu un protocole unificateur de tous les réseaux. Nous abordons le protocole SIP le plus utilisé dans tous les réseaux de la nouvelle génération pour établir une connexion pour la communication [18].

2.5. Le protocole SIP

Le protocole SIP (*Session Initiation Protocol*) est un protocole de signalisation défini par lřIETF (*Internet Engineering Task Force*) [21] et permet dřétablir, de libérer et de modifier des sessions multimédias (**RFC 3261**). Le protocole **SIP** [21] [22] [23] s'est imposé aujourdřhui sur ses concurrents, tant chez les opérateurs de téléphonie que dans le monde de l'entreprise, voire chez les particuliers. Le choix du SIP comme protocole de signalisation dans l'architecture IMS (*IP Multimedia Subsystem*), les IP-PBX actuels offrent aujourd'hui pratiquement tout une interface SIP. Microsoft, dans son OS grand public, a introduit SIP dans sa suite Office Live Communication Server. Dans le contexte de la Téléphonie IP, le SIP a remplacé H.323 et SS7. Il facilite l'intégration des communications de type téléphonique au sein des services variés en émergeant lřInternet comme réseau de transport de données

multimédia et comme plateforme de développement dřapplications, et des services de télécommunication [19]. Le SIP a été aussi retenu pour l'UMTS par le groupe 3GPP, afin de permettre un transport de la voix et des applications multimédia en temps réel sur un réseau paquet dans le monde mobile. Il est également déployé par la plupart des opérateurs pour être le protocole le plus utilisé dans le cadre de l'évolution du réseau vers le NGN. Le SIP sřappuie sur le modèle client/serveur comme les protocoles classiques tels que le HTTP (*Hyper Text Transport Protocol*) et le SMTP (*Simple Mail Transport Protocol*) pour lesquels, il hérite de certaines fonctionnalités. Il utilise un système dřadressage basé sur des URL (*Uniform Resource Locator*) similaires au serveur de messagerie. Aussi, il dispose dřextensions supportant de nombreux services tels que la présence, le transfert dřappel, la conférence, les services additionnels de la téléphonie classique et la messagerie instantanée. Des messages courts non relatifs à un appel peuvent toutefois être transportés par le SIP de la même manière quřun SMS classique. Le Professeur Samuel OUYA et al. (Ouya et al. 2015) ont proposé une approche de SMS basé sur le protocole SIP. [24]. Les RFC consacrés à SIP sont les suivants :

- Premier RFC sur SIP : **RFC 2543** ŔMars 1999**.**
- Version actuelle : **RFC 3261** (juin 2002) Ŕ269 pages Ŕplusieurs fois étendue**.**
- En Mars 2009 : **82 RFC** contiennent SIP dans leur titre (prise en compte de la sécurité, diversité des flux multimédia, diversité des réseaux et protocoles de transport…)

Le protocole SIP est représenté principalement par la **RFC 3261** « SIP : Session Initiation Protocol » qui est complété par l'ensemble des RFC suivantes :

- **RFC 3265**, "Session Initiation Protocol (*SIP*)-Specific Event Notification".
- **RFC 3853**, "S/MIME Advanced Encryption Standard (*AES*) Requirement for the Session Initiation Protocol (*SIP*)".
- **RFC 4320**, "Actions Addressing Identified Issues with the Session Initiation Protocol's (*SIP*) Non-INVITE Transaction".
- **RFC 4916**, "Connected Identity in the Session Initiation Protocol (*SIP*)".
- **RFC 5393**, "Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies".

2.5.1. Transactions SIP

Avant lřinitialisation dřune session SIP, lřutilisateur est localisé sur le réseau avec une adresse URI (Uniform Resource Identifier). Les terminaux impliqués dans une session SIP doivent donc sřidentifier par cet URI qui définit une syntaxe permettant de désigner de manière unique, formelle et normalisée une ressource, quřil sřagisse dřun document textuel, audio ou vidéo. Le format dřun URI se présente de la manière suivante :

sip : identifiant [: pwd]@adresse_serveur [?paramètre]

- Le mot-clé ***sip*** spécifie le protocole à utiliser pour la communication ;
- La partie ***identifiant*** définit le nom ou le numéro de lřutilisateur ;
- La partie ***pwd*** est facultative. Elle est obligatoire lorsquřon veut sřauthentifier auprès dřun serveur ;
- La partie ***adresse_serveur*** spécifie le serveur chargé du compte SIP dont lřidentifiant précède lřarobase. Le serveur est spécifié par son adresse IP ou par un nom qui sera résolu par le DNS (*Domaine Name System*) ;
- La partie ***paramètre*** est facultative. Les paramètres permettent soit de modifier le comportement par défaut (par exemple, en modifiant les protocoles de transport ou les ports, ou encore la durée de vie par défaut dřune requête).

En outre, le protocole SIP utilise les protocoles TCP et UDP pour acheminer des requêtes de signalisation. De ce fait, si aucun protocole de transport nřest précisé dans lřURI de la requête, le protocole UDP est utilisé par défaut.

2.5.2. Méthodes et réponse SIP

Pendant lřinitialisation dřune session SIP entre deux terminaux, les méthodes suivantes sont définies par le RFC 3261 et échangées lors de la mise en relation de lřappelant et de lřappelé :

INVITE : Invite le terminal SIP dřun utilisateur à participer à une session.

ACK : Confirme que lřappelant a reçu une réponse à sa requête INVITE.

BYE : Met fin à une connexion entre utilisateurs ou lorsque le terminal refuse lřinvitation à participer à une session.

CANCEL : Annule une requête.

OPTIONS : Sollicite du Proxy Server afin quřil précise ses capacités à contacter le terminal de lřappelé.

REGISTER : cřest une méthode utilisée par le client pour enregistrer lřadresse listée dans le paramètre TO de lřURL par le serveur auquel il est relié. Les requêtes sont traitées par le client de manière ordonnée pour éviter lřenvoi de nouvelle requête REGISTER tant quřil nřaura pas traité la précédente. Le client doit définir une adresse dřenregistrement du type utilisateur@domaine. Cette méthode assure également un service de localisation [21] [22].

Le type des réponses aux requêtes envoyées dans les transactions SIP sont décrites dans le tableau 2.1 :

Tableau 2.1. Codes d'état

Code	Description
1XX	Réponses informatives, la requête a été reçue par le destinataire et est en cours de traitement (exemple : 180=řen train de sonnerř).
2XX	Succès, exemple : 200= Řokř, 202 = Řacceptéeř
3XX	Redirection, une autre action doit avoir lieu afin de valider la requête.
4XX	Erreurs du client, la requête contient une syntaxe erronée ou bien elle peut être traitée par ce serveur.
5XX	Erreurs du serveur, le serveur nřa pas réussi à traiter une requête.
6XX	Échec général, la requête ne peut être traitée

2.5.3. Architecture SIP

Lřarchitecture du protocole SIP (figure 2.5) sřarticule autour de cinq entités :

- **Le terminal :** lřutilisateur dispose de cet élément pour appeler ou être appelé. Celui-ci peut être un téléphone physique ou un téléphone logiciel encore appelé « *softphone* ». Le terminal a deux composants :
  - Lř**UAS** (*User Agent Server*) : il représente lřagent de la partie appelée. Cřest une application de type serveur qui contacte lřutilisateur lorsquřune requête SIP est reçue, puis renvoie une réponse au nom de lřutilisateur ;
  - Lř**UAC** (*User Agent Client*) : il représente lřagent de la partie appelante. Le client initie les appels et le serveur répond aux appels initiés par ce dernier.

- **Le serveur proxy** : il se charge de la localisation de lřutilisateur appelé. Il initie, maintient et termine une session vers un correspondant. Il agit à la fois comme un client et comme un serveur. Au besoin, il interprète et modifie les messages quřil reçoit avant de les transmettre.
- **Le serveur de redirection** : il agit comme un intermédiaire entre le terminal client et le serveur de localisation. LřUAC le sollicite pour contacter le serveur de localisation afin de déterminer la position courante dřun utilisateur.
- **Le serveur de localisation** : il permet de localiser lřutilisateur et contient la base de données de lřensemble des utilisateurs quřil gère. Cette base est mise à jour par le serveur dřenregistrement.
- **Le serveur d'enregistrement** : il enregistre les terminaux SIP lors de lřenvoie de la méthode **REGISTER**. Il offre la possibilité de localiser un correspond aisément tout en gérant sa mobilité [21].

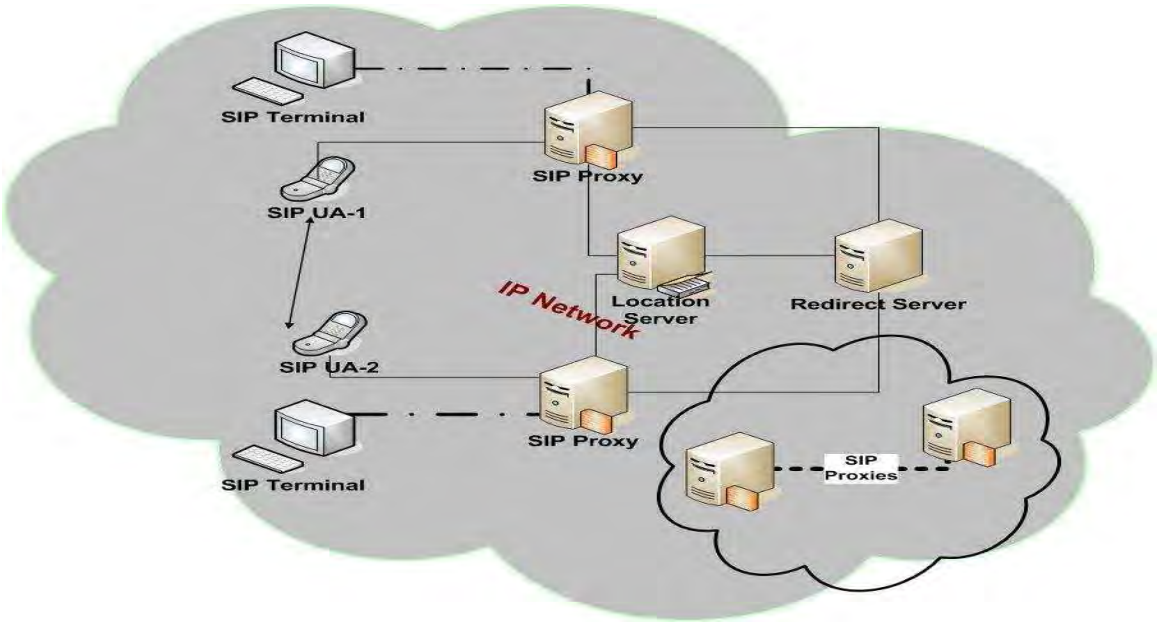


Figure 2.5. Architecture SIP

2.5.4. Apport de SIP dans la mutualisation des ressources

Beaucoup de travaux ont montré lřintérêt du protocole SIP pour le réseau IMS. Ainsi, le protocole SIP peut être envisagé dans la perspective dřintégration des environnements

dřapprentissage dans un réseau IMS [24]. Le SIP constitue un atout du fait de sa capacité à sřintégrer à dřautres protocoles standards du monde IP. En tant que standard ouvert, il offre un service modulaire, prévu pour fonctionner avec différentes applications, telles que la téléphonie, la messagerie instantanée, la vidéoconférence, la réalité virtuelle [24].

Le Session Description Protocol Ŕ **SDP** est un élément dřun message SIP. Le **protocole SDP** (*Session Description Protocol*) fournit une description du flux média pour lequel lřétablissement de la session est mis en œuvre par le protocole SIP. Le **SDP** est un élément dřun message SIP qui décrit les caractéristiques de qualité de service échangées entre deux (2) extrémités à lřétablissement dřune session IMS. Les paramètres SDP incluent le type de média (voix, audio, vidéo, etc.…), les codecs (G.711, etc.), la bande passante demandée, le type de flux, etc… Le SDP définit les protocoles multimédias dans la **RFC 2327**. Le message SDP constitue le corps de message attaché au message SIP. Il apparait généralement dans la requête INVITE et dans la réponse 200 OK. Les paramètres qui caractérisent le flux média sont les suivantes : le type de média (audio, vidéo, données), le protocole de transport (par exemple RTP), le format du média (par exemple le type de codec pour la voix et la vidéo), lřadresse IP à laquelle le média doit être transmis et le numéro du port de destination.

Le **SIP** demeure un protocole puissant utilisé dans lřétablissement de la connexion mais le protocole **DIAMETER** est utilisé dans lřenregistrement des caractéristiques de lřabonné en vue de permettre la communication. LřIMS se base sur une entité très importante, le HSS une base de données dřenregistrement de profils des abonnés. Il y a des transactions entre cette base HSS et certaines entités de lřIMS pour authentifier les abonnés grâce au protocole DIAMETER. Ce protocole est décrit dans les paragraphes ci-dessous.

2.6. Le protocole DIAMETER

Le protocole DIAMETER est défini dans le :

- **RFC 4004** DIAMETER Mobile IPv4 Application ;
- **RFC 4005** DIAMETER Network Access Server Application ;
- **RFC 6733** DIAMETER Extensible Authentication Protocol Application (*EAP*) ;
- et **RFC 4740** pour DIAMETER SIP Application.

Le mécanisme dřauthentification dans le réseau IMS sřappuiera sur le **RFC 4740** (*DIAMETER SIP Application*), néanmoins une brève présentation du protocole DIAMETER de base sera faite afin de comprendre le format dřéchange des messages DIAMETER.

2.6.1. Le protocole DIAMETER de base

Le DIAMETER est un protocole avancé dans l'architecture du sous-système multimédia IP (IMS) et les réseaux LTE afin de fournir des débits de données plus élevés dans le réseau et fournir des services **AAA** (*Authentication Authorization Account*) [25]. Il a été défini pour gérer lřauthentification des utilisateurs sur un réseau. Il sřagit dřun protocole AAA et repose sur le protocole **RADIUS** (*Remote Authentication Dial In User Service*). Cřest une application standardisée par le 3GPP qui permet dřinterfacer avec les différentes entités du réseau IMS. Les échanges DIAMETER sont toujours du type un message requête et une réponse associée (figure 2.6). Il définit un ensemble de commandes et de pair dřattributs de valeurs (*AVP*) pour gérer lřauthentification, lřautorisation et évidemment la facturation dans un contexte donné [25] [26] [27].

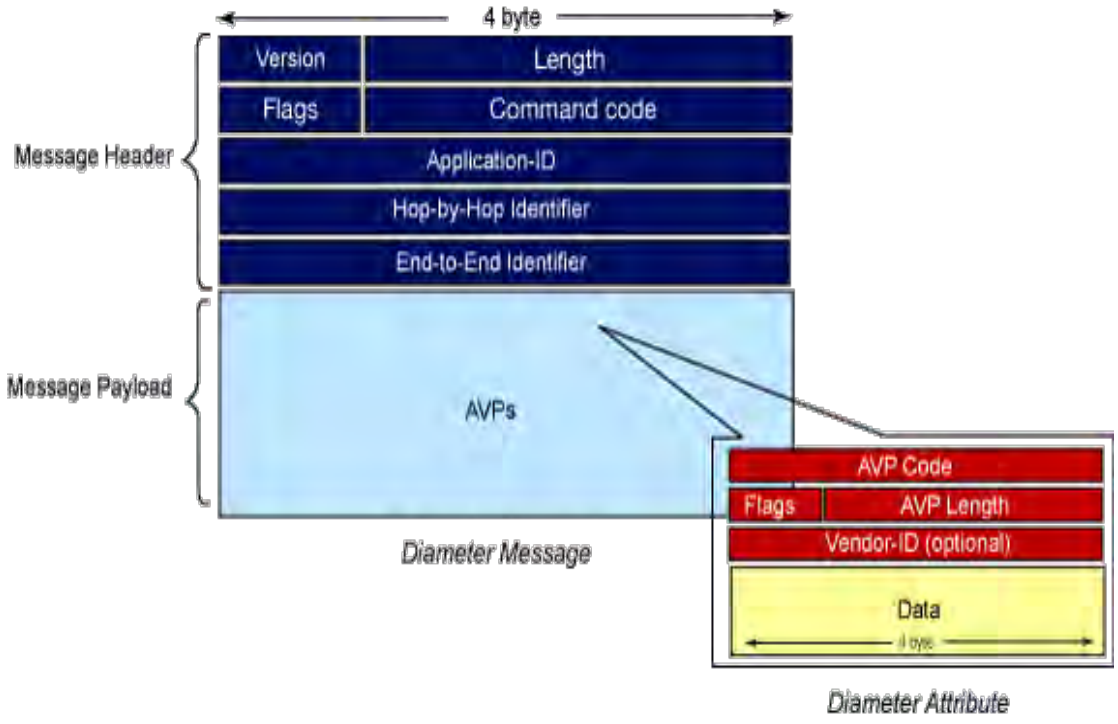


Figure 2.6. Format d'un message Diameter

Une architecture DIAMETER est composée de différents nœuds appelés « **Agents DIAMETER** ». Chaque nœud a une tâche bien définie. Ils forment un réseau dit « **pair-à-pair** ».

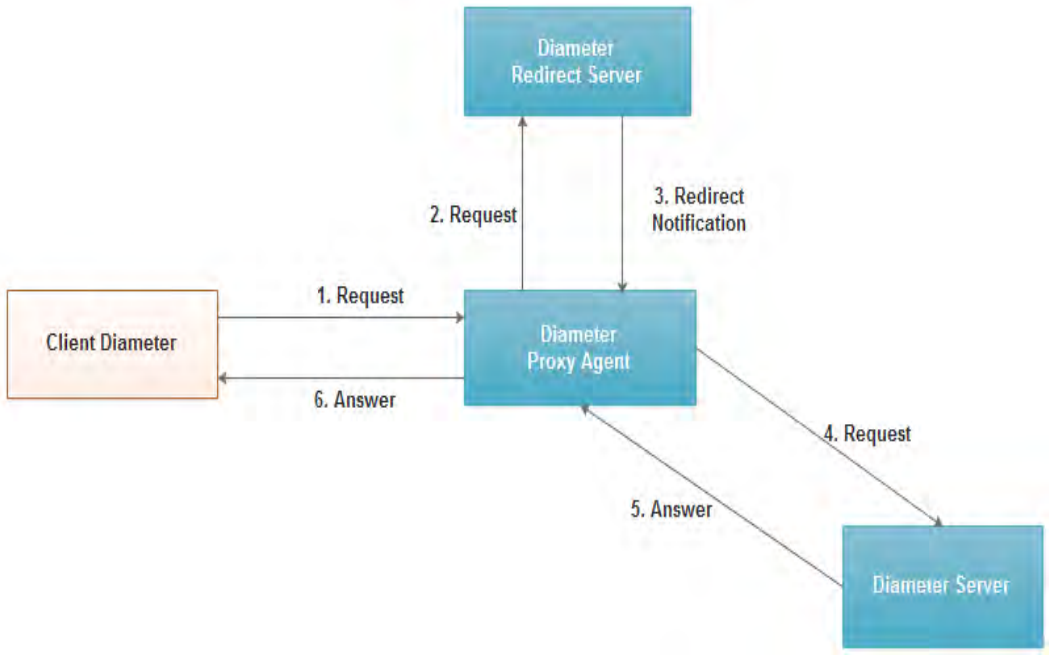


Figure 2.7. Architecture DIAMETER de Base

- ✓ **Client DIAMETER** : il est un nœud à la frontière du réseau, contrôle lřaccès ;
- ✓ **DIAMETER Proxy Agent** : cřest un agent relais, route le message DIAMETER. Toutefois, un agent Proxy peut modifier les messages afin de réaliser un contrôle dřaccès, un contrôle de politiques, etc. Exemple agent proxy : le **PCRF** de LTE **;**
- ✓ **DIAMETER Redirect Server** : il est un agent de redirection qui fournit aussi une fonction de routage. Il sert de directory permettant la traduction du nom de domaine et adresse du serveur. A la différence des autres types dřagent (relais et proxy) qui acheminent les messages DIAMETER, lřagent de redirection retourne un type particulier de réponse à lřémetteur de la requête. La réponse contient lřinformation de routage afin que lřémetteur puisse retransmettre son message directement au serveur destinataire. Exemple dřagent de redirection : le **SLF** dans lřarchitecture IMS ;
- ✓ **DIAMETER Server** : il prend en charge les demandes dřauthentification, dřautorisation et de taxation pour un domaine donné. Exemple de serveur : le **HSS** [26]**.**

Lorsque le client et le serveur DIAMETER se trouvent dans le même domaine, le DIAMETER Proxy Agent redirige la requête dřauthentification directement vers le serveur. Dans ce cas, le chemin de la réponse est 1-4-5-6. Cependant lorsque le client et le serveur DIAMETER se trouvent dans deux domaines différents, un serveur de redirection centralise lřensemble des routes connues, le chemin de la réponse devient 1-2-3-4-5-6 (Figure 2.7).

2.6.2. Le DIAMETER SIP Application et son architecture

Le DIAMETER SIP Application :

Elle est définie dans le **RFC 4740,** permet à un client DIAMETER de demander les informations dřauthentification et d'autorisation à un serveur DIAMETER pour les services multimédia IP SIP.

De plus, cette application fournit au client DIAMETER des fonctions qui lui permettent de télécharger ou de recevoir des profils d'utilisateurs, les mises à jour ou des fonctions de routage qui peuvent aider un serveur SIP à trouver un autre serveur SIP alloué à l'utilisateur.

Ce paragraphe décrit les procédures DIAMETER pour implémenter certaines fonctionnalités requises lorsque le protocole SIP est désigné pour ouvrir et supprimer des sessions multimédias ou lorsque SIP est utilisé pour d'autres applications non liées à la session.

Dřaprès le RFC, aucun mappage particulier nřest prévu entre les procédures SIP et les requêtes SIP DIAMETER. Cependant, il fournit des exemples utiles pour montrer l'interaction entre SIP et l'application DIAMETER SIP afin d'atteindre les fonctionnalités souhaitées **[27].**

L'architecture du DIAMETER SIP Application :

Le DIAMETER SIP Application peut être utilisée dans un environnement SIP où une interface pour une infrastructure AAA est nécessaire dřauthentifier et dřautoriser l'utilisation des ressources SIP. Cette application fournit un support pour les agents utilisateurs SIP et les proxy qui implémentent et utilisent l'authentification HTTP Digest [28], qui est le mécanisme d'authentification requis par le protocole SIP [21]. Elle fournit un support limité pour les services de facturation comme suit : le serveur DIAMETER est capable de fournir les adresses des agents de facturation au client DIAMETER. La figure 2.8 montre un aperçu général de l'intégration de l'architecture SIP avec l'architecture AAA.

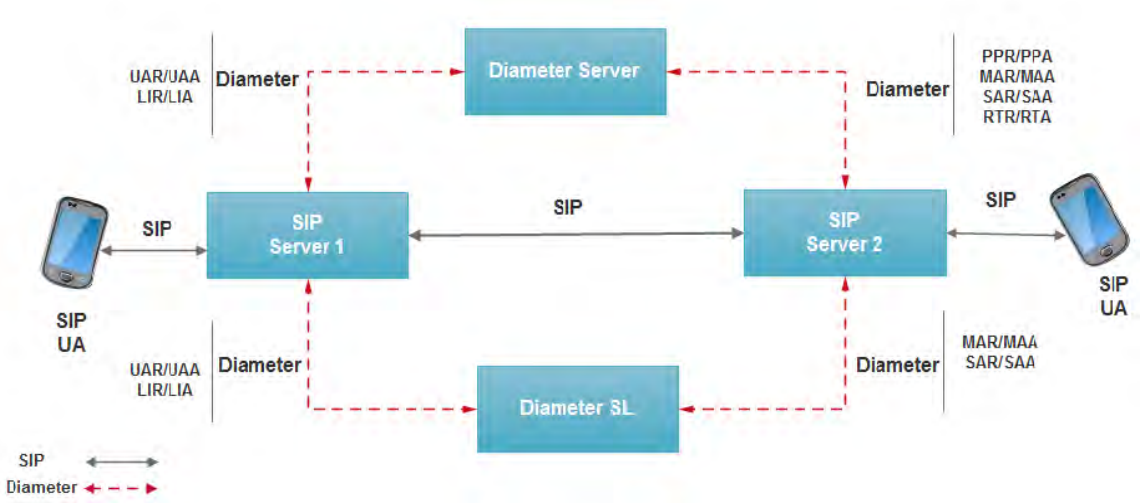


Figure 2.8 Architecture générale SIP DIAMETER Application

Dřaprès la figure 2.8, le SIP server 1 envoie différentes commandes DIAMETER et reçoit des réponses différentes de celles envoyées et reçues par le SIP server 2. Ceci est dû au fait que le serveur SIP 1 de la figure 2.8 se trouve au bord d'un réseau et la tâche principale consiste à localiser le serveur SIP 2 (deux domaines différents). Les fonctions du DIAMETER SL peuvent être incluses dans les fonctions du DIAMETER Server afin de simplifier lřarchitecture.

- **SIP UA** : le client SIP qui permet à un utilisateur dřémettre ou de recevoir des appels y compris les fonctions de messagerie. Il sřagit dřun terminal utilisateur ;
- **SIP Server 1** : il utilise le protocole SIP qui sert à lřouverture, lřétablissement et la libération des sessions multimédia incluant la téléphonie. Il sert aussi à lřinvocation des plateformes de services IMS [21] ;
- **DIAMETER SL** : cřest le serveur de localisation DIAMETER. Il contient les données relatives à l'utilisateur. Il contient une base de données ou des tables de routage qui mappent les URI SIP aux URI du serveur DIAMETER ;
- **SIP server 2** : il demande et reçoit des données d'authentification et d'autorisation du serveur DIAMETER et n'est pas situé au bord du réseau ;
- **DIAMETER Server** : il réalise lřauthentification des utilisateurs en fonction des paramètres fournis pour lřauthentification [29].

2.6.3. Processus d'authentification SIP DIAMETER Application

Ce diagramme de la figure 2.9 montre le mécanisme générique permettant d'authentifier les utilisateurs [27], [30]. Il sřagit dans ce diagramme dřun réseau administratif où le serveur DIAMETER authentifie les demandes des utilisateurs SIP. Le cas mis en évidence est celui dřune requête SIP REGISTER et donc dřautres requêtes peuvent également être présentées au besoin.

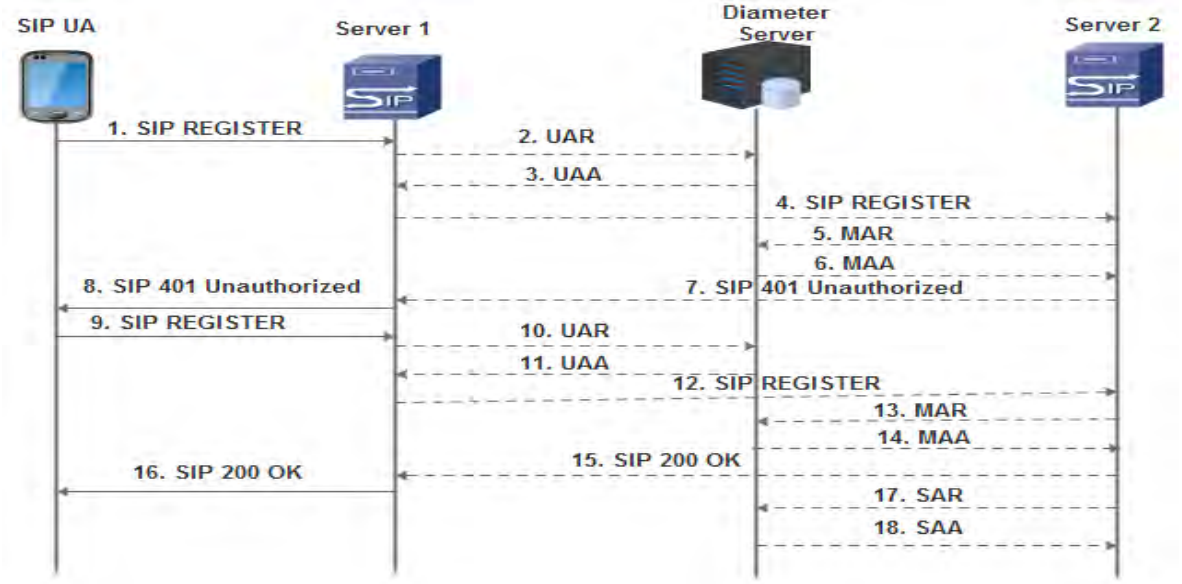


Figure 2.9. Authentification SIP DIAMETER Application

La figure 2.9 montre le processus générique dřauthentification dřutilisateur basé sur le support SIP DIAMETER. Dans ce processus, on suppose que le serveur SIP 1 est situé au bord dřun domaine administratif. Il reçoit une requête SIP REGISTER du SIP UA et le transmet au DIAMETER server via un message UAR pour déterminer si cet utilisateur est autorisé à recevoir un service ou non. Dans certaines architectures, un serveur SIP est alloué dynamiquement au client, cřest le cas de lřarchitecture IMS.

La figure 2.10 montre le mécanisme dřauthentification dans lřIMS.

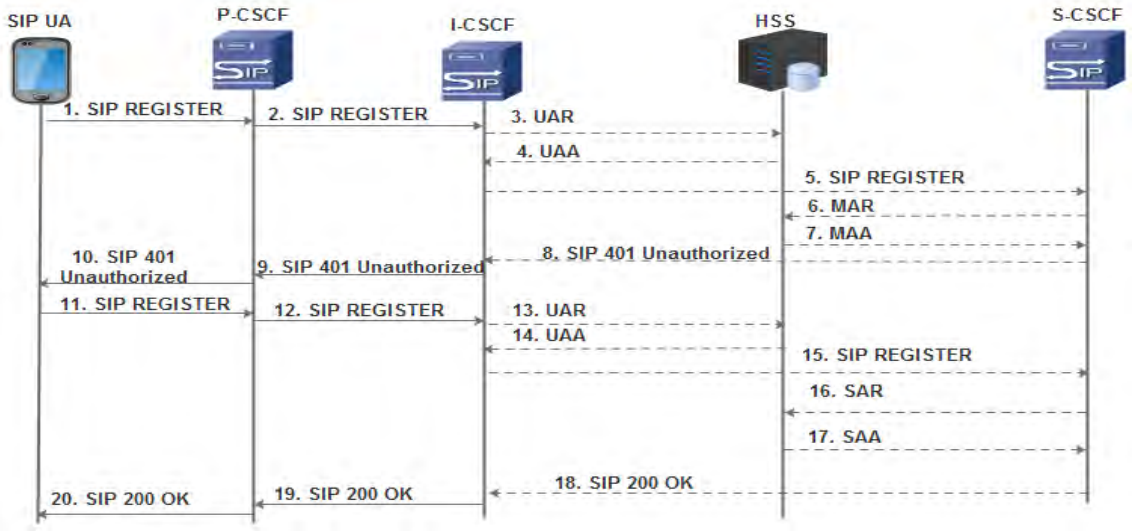


Figure 2.10. Processus d'authentification utilisateur dans le réseau IMS

La procédure dřenregistrement explique les différentes étapes dřaccès au réseau IMS qui permet à un SIP UA de se déclarer joignable de point de vue service IMS. Comme toute autre procédure dřaccès, le terminal sera authentifié par le réseau IMS et son profil sera chargé dans le S-CSCF nominal qui est une sorte de central de rattachement ou un MSC/VLR qui est alloué à lřutilisateur quel que soit sa localisation dans le monde. Le S-CSCF contient lřadresse du Proxy P-CSCF où le terminal est rattaché (équivalent à un BSC).

- Le SIP UA fournit ses paramètres de connexion dans une requête SIP REGISTER. Cette requête contient lřURI de son réseau domestique, ses identités publique et privée ainsi que lřadresse du terminal à partir duquel il souhaite sřenregistrer. Il transmet alors la requête SIP REGISTER au Proxy-CSCF sur lřinterface Gm/SIP **(étape 1)** ;
- Le Proxy-SCSF recevant la requête SIP REGISTER sur son interface Gm/SIP ajoute lřidentifiant du réseau visité : P-Visited-Network-ID et un en-tête PATH contenant son URI, puis transmet la requête à lřentité I-CSCF sur lřinterface Mw/SIP **(étape 2)** ;
- Lřentité I-CSCF reçoit la requête SIP REGISTER. Ensuite, le client DIAMETER dans ce serveur SIP, demande au serveur DIAMETER par le biais du support DIAMETER SIP Application, lřautorisation pour procéder à lřenregistrement en envoyant au serveur DIAMETER un **message UAR (étape 3)**. Ce message contient entre autres les AVP, le SIP Address-O-Record (*AOR*) inclus dans la requête SIP REGISTER. LřAOR contient les identités publique et privée plus lřID du réseau visité. Le serveur

DIAMETER vérifie le SIP AOR et, s'il s'agit d'un utilisateur défini, valide dans le réseau domestique, il autorise alors l'enregistrement à continuer **;**

- Le serveur DIAMETER répond avec un message DIAMETER User Authorization-Answer, qui informe le client DIAMETER / SIP sur le résultat de l'autorisation de l'utilisateur. Dans le cas d'une autorisation réussie, le **message DIAMETER UAA (étape 4)** indique l'adresse d'un serveur SIP local (dans ce cas de figure, il sřagit de lřadresse de lřentité S-CSCF) et / ou une liste de capacités que le serveur I-CSCF peut utiliser pour sélectionner un serveur S-CSCF approprié. Lorsque l'autorisation est réussie, le serveur I-CSCF transmet la requête SIP REGISTER **(étape 5)** (ayant reçu lřadresse du S-CSCF approprié) au serveur S-CSCF **;**
- Le client DIAMETER dans le serveur S-CSCF demande des paramètres d'authentification en envoyant un message DIAMETER Multimedia-Auth-Request (***MAR***) **(étape 6)** au serveur DIAMETER. Cette demande rend également le serveur DIAMETER au courant de l'URI SIP du serveur S-CSCF afin de renvoyer les demandes ultérieures du même utilisateur sur le même serveur. Le serveur DIAMETER répond avec un message DIAMETER Multimedia-Auth-Answer (***MAA***) **(étape 7)**, qui comprend le SIP URI du serveur S-CSCF, le nom de lřutilisateur ainsi que les autres vecteurs dřauthentification notamment l'algorithme d'authentification désigné associé à l'utilisateur. Entre autres, le message MAA comprend un Digest-HA1 AVP qui contient H (A1) tel que défini dans RFC 2617 [28]**,** et qui permet au client DIAMETER de calculer la réponse attendue. Ensuite, le client DIAMETER peut comparer cette réponse attendue avec la réponse au défi envoyé par l'UA SIP. L'absence de Digest-HA1 AVP dans MAA indique que l'authentification et l'autorisation ont lieu dans le serveur DIAMETER ;
- Le serveur S-CSCF crée une réponse SIP 401 **(étape 8)** en fonction des défis inclus dans le message MAA, y compris le matériel d'authentification requis par le SIP UA pour inclure les informations d'identification appropriées. Le serveur I-CSCF transmet la requête au client SIP UA (**étapes 9 et 10**) ;
- Le SIP UA prépare une nouvelle requête SIP REGISTER **(étape 11)** quřil transmet au serveur P-CSCF, celui-ci relaye la requête à lřentité I-CSCF. LřI-CSCF reçoit la prochaine requête SIP REGISTER contenant les informations d'identification utilisateur (**étape 12**). Étant donné quřil n'a pas besoin de conserver un état, grâce au

support SIP DIAMETER Application, il contacte le serveur HSS (*DIAMETER Server*) en envoyant un message **UAR** (**étape 13**) pour déterminer le serveur S-CSCF attribué à l'utilisateur. Le serveur HSS répond en envoyant l'URI SIP du S-CSCF dans un message **UAA (étape 14)** ;

- LřI-CSCF transmet la requête SIP REGISTER au serveur S-CSCF (**étape 15**). Le S-CSCF valide les informations d'identification en comparant la réponse fournie par le SIP UA avec la réponse attendue, calculée (basé sur le H (A1) reçu du serveur DIAMETER) ;
- Si les informations d'identification sont valides, le S-CSCF envoie un message DIAMETER Server-Assignment-Request (***SAR***) **(étape 16)** demandant au serveur HSS de confirmer l'achèvement de la procédure d'authentification et de confirmer l'URI SIP du S-CSCF qui sert actuellement l'utilisateur. Le message SAR DIAMETER sert également à demander que le serveur DIAMETER envoie le profil utilisateur au serveur S-CSCF. Le HSS répond avec un message DIAMETER Server-Assignment-Answer (***SAA***). Si la valeur AVP du code de résultat n'informe pas le S-CSCF d'une erreur, le message SAA peut inclure zéro ou plus de SIP-User-Data AVP contenant les informations que le S-CSCF a besoin pour fournir un service à l'utilisateur. Le S-CSCF insère dans une table appelé location le profil de lřutilisateur (**étape 17**) ;
- Le serveur S-CSCF génère une réponse « **SIP 200 OK** », qui est envoyée au serveur I-CSCF pour être éventuellement transmise au SIP UA lui confirmant la validation des paramètres fournis. Le SIP UA est alors enregistré **(étape 18, 19 et 20)** [31].

Localisation d'un abonné et établissement de session dans le réseau IMS :

La figure 2.11 décrit lřensemble des processus de localisation dřun abonné dans le réseau IMS ainsi quřà lřétablissement de session.

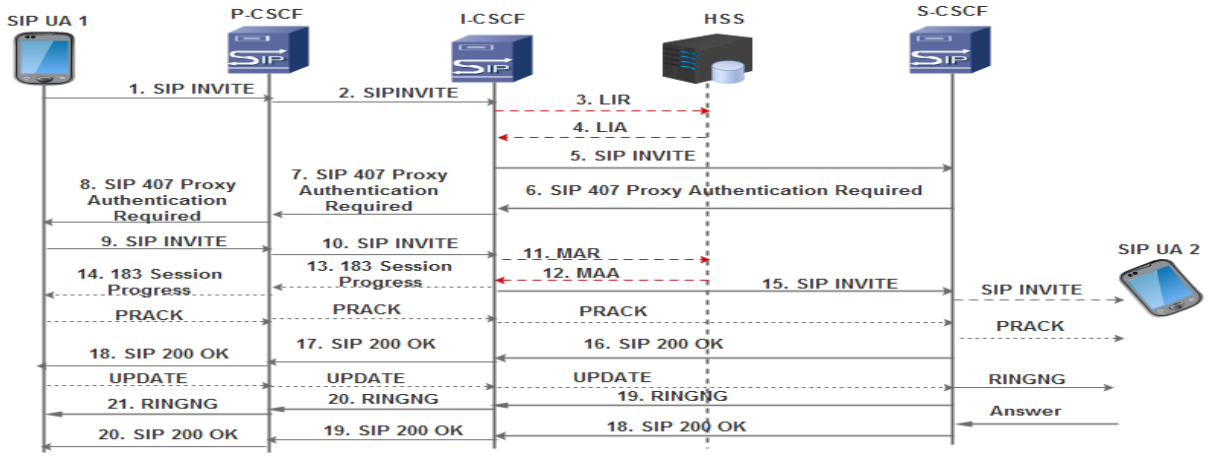


Figure 2.11. Localisation et établissement de session dans le réseau IMS avec SIP DIAMETER Application

Le concept de la signalisation et les types de protocoles utilisés tels que le SIP, le DIAMETER de base et le DIAMETER SIP, a montré leur importance dans le fonctionnement de lřIMS afin de rendre les communications fiables. Un mauvais fonctionnement de ces protocoles de signalisation impacterait la fiabilité du système par ricochet la qualité de service. Lřexemple de la SONATEL est édifiant, elle modernise son réseau et lřinterconnexion de son réseau fixe et son évolution sont prévues dans la période de 2017-2019 énoncée dans le document de référence **SNT/08/2016/V1/DRJ/DRG** du mois dřaoût 2016 intitulé : « **Service d'interconnexion catalogue 2016 de SONATEL** ».

2.7. Architecture d'interconnexion du réseau fixe de la SONATEL

La SONATEL a un vaste programme de modernisation de ses réseaux sur la technologie IP, lřIP lřunificateur des réseaux. Il convient de noter que dans son offre de service, il existe des services dřinterconnexion qui sont proposés aux opérateurs de réseau de télécommunications ouvert au public détenant une licence au Sénégal afin que tous les utilisateurs des réseaux connectés puissent communiquer librement entre eux. Il y a deux modes dřinterconnexion :

L'interconnexion est dite directe :

Lorsque la SONATEL achemine, à partir du point de connexion à son réseau jusqřà lřun de ses abonnés desservis par son réseau ou accessible depuis son réseau, le trafic provenant dřun client de lřexploitant du réseau interconnecté.

L'interconnexion est dite indirecte :

Lorsque la SONATEL achemine le trafic dřun de ses abonnés desservis par son réseau au point dřinterconnexion du réseau dřun autre opérateur afin de permettre à cet abonné de devenir un client de lřopérateur en question et dřutiliser les services de celui-ci. Un opérateur qui veut sřinterconnecter au réseau de la SONATEL, passe par un accord qui fait lřobjet dřune convention qui décrit les modalités techniques et financières des prestations dřinterconnexion [32].

2.7.1. Architecture intermédiaire d'interconnexion du réseau fixe SONATEL

Dans le cadre de son programme de modernisation de ses réseaux sur une technologie IP, la SONATEL a migré son réseau de télécommunication commuté fixe vers une infrastructure IP Multimédia System (*IMS*). Ce programme sřétale de 2017 à 2019. Nous avons vu lřimportance de lřIMS dans les réseaux mobiles et fixes précédemment (chapitre 1 et chapitre 2), nous concluons que lřIMS est le point dřancrage de tous les réseaux convergents. La SONATEL sřinspire de ces nouveaux concepts pour faire évoluer son réseau de télécommunications. Ainsi, lřinterconnexion de la SONATEL est actuellement réalisée au moyen des liens MIC transportant des flux de signalisation ISUP (*ISDN User Part, protocole de gestion de la communication sur des réseaux de circuits*) et de la Voix sur du TDM.

Durant les trois (3) ans, lřinterconnexion entre le fixe et les commutateurs mobiles de SONATEL sřest faite en SIGITRAN cřest-à-dire en BICC (*Bearer Independant Call Control*, extension du protocole ISUP sur un réseau de transport ATM ou IP) sur de lřIP pour les flux de signalisation, et en Real-Time Transport Protocol (*RTP*) pour le transport de la Voix en IP. Lřarchitecture intermédiaire de lřinterconnexion fixe lors de la période 2017-2019 est fournie par la figure 2.12 [32].

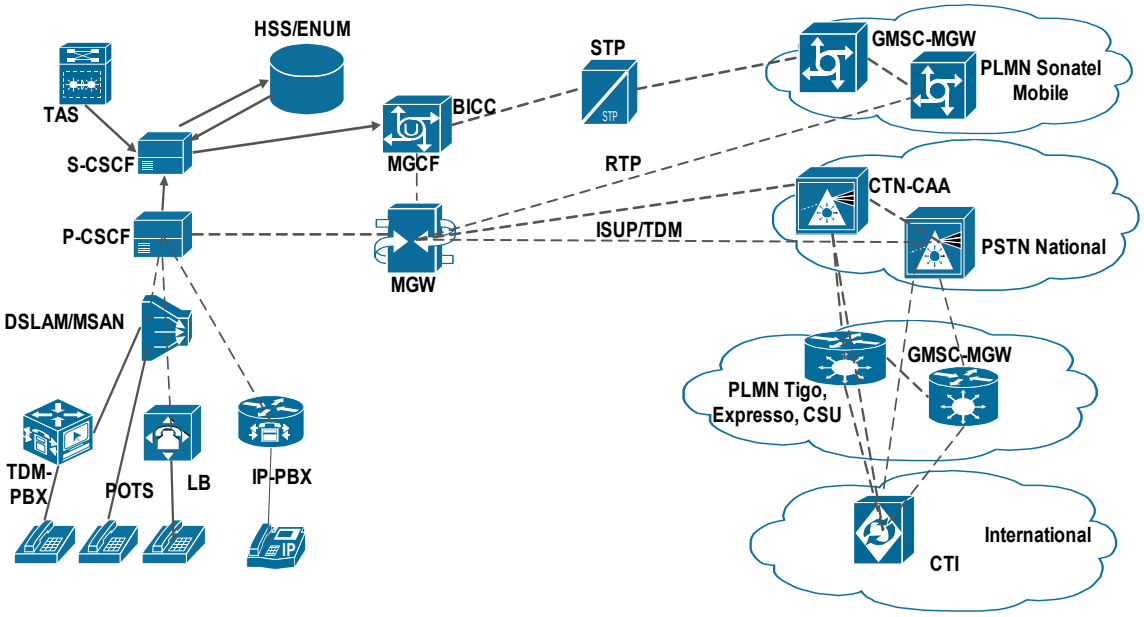


Figure 2.12. Architecture intermédiaire d'interconnexion du réseau fixe SONATEL [32]

2.7.2. Architecture cible d'interconnexion du réseau fixe SONATEL

Dans le cadre de ce même programme de modernisation de la SONATEL, il était prévu quřen 2019, les opérateurs internationaux soient connectés non plus aux centres de transit de Dakar Medina et Thiès mais aux IMS-MGW de Technopole et Médina. Le raccordement sřétait fait toutefois sur la même technologie, au moyen de liens MICs transportant des flux ISUP et voix en TDM. Lřarchitecture est présentée par la figure 2.13.

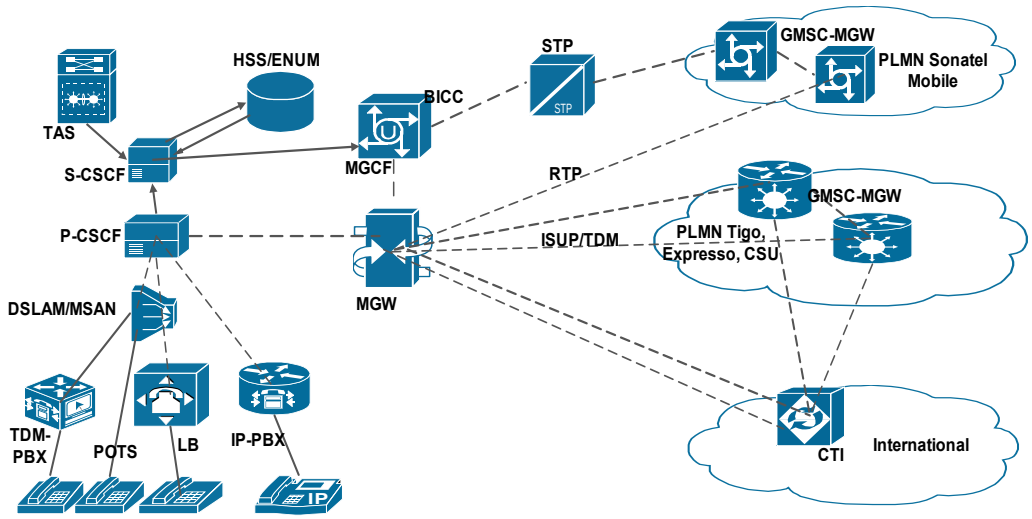


Figure 2.13. Architecture cible d'interconnexion du réseau fixe SONATEL post 2019 [32]

Ces deux (2) figures dřinterconnexion ci-dessus du réseau fixe de la SOANTEL montre bien la migration du réseau fixe vers lřIMS qui était effective en 2019, lřIMS est la solution de la convergence des systèmes de télécommunications.

2.8. Conclusion

Dans ce chapitre, nous avons décrit lřévolution de la signalisation dans lřétablissement de la communication. Le protocole DIAMETER SIP Application permet dřauthentifier les utilisateurs pour les sessions Multimédia IP sur SIP (IMS) grâce aux interfaces normalisées.
LřIMS et le protocole SIP permettent aux utilisateurs de se connecter facilement au système téléphonique PBX (*autocommutateur privé*) de lřentreprise.
Le réseau fixe de la SONATEL qui a migré progressivement vers lřIMS est une réalité. LřIMS est une architecture standardisée de type NGN, utilisée par les opérateurs de téléphonie, permet de fournir services multimédias fixes, mobiles et aussi Internet. Les systèmes téléphoniques traditionnels (*commutations de paquets et circuits*) sont aussi pris en charge. LřIMS facilite lřoffre de presque tous les services basés sur IP. Parmi ceux-ci : la voix sur IP (*VoIP*), la voix sur réseau mobile LTE (*VoLTE*), le Push to talk sur téléphones cellulaires, les jeux multijoueur, la vidéoconférence, la messagerie instantanée, les services communautaires, les informations de présence et partage de contenus.

De ce qui précède, lřIMS est au cœur des systèmes convergents de télécommunications, il est important dřétudier le réseau IMS qui demeure un réseau sûr aujourdřhui, cela nécessite une étude détaillée de lřIMS dans le chapitre qui suit.

Chapitre 3 : Etude de l'architecture de l'IMS et de l'intégration avec le WebRTC

Lřarchitecture Tout IP a conduit à la convergence des technologies de télécommunications car la technologie IP est dite Best Effort, facilitant le développement des services qui combinent télécommunications et informatique. Le concept dřIMS est de permettre la mutualisation de plusieurs médias, points dřaccès et modes de communication dans un seul réseau. Lřutilisateur final pourra profiter simultanément de la voix, des données et des sessions multimédias en utilisant tout accès haut débit et une commutation de paquets IP. LřIMS est développé autour du SIP qui est le protocole de signalisation, cřest lui qui gère les connexions et les types de communications (*services*).

Dans le contexte de la convergence, lřIMS devient ainsi le fédérateur des réseaux téléphoniques classiques, de la télévision numérique et du web. Les nouvelles capacités de réseaux et des terminaux, lřassociation entre Internet et voix, le contenu et la mobilité donnent naissance à de nouveaux modèles de réseau. Ils offrent un formidable potentiel pour développer de nouveaux services de communications simples, transparents, sécurisés, portables et fiables. LřIMS est une architecture indépendante de lřaccès physique, et par conséquent le service est délivré quel que soit le terminal (téléphone mobile, PC via ADSL ou FO, …), ce qui permet une convergence des accès. De plus, les services sont accessibles par lřutilisateur même en cas de mobilité tels que les appels vocaux et la vidéo, la messagerie instantanée, le chat individuel et groupe, le transfert de fichier, la présence et la géolocalisation. Lř**IMS** est donc le **réseau d'avenir**, **gage d'émergence numérique**.

Le réseau IMS peut sřinterconnecter avec un réseau basé sur le WebRTC qui fournit de services de riches communications à lřaide des navigateurs sans installation de logiciel chez les utilisateurs, offrant une grande souplesse par ces plateformes. Le WebRTC offre les mêmes services que lřIMS, leur intégration offrira de gros avantages aux utilisateurs. Dans le cadre cette thèse, nous allons faire lřétat de lřart de lřIMS afin de montrer combien sa fiabilité garantira lřoffre et la qualité de tous les services. Enfin, nous terminerons ce chapitre par une conclusion.

3.1. Architecture fonctionnelle en couches de l'IMS

A la conception de lřIMS, de besoins ont été définis comme suit : lřindépendance par rapport à lřaccès, la garantie de QoS des services multimédias, le contrôle de service et la tendance à supporter les mobilités. La mobilité de lřusager sans coupure et de ses services doivent être prise en compte [33].

Dans tout type de réseau, il y a toujours quatre (4) types de signalisation :

- **Signalisation d'enregistrement** : par elle, un terminal sřenregistre dans le réseau. Elle contient les procédures de téléchargement du profil et la gestion de la localisation. Elle est effectuée par la procédure dřenregistrement SIP (***SIP REGISTER***) (figure 3.1).

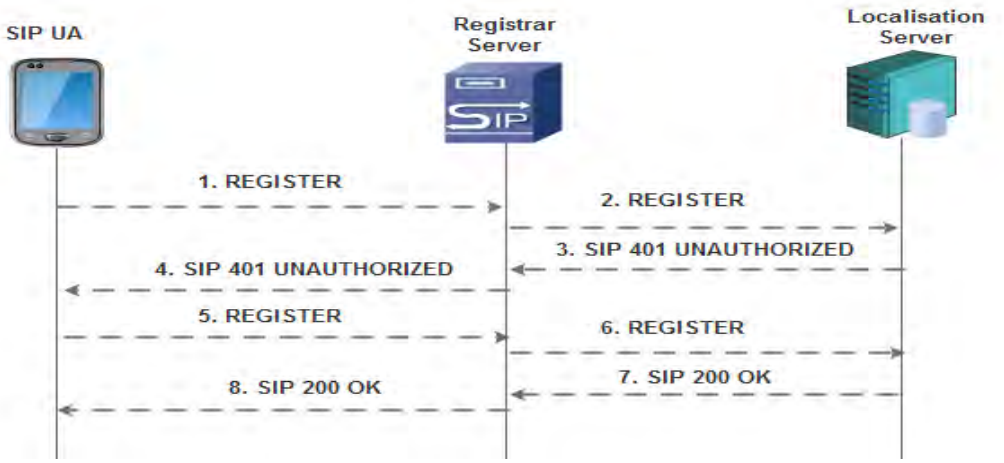


Figure 3.1. Procédure d'enregistrement SIP REGISTER

- **Signalisation d'appel** : par elle, nous établissons une association de bout en bout entre les points dřextrémité désirant communiquer. Ceci est réalisé par lřIMS grâce à la procédure dřétablissement de session (***SIP INVITE***) (figure 3.2).

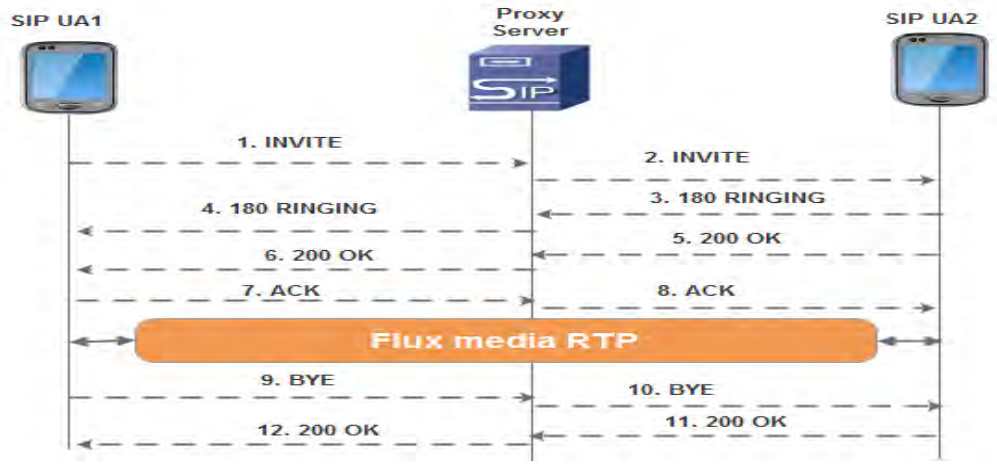


Figure 3.2. Procédure d'établissement session INVITE

- **Signalisation de connexion** : cřest lřaffectation dřun service support à un appel. Nous allons réserver des ressources dans le réseau selon la QoS requise pour le service. Dans le SIP, cette signalisation est effectuée grâce aux entêtes SDP qui permettent de décrire le trafic et les ressources requises. Au niveau transport, nous utilisons les mécanismes **RSVP** (*Ressource ReserVation Protocol*), **DiffServ** (*Differentiated Services*), pour assurer la qualité de service dans le réseau IP.
- **Signalisation d'intelligence** : elle permet de faire un traitement substitutif par rapport au traitement dřappel normal. Dřune façon similaire aux réseaux intelligents de type RI (*INAP*) ou CAMEL, les services sont exécutés par des serveurs dřapplications (AS) [33].

L'IMS est une architecture centralisée, divisée en plusieurs couches. Il permet lřintroduction des applications multimédias dans les réseaux fixes et mobiles. Les différentes couches de lřarchitecture de lřIMS sont présentées par la figure 3.3 ainsi que la description de chaque couche :

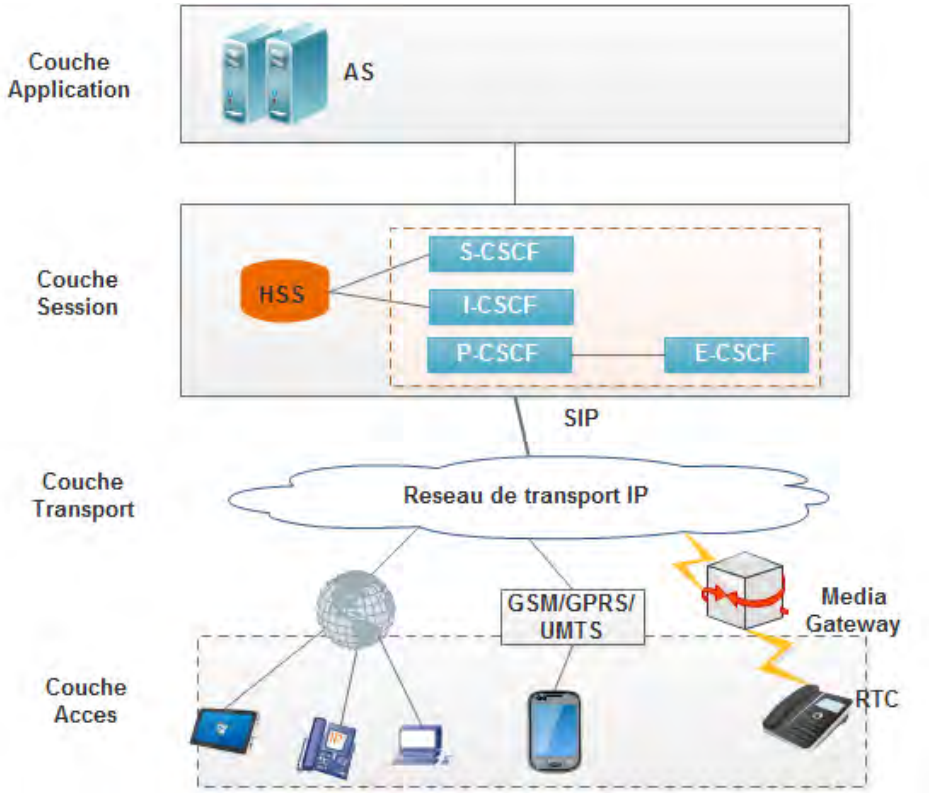


Figure 3.3. Architecture d'IMS

- **La couche physique (accès)**

Elle permet un large choix de terminaux aux utilisateurs. En effet, tous les systèmes comme les ordinateurs, les téléphones mobiles, les PDAs, les téléphones fixes numériques, sont capables de se connecter à lřarchitecture IMS via le réseau. Les téléphones traditionnels analogiques se connectent aussi à lřIMS par le biais de passerelles. Elle représente tout accès hauts débits tel que : **UTRAN**, **xDSL**, **CDMA2000**, **Wireless IP**, etc. En regroupant les différents types de réseaux au sein de cette couche, ceci montre la vision à lřorigine de lřidée des convergences des réseaux vers un réseau unique qui est lřIMS. Ainsi, lřIMS est indépendant du réseau dřaccès [1] [8] [33] [34].

- **La couche transport**

Elle représente le réseau IP constitué par des routeurs reliés par un réseau de transmission. Différentes piles de transmission peuvent être considérées pour le réseau IP : **IP/ATM/SDH**, **IP/Ethernet**, **IP/SDH**, etc… [33]. Ce réseau IP intègre des mécanismes de QoS avec Diffserv, RSVP, MPLS, etc…Un des principaux enjeux au niveau de cette couche est de réaliser la convergence entre le réseau à routage par paquet (*TCP/IP*) et le routage par circuit (*RTC*). Cřest à ce niveau quřinterviennent les passerelles PSTN [1] [8].

- **La couche contrôle de session (contrôle)**

Elle consiste en des contrôleurs de session responsables du routage de la signalisation entre utilisateurs et de lřinvocation des services. Ces nœuds sřappellent des **CSCF** (*Call Session Control Function*). LřIMS introduit donc un environnement de contrôle de session sur le domaine paquet. Le contrôle et la gestion des sessions se font grâce aux protocoles **SIP**, **COPS** et **DIAMETER**. Cřest la partie intelligente de lřarchitecture, qui offre toutes les fonctionnalités de gestion des utilisateurs et constitue le véritable socle de lřIMS [33] [35].

- **La couche application**

Elle regroupe lřensemble de services (*services à valeur ajoutée*) proposés aux utilisateurs du réseau. Le réseau IMS offre une plateforme de déploiement unifiée, simple, rapide, productive et sécurisée pour la mise en place de nouveaux services. Tout service est exécuté par un serveur applicatif en liaison avec les équipements de la couche de session par lřintermédiaire des protocoles **SIP** et **DIAMETER**, assurant ainsi la sécurité des utilisations. **[37].** Trois (3) plateformes de services ont été standardisées pour offrir les services à valeurs ajoutées. Il sřagit de : **SIP-AS** (*SIP Application Server*), **OSA- SCS** (*Open Service Access Service Capability Server*) et **IM-SSF** (*IP Multimedia Service Switching Function*).

3.2. Principales composantes de l'architecture de l'IMS

LřIMS introduit une nouvelle entité fonctionnelle dans le réseau appelé **CSCF**, elle joue le rôle de Proxy SIP et ses trois (3) principales fonctions sont :

- la localisation des utilisateurs en traduisant lřadresse SIP de destination en une adresse IP ;
- le routage des messages SIP pour établir, modifier et libérer des sessions multimédias ;
- le maintien des informations dřétat de la session pour invoquer les services souscrits par les utilisateurs, de contrôler la session pendant sa durée de vie et la facturer [33].

Nous présentons les composantes du réseau IMS et leurs fonctionnalités ci-dessous :

Les terminaux IMS :

Cřest une application installée sur un équipement dřun utilisateur qui émet et reçoit des requêtes SIP. Il peut être un PC, un téléphone IP ou une station mobile UMTS (*UE*).

CSCF *(Call Session Control Function):*

Ce sont des serveurs de contrôle de sessions, échangent les messages de signalisation via le protocole SIP. Ils orientent et contrôlent lřouverture dřune session. Il existe quatre (4) types de serveur CSCF :

3.2.1. Le P-CSCF

Il est un serveur proxy et sert dřintermédiaire entre le terminal et le réseau IMS. Cřest le premier point de contact de lřutilisateur avec le réseau IMS. Il reste attribuer au même terminal tout au long de la session. La procédure de contact du serveur P-CSCF commence par lřautorisation du terminal sur le réseau. Cette identification est réalisée par la couche de transport. Dès que le terminal a la possibilité dřéchanger des données sur le réseau, il recherche et contacte le P-CSCF. Cette phase de contact permet lřauthentification de lřutilisateur. Une fois, lřutilisateur authentifié, le P-CSCF certifie lřidentité de lřutilisateur pour les autres nœuds du réseau. Il conserve un lien constant entre lřutilisateur et le terminal. Au delà dřune simple table de correspondance, il joue le rôle de proxy de sécurité en sřassurant que les messages SIP sont bien formés. Ce proxy est sollicité dans le réseau IMS, quřil existe ou non du trafic. Malgré la présence de plusieurs P-CSCF, il nřest pas possible pour lřutilisateur dřen changer au cours dřune session réseau. Les messages SIP en provenance de lřutilisateur sont relayés par le P-CSCF, ensuite transférés à une des deux autres entités (*I-CSCF ou S-CSCF*). Ce sont des unités de traitement des messages de signalisation. Le P-CSCF détecte aussi les appels dřurgence et les transfère vers lřentité E-CSCF et fournit les informations nécessaires à la génération des tickets de taxation. Il établit une association de sécurité IPSec avec lřUE lors de son enregistrement. Il contrôle à partir des messages DIAMETER échangés avec le PCRF le type de ressources requis par lřUE en fonction des capacités autorisées par le réseau EPS [1] [8].

3.2.2. L'I-CSCF

Cřest un serveur de routage de messages. Il prend en charge les requêtes en provenance du P-CSCF et les transfère :

- si cřest une demande dřauthentification, il route le message vers un S-CSCF sans distinction préalable ;
- si lřutilisateur est déjà enregistré, il route le message vers le S-CSCF qui a authentifié lřutilisateur, pour les raisons évoquées ci-dessus.

Un réseau IMS peut inclure plusieurs I-CSCF pour assurer une scalabilité et une redondance. Elle génère aussi les informations nécessaires à la génération des tickets de taxation [1] [8].

3.2.3. Le S-CSCF

Il est à la fois une entité SIP standard (*REGISTRAR*) et un serveur SIP avec sa propre logique. Un serveur dřenregistrement SIP authentifie et enregistre les utilisateurs. Chaque utilisateur est identifié par une URI SIP. Lřenregistrement associe la ou les adresses IP utilisées par lřutilisateur avec son URI. Concrètement, un S-CSCF :

- récupère dans la base HSS les informations de lřutilisateur pour les mettre en cache ;
- associe lřadresse IP utilisée par le terminal de lřutilisateur avec lřURI de ce dernier ;
- effectue les requêtes de bande passante auprès des éléments de la couche transport ;
- appelle les fonctions de facturation ;
- contrôle lřaccès aux ressources en utilisant le profil de lřutilisateur depuis le HSS ;
- route les messages SIP vers les autres entités du réseau.

Le routage des messages SIP dépend de lřopération à effectuer :

- un besoin de services transfère le message vers le serveur dřapplications correspondant ;
- une communication vers un autre utilisateur du réseau, route le message SIP vers lřUE ou un autre S-CSCF ;
- une communication vers un utilisateur IMS extérieur au réseau, route le message vers le I-CSCF ;
- une communication vers un utilisateur de réseau traditionnel, route la requête vers les passerelles correspondantes.

3.2.4. L'E-CSCF

Lřentité E-CSCF est dédiée au traitement des demandes dřurgence vers la police ou le standard du service des sapeurs-pompiers (*numéro vert*). Elle effectue le traitement des appels dřurgence transmis par lřentité P-CSCF et le routage des requêtes vers le centre dřurgence le plus proche de lřUE. Lorsquřune requête SIP INVITE arrive à lřentité E-CSCF, elle contacte

lřentité LRF pour obtenir la localisation de lřUE ou valider si elle est incluse dans la requête. Elle transfère la requête vers le centre dřurgence le plus proche [1**]**.

Pour conclure, les entités de gestion et de contrôle sont au nombre de trois : un P-CSCF, un I-CSCF et un S-CSCF. Leur travail ne concerne pas uniquement le contrôle dřaccès et lřauthentification des utilisateurs sur le réseau. Les CSCF supervisent lřensemble des sessions dřun réseau IMS : lřouverture de session entre utilisateurs dřun même réseau, lřouverture de session entre utilisateurs dřun autre réseau IMS et lřouverture de session entre utilisateurs et serveurs dřapplications. Ces trois équipements (*CSCF*) sřappuient sur le HSS qui leur sert de support de stockage. Une quatrième entité non de moindre, E-CSCF dépend de P-CSCF et traite les appels dřurgence (police, sapeurs-pompiers).

3.2.5. Le HSS (Home subscriber server)

Le HSS est une base de données assurant le stockage des données propres à chaque utilisateur (profil) du réseau IMS à lřexemple du HLR pour le GSM. Les données enregistrées comprennent les identités des utilisateurs, les paramètres dřaccès et les règles dřinvocations de serveurs dřapplications par lřentité S-CSCF. Les données à un utilisateur pour établir une session multimédia sont : le profil de lřutilisateur cřest à dire lřensemble des services auxquels lřutilisateur est abonné, les identifiants privés et publics, lřadresse du S-CSCF qui lui a été allouée, des informations de sécurités (*son vecteur d'authentification*), lřadresse AS, les iFC etc. Lřentité HSS interagit avec les entités du réseau grâce au protocole DIAMETER **[1] [33]**. Lřentité HSS dispose de la :

- **Table SVP** : elle contient le profil de service associé à chaque utilisateur ;
- **Table IMPI** : elle contient les identifiants des adresses publiques et privées de lřutilisateur avec les informations d'authentification et dřautorisation ;
- **Table IMPU** : elle contient des informations dřenregistrement ;
- **Table IMS Subscription User (IMSU)** : elle contient des informations de souscription ;
- **Table Charging information (Chginfo)** : elle contient des informations de tarification ;
- **Table Networks** : elle contient la localisation du réseau où lřutilisateur est abonné ;
- **Table Roam** : elle contient les réseaux avec lesquels des accords de roaming sont passés.

- **Table as_perm_list** : elle contient les services autorisés auxquels lřutilisateur est abonné ;
- **Table Application Server (APSVR)** : elle contient lřadresse de lřAS à contacter.
- **Table Initial Filter Criteria (IFC)** : elle représente les informations de filtrage initial, caractérisant un certain service pour l'utilisateur [33].

Ainsi, toutes les données relatives à un même compte utilisateur doivent être stockées sur un même **HSS**. Néanmoins, lorsque le nombre dřutilisateurs devient important, il est possible de les répartir au sein de plusieurs HSS. Dans ce cas, il faut mettre en place une entité complémentaire, appelée le **SLF** (*Subscriber Location Function*), qui a pour rôle de déterminer le HSS contenant les données relatives à un utilisateur.

3.2.6. Le PDF (Policy Decision Function) et le MRF (Multimedia Resource Function)

Il a été prévu dans la release 5 de spécifications de 3GPP, lřutilisation dřune plateforme de distribution de politique de provisionning, de routage et de qualité de service. Cette **fonction PDF** a été introduite dans le P-CSCF, tandis que pour la version 6, la fonction PDF est gérée dans un autre bloc fonctionnel.

La fonction **MRF** permet dřétablir un pont de conférence entre les utilisateurs dřun réseau IMS. Son rôle est de gérer la signalisation vers tous les utilisateurs dřune conférence, en offrant des facilités dřexploitation, comme la sélection des types de flux. Le MRF se décompose en deux entités logiques : le MRFC (*Multimedia Resource Function controller)*, en charge de la signalisation et des paramètres sollicités par lřutilisateur pour la mise en œuvre de la conférence, le MRFP (*Multimedia Resource Function Processor)* est responsable du traitement des flux de données [35].

3.2.7. Les passerelles

- **Le BGCF (*Breakout Gateway Control Function*) :** le BGCF est une passerelle utilisée pour lřinterconnexion avec le RTC. Il communique via le protocole SIP. Il sert à préciser le routage des appels initiés par des terminaux IMS vers ceux fonctionnant en mode commutation de circuits (*RTC ou GSM*) [35].
- **Le Media Gateway *:*** le Media Gateway est situé au niveau du transport des flux média entre le réseau RTC et les réseaux en mode paquet, ou entre le cœur de réseau NGN et

les réseaux d'accès. Elle a pour rôle le codage et la mise en paquets du flux média reçu du RTC et vice versa (*conversion du trafic TDM IP*) et aussi en transmission des flux média sont reçus de part et d'autre.

- **Le Signaling Gateway :** la fonction dřune passerelle de signalisation est de convertir la signalisation échangée entre le réseau NGN et le réseau externe interconnecté selon un format compréhensible par les équipements chargés de la traiter. Elle transporte un message de signalisation ISUP dřun transport SS7 vers SIGTRAN. Il est en contact avec lřentité MGCF qui se charge de remplacer la signalisation ISUP en signalisation SIP. Elle assure l'adaptation de la signalisation par rapport au protocole de transport utilisé.
- **Media Gateway Control Function *:*** elle contrôle les passerelles et assure le passage du mode paquet au mode circuit, cřest-à-dire la conversion du protocole ISUP provenant du RTCP en protocole SIP. Il ouvre, maintient et ferme les connexions entre les réseaux IP et RTC.

3.3. Architecture de service IMS (les serveurs d'application)

Lřarchitecture en service de lřIMS est constituée des serveurs dřapplication qui sont des entités SIP (Figure 3.4), fournissant différents types de services aux utilisateurs. Ces serveurs interagissent avec le réseau IMS à travers lřinterface **ISC** (*IP Multimedia Service Control*) supportée par le protocole SIP. Ils sont connectés au serveur S-CSCF, qui joue lřintermédiaire entre lřutilisateur et les services. Le S-CSCF dispose du profil de service de lřabonné qui lui indique les services souscrits et sous quelle condition invoquée ces services. Les serveurs dřapplication hébergent les services à valeur ajoutée (*conférence, tarification en ligne, des services IP Centex, la continuité d'appel vocal VCC*). Le S-CSCF offre le service de contrôle de lřIMS et interagit avec le HSS basé sur le protocole DIAMETER, pour obtenir les informations sur le profil des abonnés.

LřIMS a été créé pour promouvoir les services au sein des réseaux de télécommunications. Les services sont hébergés et rendus disponibles par lřintermédiaire de serveurs dřapplications. Ils appartiennent soit à lřopérateur soit à un fournisseur tiers. Ces serveurs sont situés soit au sein du réseau IMS soit dans un autre réseau. Nous distinguons trois (3) catégories de serveurs dřapplications (*AS*) : les serveurs dřapplications **SIP**, **OSA** et **CAMEL** (figure 3.4) :

- Les serveurs d'application SIP (***SIP AS***) exécutent des services (*e.g,* ***Push To Talk, Présence, Prépaid, Instant messaging****, etc*.) nativement implémentés pour fonctionner avec SIP.
- Le point de commutation au service IM (***IM-SSF*** *: IP Multimedia Service Switching Function*) permet la mobilité de lřabonné tout en lui garantissant la fourniture de ses services, même sřil ne se trouve pas dans une infrastructure qui nřappartient pas à son opérateur de services, il est nécessaire dřavoir une passerelle qui sřappelle IM-SSF, afin de connecter lřabonné à son serveur dřapplications de son opérateur.
- La passerelle OSA (***OSA SCS****, OSA Service Capability Server*) est un type particulier de serveur d'application SIP qui termine la signalisation SIP sur l'interface ISC et qui interagit avec des serveurs d'application OSA en utilisant l'API OSA.
- Un type spécialisé de serveur d'application SIP appelé gestionnaire d'interaction de service (*SCIM*) entre les serveurs d'application SIP.

Les serveurs d'application peuvent interagir avec l'entité MRFC à travers le S-CSCF afin de contrôler les activités média mises en œuvre par l'entité MRFP [19].

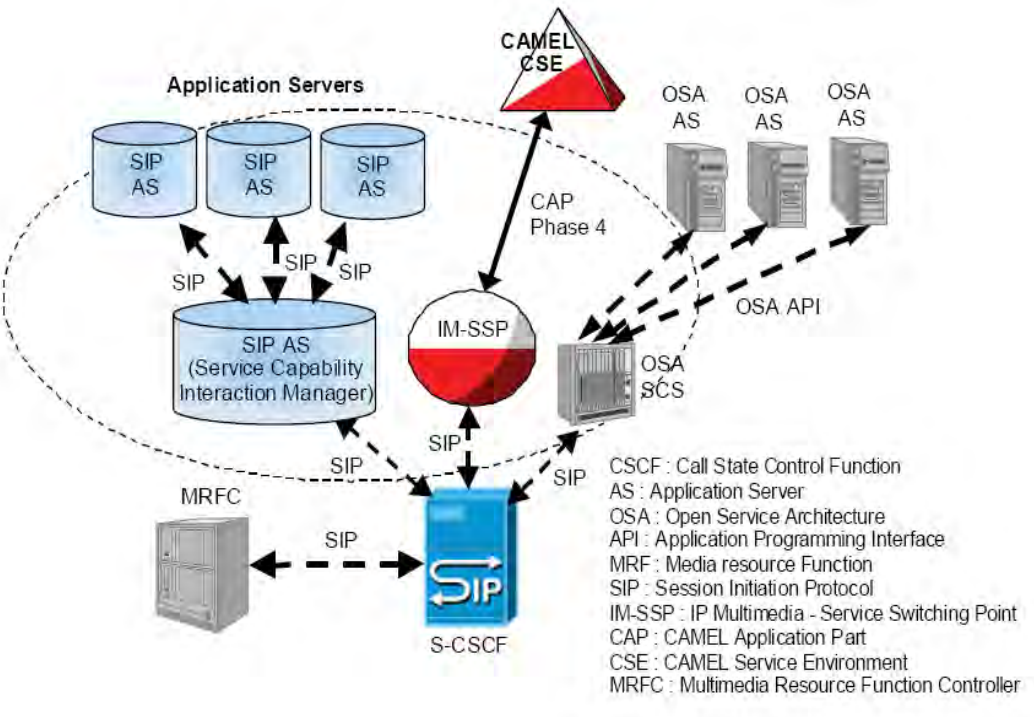


Figure 3.4. Architecture de service IMS [19]

3.4. Les protocoles et les interfaces

Les protocoles :

Les trois (3) principaux protocoles utilisés dans IMS sont les suivants : le **SIP**, le **DIAMETER** et le **COPS (*Common Open Policy Service*)**. Le COPS est un protocole flexible permet la mise en place de politiques par entité centrale appelée le **PDP** (*Policy Decision Point*) et sont appliquées sous forme des règles dans des entités appelées le **PEP** (*Policy Enforcement Point*). Le protocole **COPS** sert aux opérateurs de garantir une qualité de service.

Les interfaces :

Lřinfrastructure du réseau IMS se décompose en des interfaces standardisées. Chaque interface constitue un point de référence définit à la fois le protocole et les fonctions opérées. Nous décrivons ci-dessous les interfaces développées dans le système.

- **Interface Gm :**

Elle relie lřUE à lřIMS et est utilisée pour le transport de tous les messages SIP de signalisation entre lřUE et lřIMS. Les procédures utilisées à cette interface sont les suivantes : lřenregistrement, le contrôle de session et les transactions.

- **Interface Mw :**

Elle est basée sur le SIP et est entre les différentes entités CSCF. Les procédures sont divisées en trois catégories principales : lřenregistrement, le contrôle de session et les transactions.

- **Interface ISC :**

Pour lřenvoi et la réception de message SIP entre le S-CSCF et les serveurs dřapplication. Les procédures ISC sont divisées en catégories de routage : les demandes SIP vers les serveurs dřapplications (AS) et les requêtes SIP initiées par AS.

- **Interface Cx :**

Elle est entre le HSS et le CSCF, le protocole utilisé est le **DIAMETER**. Lorsque lřutilisateur reçoit des sessions, les données centralisées dans le HSS doivent être utilisées par lřI-CSCF et le S-CSCF.

- **Interface Dx :**

Plusieurs HSS sont déployées séparément dans le réseau, aucune des entités suivantes lřI-CSCF et le S-CSCF ne sait quel est le HSS contacter. Dans ce cas, il est nécessaire de

contacter le SLF en premier. Lřinterface Dx est utilisée en conjonction avec lřinterface Cx. Le protocole utilisé en cette interface est le DIAMETER [37].

- **Interface Sh :**

Un serveur dřapplication (AS) a besoin de savoir à quel S-CSCF envoyer une requête SIP. Ces genres dřinformations sont stockés dans le HSS. **Sh** est lřinterface entre le HSS et le serveur dřapplication (AS) et est basée sur le DIAMETER. La figure 3.5 et le tableau 3.1 illustrent les différents interfaces et protocoles utilisés.

Figure 3.5. Protocoles et interfaces de l'architecture de service IMS [33]

Tableau 3.1. Interfaces et protocoles utilisés

Entités	Interfaces	Protocoles
Cx	Interface entre CSCF et HSS	DIAMETER
Dx	Interface entre S-CSCF et SLF	DIAMETER
Gm	Interface entre UE et P-CSCF	SIP
Isc	Interface entre S-CSCF et AS (serveur d'application)	SIP
Sh	Interface entre AS (SIP-AS ou OSA-CSCF) et HSS	DIAMETER
Rx	-Interface entre CRF et P-CSCF (Release 6) -Interface entre PCRF et CSCF (Release 7)	DIAMETER
Mw	Interface entre CSCF	SIP

3.5. La gestion des utilisateurs

Durant la procédure dřenregistrement, les données de lřutilisateur et les services auxquels il a souscrit seront téléchargées depuis le HSS par le S-CSCF. Cependant, il est possible que ces données changent pendant que le S-CSCF sert toujours à lřutilisateur. Pour mettre à jour ces

données au niveau du S-CSCF, le HSS initie une commande **PPR** (*Push profile Request*). La mise à jour est effectuée immédiatement [36].

- **Localisation :** quand lřI-CSCF reçoit une requête SIP REGISTER du P-CSCF via lřinterface Mw, la commande **UAR** (*User Authorization Request*) est invoquée. À la réception de la commande UAR, le HSS répond par une commande **UAA** (*User Authorization Answer*) qui contient un nom du S-CSCF ou les S-CSCF disponibles selon le statut courant de lřutilisateur. Les S-CSCF disponibles sont envoyés si cřest la première fois que lřutilisateur se connecte et nřa pas de S-CSCF associé dans la base HSS. Après cela, lřI-CSCF renvoie la requête SIP REGISTER au S-CSCF renvoyé ou sélectionné [36].
- **L'authentification des utilisateurs :** lřauthentification des utilisateurs de lřIMS est basée sur un secret partagé préconfiguré. Le secret partagé et les séquences de nombre sont stockés dans lř**ISIM** (*IP Multimedia Service Identity Module*) ou lř**USIM** (*UMTS Subscriber Identity Module*) dans lřUE et dans le HSS du réseau. Comme le S-CSCF sřoccupe de lřauthentification de lřutilisateur, il existe un besoin de transférer les données de sécurité par lřinterface Cx. Lorsque le S-CSCF a besoin dřauthentifier un abonné, il envoie une commande **MAR** (*Multimedia-Auth-Request*) au HSS. Le HSS répond par une commande **MAA** (*Multimedia-Auth-Answer*). La réponse contient entre autres lřinformation dřauthentification. Elle inclut un ou plusieurs vecteurs selon lřalgorithme utilisé (exemple Digest-AKAv1-MD5), lřinformation dřauthentification (le challenge RAND dřauthentification et la valeur AUTN prise), lřinformation dřautorisation (expected response ou **XRES**), la clé dřintégrité et la clé de confidentialité [36].
- **La gestion des données :** la gestion des données permet de récupérer les données depuis le HSS. Ce sont de données relatives au service, aux informations dřenregistrement, aux identités publiques, aux filtres, au nom du S-CSCF destiné à lřutilisateur, aux adresses des entités de la facturation et même aux informations de localisation provenant de domaines de paquets ou circuits. Le serveur dřapplication (AS) utilise la commande **UDR** (*User-Data-Request*) pour demander les données et le HSS répond par la commande **UDA** (*User-Data-Answer*).
- **Souscription/Notification :** ces procédures de souscription/notification permettent à lřAS dřavoir des notifications quand une donnée particulière dřun utilisateur

spécifique a été mise à jour dans le HSS. LřAS envoie la commande **SNR** (*Subscribe-Notification-Request*) pour recevoir les notifications et le HSS répond par la commande **SNA** (*Subscribe-Notification-Answer*).

3.6. Gestion des identités

Dans tout type de réseau déployé par les opérateurs, il est impératif de pouvoir identifier les utilisateurs dřune façon unique et quřils soient joignables de nřimporte quel réseau. Il existe un nouveau concept dřidentification dans lřIMS, par rapport à ce qui se faisait dans les réseaux mobiles tout en restant compatible. Cette identification fournit plus de flexibilité pour réaliser des nouveaux services. La technique dřidentification sřappuie sur le protocole **SIP** (*Session Initiation Protocol*).

3.6.1. Identification d'un utilisateur public et privé

Identification d'un utilsateur public :

Le **PUI** (*Public User Identity*) est une adresse publique qui permet dřidentifier un utilisateur. Lřopérateur attribue une ou plusieurs adresses publiques à chaque utilisateur IMS. Lřidentité publique est lřéquivalent du **MSISDN** (*Mobile Station ISDN Number*) en GSM, qui permet de joindre un abonné et à router les messages SIP. La PUI est sous deux formats :

- ***SIP URI*** : sous la forme « **sip : premier.dernier@opérateur.com** ». Il est aussi possible dřinclure un numéro de téléphone dans une SIP URI sous le format suivant : « sip : +221-77-643-97-09@opérateur.com; user = phone ».

  Exemple : sip:daniel@lirt.sn

- ***TEL URL*** : permet de représenter un numéro de téléphone dans un format international « tel : +221-77-643-97-09 ». Il est utilisé pour les appels entre le monde RTC et le monde IMS. En effet, en RTC, les téléphones sont identifiés par des numéros et ne peuvent composer que des numéros. Lřopérateur IMS doit ainsi allouer à chaque utilisateur au moins un SIP URI et un TEL URL [38].

Identification d'un utilisateur privé :

A chaque utilisateur est attribuée une identité privée. Elle est identique à IMSI en GSM et permet lřauthentification et lřenregistrement de lřabonné. La **PUI** (*Private user identity*) est en

principe stockée dans la carte à puce sous le format dřun « Network Access Identifier » : « username@opérateur.com ».

3.6.2. Relation entre une identité publique et une identité privée

Dans le réseau GSM/UMTS, la carte à puce stocke lřidentité privée et au moins une identité publique. Le HSS contient pour chaque utilisateur son identité privée et la collection dřidentités publiques qui lui sont attribuées. Dans le cas où lřutilisateur utilise une carte GSM/UMTS qui ne contient pas ces informations, le terminal est capable de les construire à travers lřIMSI. La relation entre lřutilisateur IMS et ces identités dans la Release 5 est montrée par la figure 3.6 :

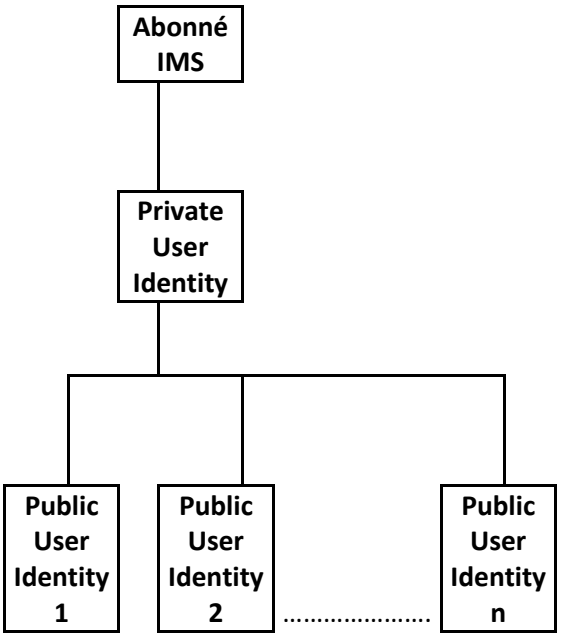


Figure 3.6. Relation entre l'identité privée et publique en IMS 3GPP R5.

Dans lřIMS 3GPP Release 6, un abonné peut avoir plusieurs identités privées comme illustré dans la figure 3.7. Dans le cas de lřUMTS, une seule identité privée peut être contenue dans la carte à puce, même si lřutilisateur peut avoir plusieurs cartes contenantes chacune une identité privée différente. Il est encore possible dřutiliser simultanément la même identité.

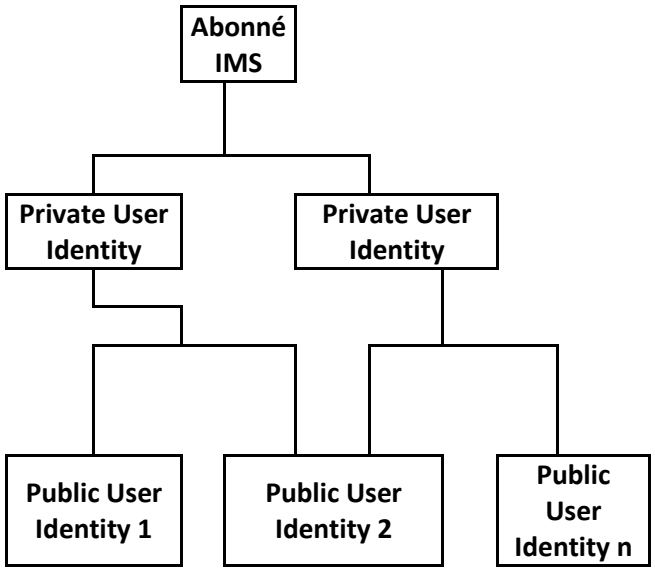


Figure 3.7. Relation entre l'identité privée et publique en IMS 3GPP R6.

Exemple de gestion des identités dans le réseau IMS :

Les identités dřun utilisateur dans le réseau IMS sont gérées par deux identificateurs : lř**IMPU (***public)* et lř**IMPI (***privé*)**.** Lřidentité publique dřun utilisateur est désignée par un lř**URI** qui sera utilisé par ses correspondants pour le joindre.

- **URI SIP** → sip: [nom_user]@[nom_domaine]

Exemple : sip:daniel@lirt.sn

- **URI TEL** désigne le numéro du téléphone conventionnel appelé **MSISDN** (*Mobile Suscribe ISDN Number*).
- **L'IMPI** est utilisé pour identifier et authentifier un abonné et nřa aucun impact dans le routage des messages SIP. Cette identité privée est fournie par lřopérateur du réseau IMS. Il est stocké dans une **ISIM** (*IMS Subscriber Identity Module*), lřéquivalent dans les réseaux mobiles est la carte SIM
    - Format de lřIMPI : [nom utilisateur]@[nom_domaine]

Exemple : daniel@lirt.sn

A côté de ces deux identités, lřIMS utilise aussi une autre identité appelée **IMSU**, utilisé pour la facturation. Cřest en général, le nom complet de lřutilisateur [35].

Exemple : Daniel Kag-teube

3.6.3. Profil d'usager et profil de service

Le profil de service est une collection dřinformations spécifiques à lřutilisateur, stockée en permanence dans le HSS. Il est transféré du HSS à un S-CSCF à lřaide de deux opérations : Server-Assignment-Answer (***SAA***) et Push-Profile-Request (***PPR***). Le profil de service est obtenu par l'entité S-CSCF auprès du HSS à travers l'interface Cx lorsque l'utilisateur s'enregistre au sous-système IMS **[33]**. Chaque usager IMS est associé à son profil dřutilisateur lié à un ensemble de profils de service dans le HSS. Un profil de service contient (figure 3.8) :

- une ou plusieurs IMPUs ayant la forme dřune adresse téléphonique ou dřune URI SIP, zéro ou une instance de la classe Core Network Service Authorization indiquant les différents médias utilisés pour les sessions établies avec ces identités publiques ;
- un ensemble (0 à N) de critères de filtrage (iFC, initial Filter Criteria). Cřest une information statique correspondant à une souscription dřun utilisateur à un service du domaine IMS ;
- un ensemble (0 à N) de "Shared iFC set". Un "Shared iFC Set" pointe sur un ensemble dřiFC administrés localement et stockés sur le S-CSCF. Il peut être partagé par plusieurs profils de service, permettant de minimiser la taille du profil de lřusager **[36].**

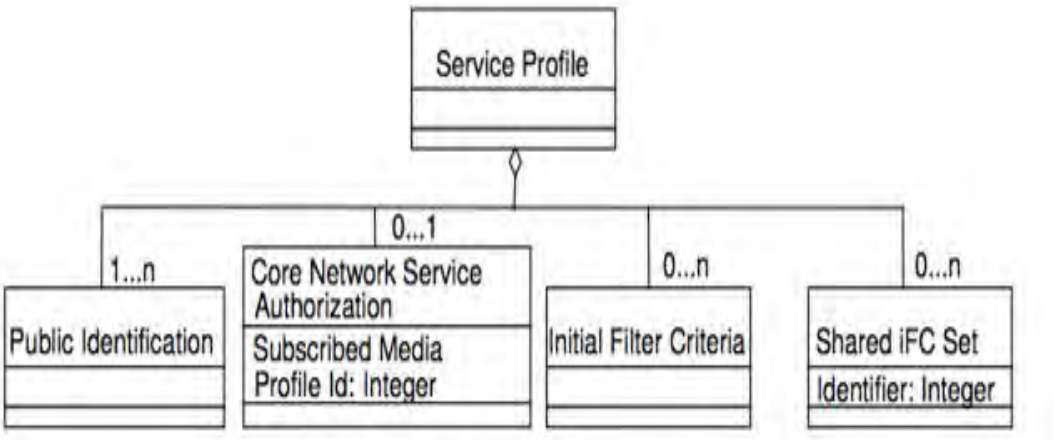


Figure 3.8. Gestion des profiles de service

3.6.4. La Carte USIM et ISIM

Dans chaque terminal, il y a une carte à puce appelée **UICC** (*Universal Integrated Circuit Card*), utilisée pour stocker des informations telles que lřétat dřenregistrement, les clefs

dřauthentifications, les messages et le carnet dřadresses. Il contient plusieurs applications logiques qui peuvent être : la SIM, lřUSIM et lřISIM.

- **L'USIM (***Universal Subscriber identity Module***)**

Lřaccès au réseau UMTS en mode circuit ou paquet se fait par la carte **USIM**. Elle contient les paramètres suivants :

- **IMSI** : comme en GSM, elle permet dřidentifier et dřauthentifier lřutilisateur. La *Private User Identity* est lřéquivalent à lřIMSI pour lřIMS ;
- **MSISDN** : il contient un ou plusieurs numéros de téléphone pour lřutilisateur. La *Public User Identity* est lřéquivalent au MSISDN pour lřIMS ;
- **CK** (*Ciphering Key*) et **IK** (*Integrity Key*) : les clefs de chiffrement et dřintégrité sont utilisées pour la sécurité de lřinformation sur lřinterface radio ;
- **Long term secret** : le secret utilisé pour authentifier lřutilisateur et pour générer les clefs de chiffrement et dřintégrité utilisées entre le terminal et le réseau ;
- **SMS** : dans ce champ sont stockés les messages courts *;*
- **SMS parameters** : les paramètres de configuration du service SMS (adresse du SMS center) ;
- **MMS user connectivity parameters** : il contient les paramètres de configuration du service MMS (adresse du *MMS server* et du *MMS gateway*) *;*
- **MMS user preferences** : il contient les préférences de lřutilisateur sur le service MMS comme le drapeau de rapport dřexpédition.

- **L'ISIM (***IMS Subscriber identity Module***)**

LřISIM contient les paramètres utilisés pour lřidentification et lřauthentification de lřutilisateur ainsi que la configuration du terminal IMS. LřISIM peut coexister simultanément avec une USIM ou une SIM. Les paramètres essentiels contenus dans une ISIM sont : ***Private User Identity***, ***Public User Identity, Home Network Domain URI*** *(*SIP URI du réseau nominal de lřutilisateur qui est unique dans la carte) et ***Long-term secret,*** le secret utilisé pour authentifier lřutilisateur et pour générer les clefs de chiffrement et dřintégrité utilisées entre le terminal et le réseau. Les messages SIP envoyés entre le terminal et le P-CSCF sont chiffrés et protégés par ces clefs de chiffrement et dřintégrité.

Lřétat de lřart de lřIMS montre son architecture, ses différentes composantes et leur fonctionnement dans le système. La fiabilité de chaque entité que constitue lřIMS montre sa robustesse et sa capacité à assurer la convergence et offrir les services à valeur ajoutée de qualité requise aux utilisateurs finaux. LřIMS demeure le socle pour les réseaux de nouvelle génération, permet de réaliser la convergence Fixe/Mobile/Internet et garantit la satisfaction des clients et les opérateurs en tire profits. Lřinterconnexion de lřIMS avec le WebRTC offre une autre bonne possibilité à exploiter pour lřamélioration de lřoffre de services aux utilisateurs.

3.7. Interconnexion d'un réseau IMS avec un réseau basé sur WebRTC

Le standard WebRTC propose les mêmes services que lřIMS avec lřavantage dřinstaller un navigateur, connait un essor. Nous montrons dans ce paragraphe, la possibilité de lřinterconnexion dřun réseau IMS avec un réseau basé sur WebRTC, qui fournit de services de riches communications à lřaide des navigateurs sans lřinstallation de logiciel chez les utilisateurs. Le développement rapide de lřInternet a ouvert la porte à lřapparition de nouvelles applications, mais aussi de nouvelles technologies du web : le **WebRTC**. Cřest une interface qui permet des communications temps réel dans le Web à partir des navigateurs sans nécessiter lřajout de nouveaux plugins. Nous parlerons de la technologie WebRTC, les composantes de son architecture et de son plan de signalisation, les protocoles sous-jacents ainsi que la communication centrée sur lřIMS supportant les points de terminaison WebRTC.

3.7.1. La technologie WebRTC

Le WebRTC est une technologie, elle constitue une plateforme qui permet d'effectuer des communications temps réel de façon pair-à-pair au moyen des navigateurs en utilisant les API JavaScript. Le WebRTC rend effectif les services temps réel tels que les appels vocaux, la vidéoconférence, le chat, et même les services de partages de ressources (fichiers, écrans…) au moyen des navigateurs en temps réel sans passer nécessairement par des protocoles propriétaires et ne nécessite pas dřinstallation de plugins additionnels **[39]**. Cřest un projet initié par le groupe de travail RTCWeb de l'IETF qui vise à intégrer dans les navigateurs des plugins permettant des communications en temps-réel (figure 3.9).

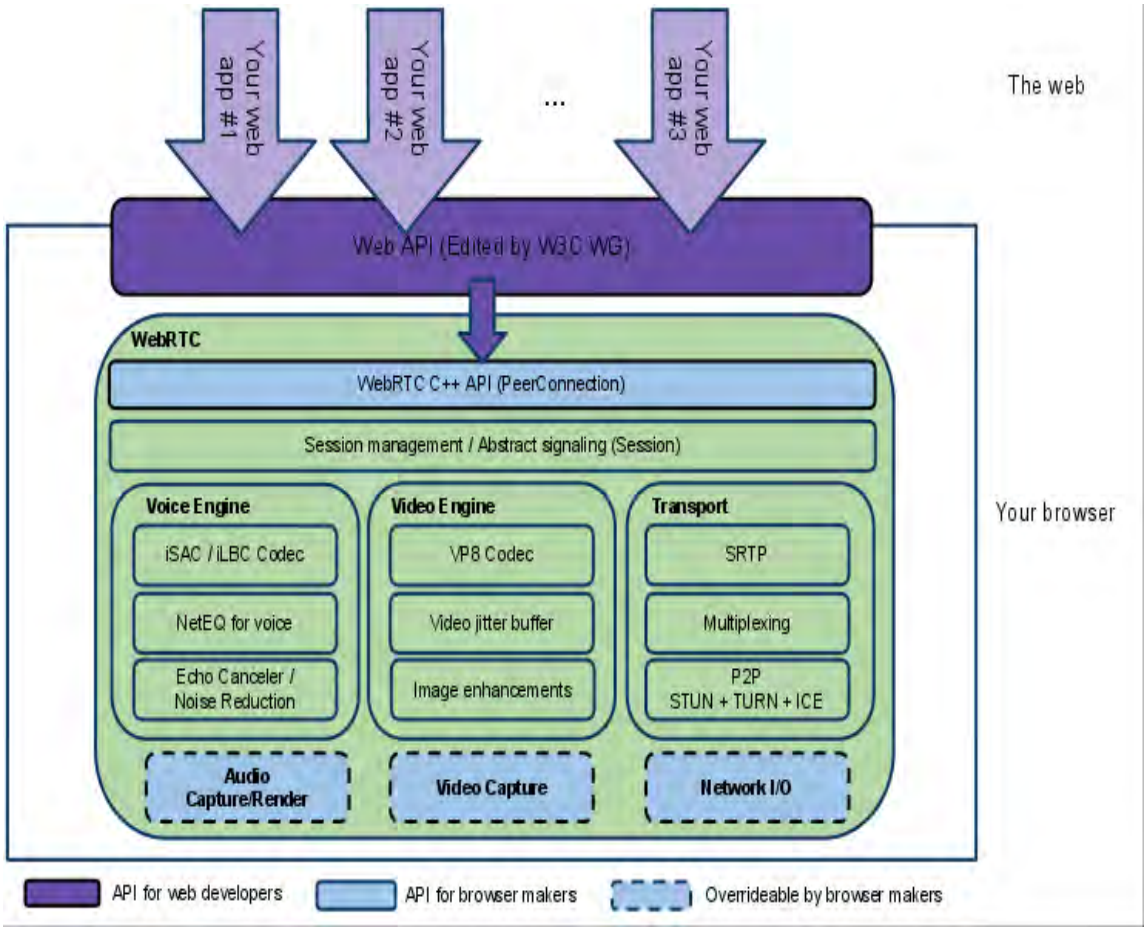


Figure 3.9. Architecture WebRTC

3.7.2. Signalisation du WebRTC et Plan de signalisation WebRTC

Signalisation du WebRTC :

Le WebRTC est un média engine avec des API javascripts. Les communications dans le WebRTC étant pair-à-pair, cela nécessite qu'il y ait un serveur de signalisation qui doit être mis en place pour la coordination et permet aux navigateurs de communiquer. Plusieurs navigateurs web disposant des plugins WebRTC échangent des données par le biais des canaux médias pair-à-pair établis directement entre les deux pairs. Le WebRTC n'a pas défini un protocole de signalisation spécifique ni la manière dont la signalisation va être établie **[39]** (figure 3.10).

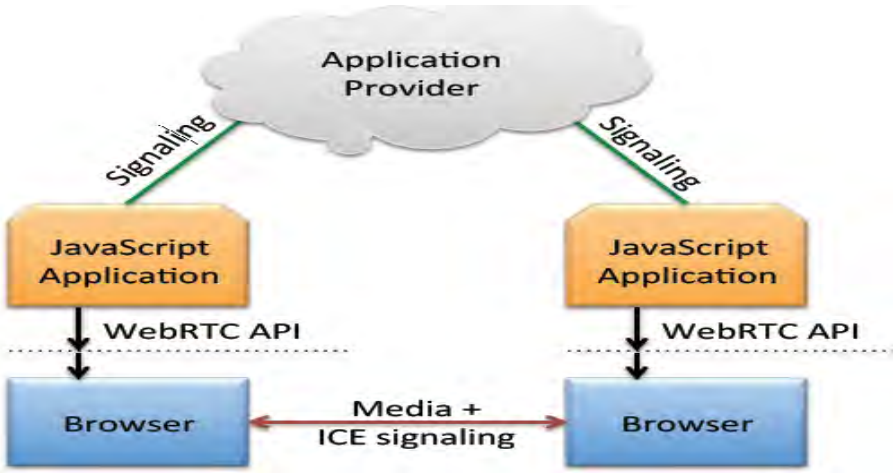


Figure 3.10. Signalisation dans le WebRTC

Plan de signalisation WebRTC :

La signalisation dans le WebRTC décrit le mécanisme pour coordonner la communication et envoyer les messages de contrôle de session, de configuration du réseau, de capacités des médias. Dans la procédure d'établissement de connexion entre pairs WebRTC, trois (3) types d'informations sont échangés via un canal de signalisation :

- **le contrôle de session média** : son rôle est d'établir et de libérer la communication ;
- **la configuration réseau des nœuds** : cette procédure identifie le socket c'est-à-dire détermine l'adresse IP et le numéro de port en utilisant un serveur NAT ;
- **les capacités multimédias des nœuds** : cette procédure détermine les médias supportés, les codecs disponibles, les serveurs de noms supportés (pour la résolution), la fréquence d'envoie des paquets. Le transport des flux multimédias est effectué si les trois procédures de signalisation citées ci-dessus sont correctement échangées et négociées **[40]**.

3.7.3. Les différentes signalisations WebRTC et leur transport

- **Signalisation XHR :** plusieurs approches sont utilisées pour expliquer le mécanisme de la signalisation dans le WebRTC parmi lesquelles il y a la signalisation XHR. Il s'agit d'une signalisation à base de polling HTTP. Des appels ou méthodes XML HTTP Request (*XHR*) sont utilisés au sein de JavaScripst permettant à une application

JavaScripts de générer une nouvelle requête HTTP à un serveur et de traiter les réponses. La XHR est une API standardisée par le W3C. Elle est utilisée pour envoyer des requêtes au format XML ou JSON. L'API XHR spécifie les méthodes à utiliser pour générer une nouvelle requête HTTP ou HTTPS. L'utilisation de XHR comme canal de signalisation pour le WebRTC nécessite que le serveur exécute une application qui reçoit les requêtes HTTP et transmet les informations reçues d'un navigateur à un autre sur un autre canal XHR. Les messages de signalisation sont échangés par JavaScripts qui envoient des requêtes HTTP au serveur de signalisation à des intervalles réguliers pour l'interroger. Le navigateur envoie les informations de signalisation dans la méthode HTTP POST. Cependant, les messages de signalisation reçus par le serveur sont inclus dans la réponse 200 OK associé à la méthode POST.

- **Signalisation Websocket *:*** la montée importante d'interaction entre les applications sur Internet et les sites Web, utilisant le mode de communication HTTP, montre que le protocole HTTP présente des limites par rapport aux ouvertures et maintiens des connexions TCP dans les interactions client/serveur. AJAX propose des techniques et un rafraîchissement du contenu Web. A lřorigine, les communications dans le Web sont unidirectionnelles. Le client initie toujours la communication en envoyant des requêtes et le serveur fournit une réponse après le client l'affiche. LřIETF a standardisé un nouveau protocole TCPWebSocket qui permet les communications bidirectionnelles dont l'API a été implémentée au niveau des navigateurs. Un client connecté à un serveur Web peut lui envoyer et recevoir des messages. La connexion est alors établie de façon persistante.
- **Signalisation SIP Over Websocket *:*** les communications Web sont basées sur le protocole HTTP en utilisant la méthode HTTP GET accompagnée d'une requête upgrade. Le message est envoyé par le client et acquitté par le serveur avec un code de réponse 101 si la négociation aboutie. Une fois que la phase de négociation est terminée, le protocole de communication passe de HTTP à WebSocket. Pendant la phase dřinitiation de connexion, le client et le serveur s'accordent sur le protocole à utiliser au-dessus de WebSocket **[41]**.
- **Transport de la signalisation WebRTC *:*** les communications dans le WebRTC sont effectuées à partir des navigateurs. Le protocole HTTP est utilisé dans le Web pour

l'échange entre le client Web et le serveur Web. De ce fait, le protocole HTTP peut être utilisé pour le transport des messages de signalisation.

3.7.4. Les API WebRTC et les protocoles sous-jacents

Les API WebRTC :

Le WebRTC est un environnement qui permet d'effectuer des communications multimédias temps réels au moyen des navigateurs. L'activation de la caméra et du micro se fait au moyen des APIs javascript **[41].** Les principales fonctions des API WebRTC sont :

- **GetUserMedia** : elle est utilisée pour l'obtention du média (*détection et activation de la caméra et du micro*). Elle est chargée de gérer les flux médias. Elle capture les flux audio/vidéo et accède à partir du fureteur aux périphériques caméra, micro et les active ;
- **RTCPeerConnection** : elle est chargée des flux de signalisation, permet d'établir la connexion entre les pairs. Elle gère la sémantique, le format (codage et décodage) des médias, les mécanismes de traversée de NAT ;
- **RTCDataChannel** : elle gère l'échange des données, transfert des données (flux audio, vidéo, ...).

Les protocoles sous-jacents :

Le protocole **ICE** est défini dans la **RFC 5245**, il s'appuie sur les protocoles **STUN** et **TURN**. Il décrit comment les pairs communiquent entre eux. Il permet de déterminer lřadresse IP et les ports externes des pairs. Lorsque les pairs se trouvent derrière un routeur NAT ou un pare-feu, ICE utilise des techniques basées sur les protocoles STUN et TURN. Son fonctionnement repose essentiellement sur la découverte des adresses IP et les ports utilisables pour établir la communication.

3.8. Communication centrée sur IMS supportant les points de terminaison WebRTC

La convergence a au-delà des normes et son aboutissement pousse à la recherche dřinteropérabilité entre les points dřextrémité traditionnels et ceux orientés vers le Web donnant ainsi la possibilité dřexplorer de nouvelles fonctionnalités telles que les services multimédias. Les auteurs du **[42]** ont proposé un prototype intégré lřIMS dont ils ont fait une

évaluation en termes de débit dřappel et du retard de bouche-oreille induit par le système. Il est clair que lřévolution des architectures des réseaux de télécommunication augmente les possibilités de créer des services orientés Web. Il y a aujourdřhui les services OTT haut de gamme, non intégrés aux réseaux de télécommunications traditionnels, cela réduit la portée et le cadre dřutilisation de ces services**.** Les auteurs parlent dřOneAPI (*du Groupe Special Mobile Association*) comme solution à standardiser pour les opérateurs de télécommunications, car elle intègre les fonctionnalités de contrôle dřappel, de facturation, de localisation et de découverte de capacités. Dřun côté, le WebRTC définit beaucoup dřAPIs qui développent des services multimédias accessibles directement dans les navigateurs. Le renforcement du lien entre le réseau traditionnel et lřInternet de lřarchitecture du sous-système multimédia IP du 3GPP motive lřidée dřune intégration ou interopérabilité WebRTC-IMS. Les auteurs ont proposé une architecture dans laquelle ils ont intégré des points dřextrémité (endpoints) du WebRTC avec ceux des réseaux IMS **[42] [43].** La vision décrite par les auteurs **[42]** montre essentiellement la mise en place dřun système dřappel entre le WebRTC et lřIMS avec la gestion du média, en utilisant deux SDK et une passerelle vers laquelle se connectent les clients. Cette architecture présente lřavantage quřaucun composant du réseau nřest nécessaire à part la passerelle pour gérer les médias. Lřarchitecture de référence adoptée (figure 3.11) en vue de la mise en œuvre de la passerelle IMS-WebRTC dont les différents éléments qui la constituent sont définis ci-dessous :

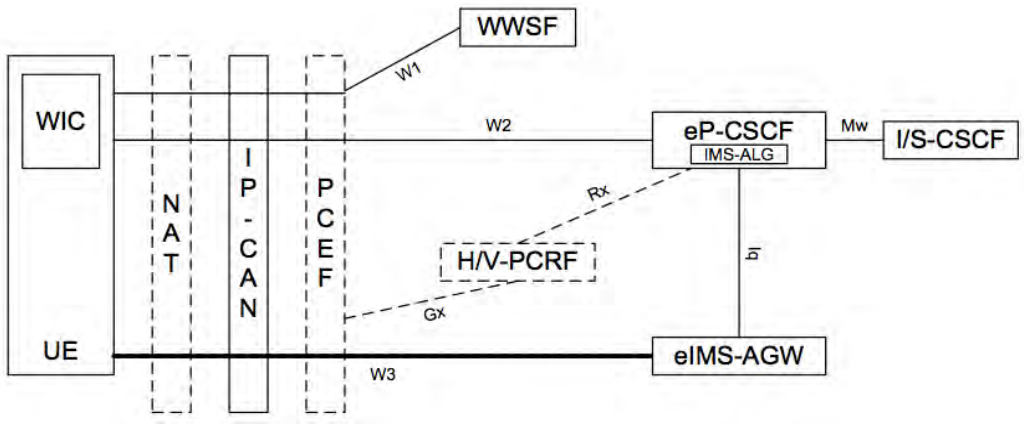


Figure 3.11. Architecture WebRTC IMS

3.8.1. Les composantes de l'architecture WebRTC-IMS

- **WebRTC IMS Client *(WIC)* :** le **WIC** est l'application WebRTC basée sur Javascript. Elle est téléchargée à partir de la fonction WWSF au sein du réseau de l'opérateur ou d'un réseau tiers. Il fournit une logique applicative et des appels API WebRTC pour accéder aux services de communication du système IMS. Le WIC fonctionne sur tout périphérique prenant en charge un navigateur (*ou un environnement d'exécution JS équivalent pour applications mobiles ou décodeurs*) prenant en charge WebRTC sur tout réseau d'accès IP connecté à Internet.
- **User Equipment (*UE*) *:*** cřest un dispositif ou l'application utilisée par l'abonné pour interagir avec le noyau IMS pour émettre et recevoir des appels, envoyer un message instantané, l'état de présence, etc. Grâce à la technologie WebRTC, lřUE peut être une application Web (*WIC dans la terminologie IMS*) fonctionnant sur un navigateur avec des capacités WebRTC.
- **Network Address Translation (*NAT*)** : le client WebRTC (WIC) sera normalement derrière un élément NAT, de sorte qu'une zone NAT a été incluse dans le diagramme. Lř**ICE** est le protocole implémenté par le WebRTC pour permettre des flux SRTP bidirectionnels derrière le NAT, de sorte que la passerelle de média utilisée pour échanger des flux de média avec le cœur IMS doit le prendre en charge.
- **IP Connectivity Access Network (*IP-CAN*)** *:* Le réseau d'accès à la connectivité IP (*réseau IP simple*) utilisé pour atteindre le cœur IMS par lřUE. Cřest peut-être le LTE pour les mobiles mais aussi le DSL et le Wireless LAN / WiFi**.**
- **WebRTC Web Server Function (*WWSF*)** *:* la fonction de serveur Web WebRTC (*WWSF*) peut être située dans le réseau de l'opérateur ou dans un réseau tiers. Cřest le premier élément contacté par l'utilisateur et à partir duquel le client Web (*WIC*) est téléchargé. Alternativement, il peut implémenter des fonctions avancées ou s'intégrer à d'autres éléments déployés dans le réseau. Certaines de ces options incluent :
  - ✓ Fournisseurs d'identité pour la gestion de l'identité basée sur le Web ;
  - ✓ Le HSS pour la synchronisation / mappage des identités Web et IMS ;
  - ✓ Serveurs d'applications pour l'intégration avec des services basés sur lřAPI ;
  - ✓ Serveurs d'authentification pour contrôler l'accès ;
  - ✓ Active Directory pour la synchronisation des listes de contacts ;

- ✓ Intégration du OSS et du BSS pour la gestion de réseau de bout en bout et le contrôle des éléments.

Certains font référence à la WWSF en tant que contrôleur d'application WebRTC (*WAC*).

- **P-CSCF enhanced for WebRTC (*eP-CSCF*)** *:* dans lřIMS, la fonction P-CSCF est un élément bien connu. La fonction P-CSCF est le point d'entrée des demandes SIP dans le système IMS à partir de l'UE. Pour prendre en charge le client WebRTC, le 3GPP propose d'ajouter à la fonction P-CSCF la capacité de réception de SIP sur Websocket (SIPoWS) définie dans la **RFC 7118**. Le SIPoWS est le seul mécanisme explicitement mentionné, mais la spécification laisse la porte ouverte à d'autres alternatives de signalisation, telles que JSONoWS. En bref, cette fonction est la passerelle de signalisation qui adapte la signalisation utilisée par le WebRTC au protocole IMS-SIP standard vers le cœur.
- **IMS Access GateWay enhanced for WebRTC (*eIMS-AGW*)** *:* semblable à la passerelle de signalisation, lřeIMS-AGW est une norme IMS-AGW qui prend en charge le support WebRTC tel que défini par l'IETF. Il sřagit essentiellement de la fonction de passerelle multimédia WebRTC qui doit effectuer plusieurs adaptations :
  - ✓ **DTLS-SRTP** : le DTLS sur le plan des supports est utilisé dans l'échange WebRTC des clés qui seront utilisées pour chiffrer les flux SRTP tandis que SDES utilisé dans lřIMS, échange les clés sur le plan de la signalisation si le chiffrement est utilisé ;
  - ✓ **DataChannel** : il relaye les données DataChannel et convertit éventuellement le MSRP ou le BFCP en DataChannel ou relaye ces données via d'autres moyens Web ;
  - ✓ **Transcodage audio / vidéo** : aujourd'hui, seul le codec vidéo VP8 est pris en charge. Il est donc nécessaire de traduire en H.264, le codec pris en charge par les UE IMS dotés de capacités vidéo ;
  - ✓ **Multiplexage RTCP** : le WebRTC prend en charge le multiplexage audio / vidéo et le RTP / RTCP sur la même session et le même port RTP, ceci n'est pas pris en charge dans lřIMS et est donc nécessaire pour effectuer le démultiplexage.

LřeIMS-AGW doit non seulement assurer la prise en charge des réclamations de WebRTC auprès de l'UE, mais également prendre en charge les candidats à la négociation ICE, notamment STUN et TURN.

- **La fonction de règles de politique et de facturation (PCRF) et la fonction d'application de politique et de facturation (PCEF) :** la fonction **PCRF** est lřélément de lřarchitecture IMS qui prend en charge les décisions de politique et de contrôle de taxation basées sur les informations relatives à la session et aux médias obtenues de la fonction P-CSCF. La PCRF parle de DIAMETER avec un autre élément, la **PCEF** effectue une inspection approfondie des paquets, analyse le trafic intitulée **DPI** (*Deep Packet Inspection*) et décide, en fonction des règles, si le trafic est autorisé ou non. Les supports WebRTC étant cryptés et pouvant même être multiplexés sur les ports 80/443, la résolution DPI peut s'avérer délicate. Le H/V-PCRF dans le diagramme fait référence à PCRF local et au PCRF visité dans le cas d'un abonné itinérant.

Dans cette configuration des possibilités quřoffrent lřIMS et le WebRTC, une approche globale permet de comprendre leur importance dans les systèmes convergents de télécommunication.

3.9. Approche sur l'importance de l'IMS dans les systèmes convergents de télécommunication

LřIMS a permis de réaliser la convergence des réseaux et systèmes des opérateurs et fournisseurs de services. Il interconnecte les systèmes basés sur les technologies des opérateurs des télécommunications et les systèmes de communication basés sur les technologies Internet. Il nřy a plus de limites entre les télécommunications et lřinformatique, un avantage pour les opérateurs. LřIMS demeure un système fédérateur de systèmes de communication. Il a permis :

- La première convergence des systèmes de télécommunications, dřaudiovisuel et dřinformatique ;
- La deuxième convergence des systèmes de communications sur le Web ;
- Enfin, la convergence de ces deux grandes familles énumérées ci-dessus.

En effet, lřIMS a été créé pour répondre à un enjeu qui est de proposer aux clients finaux des services à valeur ajoutée. Ceci nřest possible quřavec une plateforme de communication multimédia standardisée, se basant sur les recommandations formulées par lřUIT-T. Il sřagit de regrouper deux mondes :

- **Internet :** lřInternet a eu un fort impact sur le développement de nouveaux usages et services. Lřinterconnexion de réseaux a permis lřémergence dřune multitude dřapplications accessibles à un grand nombre dřutilisateurs. De lřéchange et lřaffichage dřinformations au format texte, nous sommes arrivés à des applications enrichies tels que les logiciels de bureautique ou vidéoconférence accessibles depuis un navigateur Web. Il est aisé de réaliser des applications temps réel avec le WebRTC, puisque la qualité de service est assurée de bout en bout. Beaucoup dřoutils de communication grand public à travers le Web utilisent le **standard WebRTC**. Parmi lesquels :
  - **Teams de Microsoft** : il permet de faire du télétravail ;
  - **BigBlueBouton** : il est utilisé fortement en milieu universitaire pour les cours synchrones (classes virtuelles) ;
  - **Google meeting : il est** intégré par défaut sur les comptes gmail permettant aux utilisateurs de faire de conférences multimédia sur le Web.

A cause de COVID-19 qui sévit, le télétravail en confinement est privilégié grâce à ces outils qui sont disponibles et qui facilitent la tâche de beaucoup dřentreprises, dřinstitutions nationales et internationales.

Grâce à cette convergence, les opérateurs de communication sur Internet montent en puissance par lřutilisation des ces outils performants mais aussi un volume de données importantes transite sur le Web.

Nous avons commencé ces travaux de recherche depuis quelques années et beaucoup dřaspects abordés se réalisent aujourdřhui tel que le WebRTC très utilisé dans les communications sur le Web et prend une place importante.

Les objets connectés vont beaucoup utiliser le WebRTC et vont monter en puissance et en voulant les interconnecter cela va nécessiter que le réseau soit fiable dřoù lřintérêt de veiller à la fiabilité du réseau.

- **Les réseaux de télécommunications** : ils sont de vastes réseaux fermés mais maitrisés. Les contraintes dřacheminement des données sont totalement maitrisées mais les nouvelles applications se font rares.

Lřarchitecture de lřIMS permet de fusionner ces deux mondes pour avoir : un réseau performant, maîtrisé et ouvert aux nouvelles applications.

Ainsi, nous pouvons nous connecter avec nos terminaux aux réseaux classiques, aux réseaux mobiles 2G, 3G et 4G et même à lřInternet grâce à lřIMS. Avec la convergence, tout opérateur 2G ou 3G qui veut migrer vers la 4G, le déploie grâce à lřIMS car il permet lřinteropérabilité des systèmes.

Dans le contexte de la convergence, lřIMS devient ainsi le fédérateur des réseaux téléphoniques classiques, mobiles, la télévision numérique et le Web. LřIMS demeure le socle de la plateforme de télécommunications, **gage d'émergence numérique.** Il joue un rôle très important dans le système des télécommunications et permet lřintégration de tout type de système de communication. Grâce à lřIMS, les opérateurs de services haut débit, Tout IP, offrent de services en toute mobilité aux utilisateurs (figure 3.12).

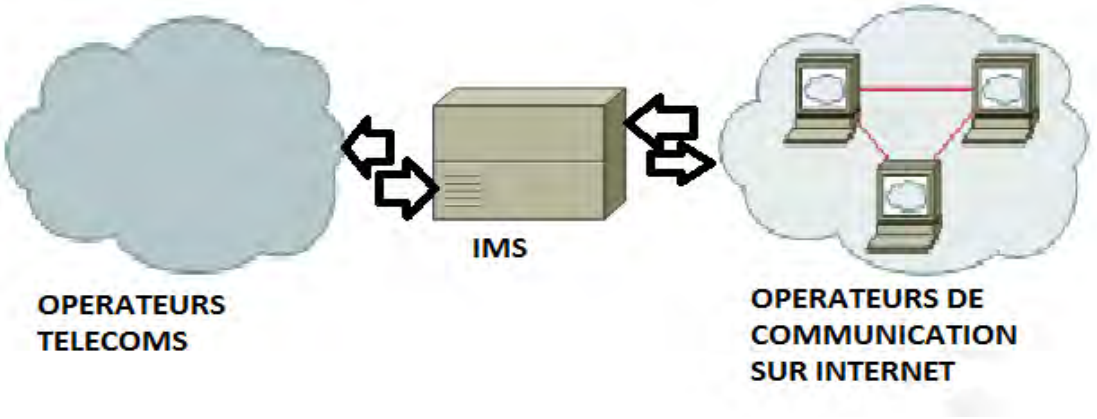


Figure 3.12. Approche de systèmes convergents de télécommunications

3.10. Conclusion

Dans les chapitres précédents, la convergence des réseaux mobiles et fixes est une réalité. LřIMS a prévu une passerelle de connexion avec le WebRTC pour accéder aux services Internet. LřIMS et le WebRTC sřinterconnectent pour offrir de services à valeur ajoutée. Le WebRTC a donné naissance à une nouvelle forme de communication dans le Web. Les

communications entre utilisateurs dans le Web par le biais des navigateurs sans ajout de plugins additionnels, font du WebRTC une technologie du futur pouvant être exploitée dans les réseaux de télécommunications (*LTE*) mais également dans les universités numériques pour favoriser lřapprentissage en ligne. Le fait quřaucun protocole de signalisation ne soit précisé, laisse le libre choix à lřusage de nřimporte quel protocole de signalisation. LřIMS et le WebRTC constituent des outils de recherche et de production, une contribution scientifique significative dans le monde de TIC. LřIMS a permis lřinterconnexion des réseaux mobiles/fixes et Internet. Il joue un rôle important et permet lřintégration de tout type de système de communication. Ceci renforce lřidée de bien veiller sur sa fiabilité. LřIMS est bien au cœur de la convergence des réseaux de nouvelle génération. Dans le cadre de cette thèse, après avoir fait lřétat de lřart de lřIMS, nous présentons lřenvironnement et les outils de recherche déployés ci-dessous.

Chapitre 4 : Présentation de l'environnement et outils de recherche

Notre travail de recherche porte sur lřétude de la fiabilité de systèmes convergents et leurs applications. Dans ce chapitre, nous présentons lřenvironnement de recherche ainsi que les outils utilisés dans cette étude.

Nous avons vu dans les chapitres précédents, lřimportance de lřIMS dans les réseaux mobiles et fixes ainsi que dans le Web. Nous sommes arrivés à la conclusion que lřIMS demeure le socle pour les systèmes convergents en vue de fournir de services à valeur ajoutée.

Pour réaliser nos travaux, nous ne pouvons utiliser des outils propriétaires qui ne donnent pas beaucoup de possibilités de simulations. Cependant le monde libre en offre beaucoup. Les acteurs du monde libre se sont mis ensemble pour développer des solutions basées sur les logiciels libres tels que : Asterisk, Freeswitch, Kamailio, Clearwater, OpenIMSCore, Kurento, WebRTC, OpenEPC etc…

En effet, il faut rappeler que lřémergence des logiciels de communication mobile open source a transformé les industries des télécommunications ces dernières années. Un mouvement pour introduire l'open source à la télécommunication, a commencé quand Mark Spencer a créé un commutateur téléphonique open source appelé **Asterisk** en 1999. Depuis lors, dřautres ont suivi les pas de Spencer (*Bloomberg, 2006*). Un certain nombre dřentreprises et dřinstituts de recherche ont développé des solutions open source projets. **Range Networks**, **Sysmocom**, **Core Network Dynamics**, **Fraunhofer FOKUS** et **EURECOM** comptent parmi les entreprises et instituts de recherche les plus notables qui ont été à la production d'un projet de logiciel de communication mobile open source au cours des dernières années. Lřexemple de la combinaison d'un logiciel de communication mobile open source avec une radio définie par logiciel (*SDR*), offre la possibilité de réaliser un système cellulaire à coût minimum, en termes de coût, de temps et de flexibilité.

Lřintroduction de lřinformatique en général et des logiciels libres en particulier, ont permis dřintégrer les standards qui sřappuient sur les RFC pour développer les fonctionnalités et voir leurs limites afin de les améliorer. Aujourdřhui, nous disposons de plateformes qui permettent de voir la pertinence des standards. Le fait que les logiciels libres respectent les standards, cřest une chance unique pour les chercheurs africains dřapporter leurs contributions grâce aux

logiciels libres. Comment mettre à lřévidence la non-performance ou la non-fiabilité dřun système ? Alors quřavant, il fallait sřappuyer sur les constructeurs, les équipementiers pour évaluer la performance ou la fiabilité dřun système. Aujourdřhui, lřimportance de ces logiciels libres dans le domaine de la recherche nřest plus à démontrer car beaucoup des travaux de recherche lřont prouvé. Enfin, nous terminerons ce chapitre par une conclusion.

4.1. Mode de collaboration et développement du logiciel

Les logiciels libres sont aujourd'hui omniprésents dans les architectures informatiques modernes. Au cours de ces dernières années, l'intégration de logiciels libres dans une très vaste gamme de solutions a été effective et a contribué considérablement dans le domaine des télécommunications. Les grands consommateurs de logiciels, en font déjà largement usage et apprennent à s'adapter aux caractéristiques de ce nouvel environnement. Ainsi, lřadoption des solutions libres dans le domaine de TIC en général et de télécommunications en particulier, ont été démontré dans plusieurs systèmes déployés et ont donné pleine satisfaction.

Quelques solutions de logiciel libre ont été utilisées par des grandes firmes des opérateurs de télécommunications. Il sřagit de lřutilisation dřune version améliorée de mysql comme base de données HLR chez certains équipementiers, KANNEL a été longuement utilisé par des opérateurs pour déployer de services à valeur ajoutée.

En effet, de façon générale, un logiciel peut être considéré « **libre** » s'il est possible :

- de lřexécuter pour n'importe quel usage ;
- dřavoir accès à son code source ;
- dřen étudier le fonctionnement et de l'adapter à des besoins spécifiques ;
- dřen redistribuer des copies originales ou modifiées. Une caractéristique essentielle des logiciels libres est l'accessibilité du code source.

Lřune des principales raisons qui poussent de nombreuses entreprises à s'ouvrir aux logiciels libres est leur volonté de bénéficier des avantages associés au mode de développement collaboratif qui les caractérise. Le développement d'Internet a favorisé l'apparition de cette nouvelle forme de développement logiciel, où chaque utilisateur est en mesure d'apporter sa contribution. L'évolution des logiciels libres s'opère en ligne et toute personne intéressée est en mesure d'y prendre part. Ce mode de développement ouvert, encourage la collaboration entre ceux-ci afin de concevoir, de déboguer et dřoptimiser les logiciels qu'ils partagent et utilisent en commun. Certains laboratoires de recherche exploitent les avantages du

développement collaboratif de ces logiciels libres pour atteindre leurs objectifs dans lřamélioration des systèmes qui existent.

4.2. Quelques logiciels libres de télécommunications utilisés dans la recherche

Lřaccent est mis sur les logiciels libres utilisés dans le domaine de télécommunications et leur importance dans le domaine de la recherche. Quelques logiciels libres tels que : **Asterisk**, **Freeswitch**, **Kamailio**, **Clearwater**, **OpenIMSCore**, **Kurento**, **WebRTC**, **OpenEPC** ont fait leurs preuves dans le domaine de la recherche et ont apportés une plus-value aux systèmes convergents de télécommunications. Une description de chaque logiciel permet de mieux les situer et comprendre leur utilité dans les systèmes convergents actuels.

- **Astérisk**

LřAstérisk est la solution IPBX Open Source la plus utilisée sur le marché de la téléphonie IP à lřheure actuelle. Certains projets Open source dont Astérisk a permis de donner naissance comme Bayonne, Callweaver, Freeswitch et dřautres encore. Cřest un logiciel libre (*Open Source*), publié et créé par Mark Spencer de la société Digium en 1999. Il tourne sur Linux, BSD et Mac OS X. LřAsterisk offre tous les services de téléphonie « classiques » dřun PABX ainsi que des fonctions avancées :

- ✓ boîte vocale (avis par courriel de réception dřun message vocal, voyant indicateur de message en attente…) ;
- ✓ conférence téléphonique ;
- ✓ serveur vocal interactif ;
- ✓ applications CTI (*Couplage Téléphonie Informatique*) (ex : possibilité de composer un numéro de téléphone à partir du carnet dřadresses dřOutlook) ;
- ✓ visiophonie ;
- ✓ rapport détaillé sur les appels.

LřAsterisk utilise différents protocoles afin de faire de la téléphonie, tels que SIP ou encore H323 et IAX. Il permet lřinteropérabilité avec les téléphones traditionnels mais aussi lřinteropérabilité matérielle avec RTC, RNIS, Wi-Fi, Ethernet, Bluetooth et les cartes son.

Avantages de l'Astérisk :

Le logiciel Asterisk présente plusieurs avantages. Le premier est avant tout son coût. En effet, issue du monde libre, lřAsterisk et lřensemble des paquets qui lui sont rattachés sont

disponibles en téléchargement gratuit sur Internet. La configuration dřAsterisk est également un avantage car elle se résume essentiellement à quelques lignes de commandes à rajouter dans des fichiers, et la communauté Linuxienne permet grâce aux différents forums de sřapproprier assez rapidement ces commandes et donc cette configuration. Il permet également de passer sur le réseau RTC (*téléphonique commuté*) via des cartes de téléphonie type PCI à incorporer au serveur.

Enfin, lřAsterisk propose toutes les fonctionnalités ou presque dřun commutateur PABX classique.

Inconvénients de l'Astérisk :

LřAsterisk dispose néanmoins dřun inconvénient majeur. En effet, son utilisation est dédiée uniquement aux plateformes Linux. Aujourdřhui, de plus en plus de serveur dispose de système Linux tel que Debian ou encore Red Hat. Néanmoins, Windows est le plus souvent présent dans les petites entreprises et cela peut être un frein au développement de cette solution. Une solution Asterisk sous Windows a été annoncée mais la version la plus stable reste actuellement celle sous Linux.

La mise en place de manière très efficace dřun service de téléphonie sur IP, Open Source est entièrement gratuite, avec le logiciel Asterisk. Vous trouverez aussi toutes les étapes conduisant à assurer la continuité de service 24h/24h et 7j/7j grâce à des logiciels déjà existant ou à des petits scripts à écrire nous-même [44] [45] [46] [47] [48] [49] [50].

- **Freeswitch**

Le Freeswitch est une solution open source de téléphonie sur IP, sous licence MPL, développé en C. Elle permet la mise en place des communications vers un téléphone virtuel via un commutateur virtuel. Il peut être utilisé comme un simple commutateur, un PBX, une passerelle ou un serveur dřapplication IVR utilisant des scripts ou des fichiers XML permettant dřautomatiser certaines tâches et de développer des nouveaux services.

Le Freeswitch, cřest lřautre géant de téléphonie Open Source. Cette plateforme est évolutive et permet de relier entre eux plusieurs moyens de communication (audio, vidéo, texte...). La gamme dřoutils open source de Freeswitch permet un développement dřapplications quasiment infini. Lřinitiateur de ce projet est Anthony Minessale avec lřaide de Brian West et Michael Jerris qui étaient tous les trois développeurs chez Astérisk. Lřadaptabilité et la stabilité sont maitres mots de ce projet. Le Freeswitch fonctionne sur plusieurs systèmes dřexploitation, notamment Windows, Mac OS X, Linux, BSD et sur les deux plateformes

Solaris (32 bits et 64 bits). Une interface Web pour Freeswitch est disponible sous le nom de Wiki PBX.

Le Freeswitch supporte les caractéristiques standards et avancés du protocole SIP, permettant de mettre en place un serveur de conférence, un serveur du Voicemail…, il utilise aussi les protocoles IAX2, Jingle et H323 [51].

- **Kamailio**

Le projet SIP Express Router 2 (*SER*) a été lancé en 2001. En septembre 2002, il a été publié pour la première fois. En juin 2005, le Kamailio a été créé en tant que séparation de SER, dans le but de créer un serveur SIP Open Source, robuste et évolutif. Son nom initial était OpenSER mais en raison de problèmes de copyright, le 28 juillet 2008, il a été renommé Kamailio.

En novembre 2008, l'équipe de développeurs Kamailio et SER s'est réunie pour intégrer les deux serveurs SIP. L'intégration se termine par sa version 3.0.0 dans laquelle les deux codes de développement sont réunis en un seul. En d'autres termes, Kamailio et SER deviennent la même application du point de vue du code source, bien qu'ils diffèrent par le nom choisi lors de la construction de l'application et par les modules par défaut chargés dans leur fichier de configuration.

Le Kamailio est un Server SIP open source. Ce fork du projet OpenSER (en 2005) est l'un des PBX les plus complets. Il supporte des transactions asynchrones, TCP, UDP et SCTP, l'encryptage des communications via TLS, la répartition de charge, un mécanisme natif de fail-over, l'authentification sur des backend Radius, Mysql, LDAP ou via transport XMLRCP. Il est utilisé aussi bien par des opérateurs télécoms comme plate-forme de service VoIP que pour les solutions classiques de téléphonie d'entreprise. C'est une alternative à Freeswitch et Asterisk les deux autres poids lourds du domaine.

Le Kamailio SIP server est un logiciel open source leader pour la création de services SIP tels qu'un proxy SIP, un serveur de présence SIP, un serveur de localisation SIP et bien plus encore. Avec une configuration riche, la modularité et le développement continu, le Kamailio est le choix pour la construction d'entreprises ainsi que des solutions de support. Le Kamailio fonctionne sur les systèmes Unix et Linux, allant des systèmes intégrés aux serveurs multi-core à grande échelle. Il est le résultat de plus de dix (10) ans de développement, dans le projet SIP Express Router (SER), le projet Open SER et le projet SIP Router. Le Kamailio est le résultat d'une fusion de plusieurs projets, un processus de collaboration qui a démarré le 4

novembre 2008 **[36]**. Le Kamailio est publié sous GNU Public License v2 (*GPLv2*). À partir de 3.0.0, l'application comprend des parties du code sous licence BSD qui peuvent être utilisées telles que des composants individuels.

Il est capable de gérer des milliers dřappels par seconde. Il est caractérisé par la communication sécurisée via TLS pour la VoIP (voix, vidéo), la messagerie instantanée et notification de présence, le routage, lřéquilibrage de charge, la comptabilité, lřauthentification et lřautorisation avec MySQL, le postgrès, lřOracle, le Radius, le LDAP. Depuis la version 4 des extensions lui ont été ajoutées afin dřimplémenter les serveurs P-CSCF, I-CSCF et S-CSCF. Les entités de cœur du réseau tels que : lřE-CSCF et le HSS ne sont pas encore implémentées.

Aujourdřhui le code du logiciel est la version 5.0.3. Le diagramme suivant de la figure 4.1 montre quelles parties de l'arbre source du routeur SIP sont incluses dans les paquets binaires (le tarball source comprend tout) **[52].**

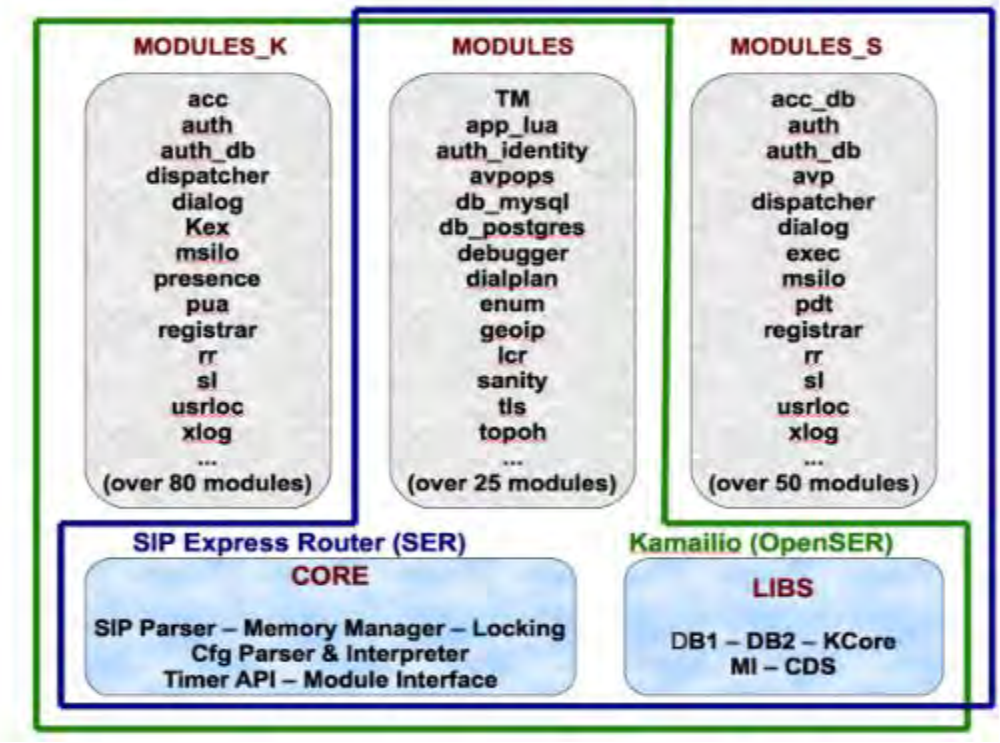


Figure 4.1. Pile de module Kamailio et SER

- le binaire principal est compilé et installé avec le nom « **kamailio** ». Le fichier de configuration par défaut est « **kamailio.cfg** » qui a le mode de compatibilité KAMAILIO réglé ;

- la configuration par défaut implémente les mécanismes dřauthentification, la traversée de NAT, prise en charge de la présence, etc. avec des modules spécifiques Kamailio. Les outils « **kamctl** » et « **kamdbctl** » sont installés. Les pages de manuel sont nommées « kamailio » et « kamailio.cfg ». Les fichiers de configuration sont situés dans **/usr/local/ etc /kamailio/** (ou **/etc/kamailio/** si installé à partir de paquets) ;
- les libs et les modules sont situés dans **/usr/local/lib/kamailio/** (ou **/usr/lib/kamailio/** si installé à partir de paquets). Les chemins des modules peuvent varier en fonction de lřarchitecture et de la distribution du système. Les statistiques de base ainsi que les statistiques de la mémoire partagée sont activées. Seuls les modules et les dossiers d'extension « **modules_k** » sont compilés et installés par défaut ;
- la structure de la base de données requise par le module emballé peut être créée avec la commande : « **kamdbctl create** » ;
- le **module tm** vérifie si les valeurs des temporisations de retransmission sont trop petites (millisecondes now in 1.5.x étaient secondes), invalide les réponses automatiques des branches précédentes de la fourche en série et prend les paramètres AVP dans format $AVP (nom).

Les principaux modules Kamailio pour IMS :

Le Kamailio, à la base était un proxy SIP et développé en C++, à partir de la version 4, les fonctions CSCF ont été ajoutées au code du logiciel. Les principaux modules du Kamailio pour lřIMS sont décrits ci-dessous :

- **auth_diameter** : ce module implémente l'authentification SIP et l'autorisation avec le serveur DIAMETER, appelé DIAMETER Server Client (DISC). Le support de DIAMETER a été développé pour DISC. Ce projet nřest plus maintenu et les spécifications DIAMETER ont été mises à jour entre-temps. Ainsi, le module est obsolète et nécessite un retrait pour être utilisé avec Opendiameter ou d'autres serveurs DIAMETER ;
- **db_mysql** : il s'agit d'un module qui fournit une connectivité MySQL pour Kamailio. Il implémente l'API DB définie dans Kamailio ;
- **ims_auth** : ce module est utilisé pour l'authentification dans IMS. Dans IMS, le S-CSCF se connecte au HSS via l'interface Cx pour récupérer les vecteurs

d'authentification des abonnés. Actuellement, le module prend en charge les schémas d'authentification **MD5** et **AKAv1/2** ;

- **ims_isc** : ce module implémente l'interface IMS Service Control entre le S-CSCF et le SIP AS. Il fait la logique requise au S-CSCF pour déterminer quel SIP AS à invoquer et quand, en fonction des critères de filtre initial spécifiques à l'abonné ;
- **ims_icscf** : ce module implémente les fonctions requises pour créer un IMS I-CSCF. Il est déclenché à partir du fichier de configuration et peut interroger un HSS tiers pour trouver le S-CSCF concerné pour une demande ;
- **ims_qos** : ce module implémente les fonctions d'autorisation entre le P-CSCF et le PCRF. Le fichier de configuration déclenche le P-CSCF pour envoyer des demandes d'autorisation de DIAMETER au PCRF. Les appels de rappel CDP, Dialog et Usrloc sont utilisés pour signaler lorsqu'une boîte de dialogue est terminée, la session DIAMETER a pris fin ou l'utilisateur a été désenregistré ;
- **ims_registrar_pcscf** : ce module implémente simplement la logique de traitement REGISTER pour les messages REGISTER dans une configuration P-CSCF ;
- **ims_registrar_scscf** : ce module implémente simplement la logique de traitement REGISTER pour les messages REGISTER dans une configuration S-CSCF ;
- **ims_usrloc_pcscf** : il est l'équivalent de lřIMS du module de stockage kamailio usrloc. Il stocke les informations d'abonné IMS au P-CSCF. Ce module est requis parce que, au niveau du P-CSCF, un abonné peut se trouver dans de nombreux états différents (non enregistrés, enregistrés, désinscrits, oui, tous sont différents). De plus, il existe des métadonnées très différentes pour un abonné par rapport à SIP standard, par exemple, les informations IPSec, les informations de session DIAMETER Rx, plusieurs identités publiques (*IMPU*) par contact, etc. ;
- **ims_usrloc_scscf** : il est semblable au module ims_usrloc_pcscf, cřest un module de stockage d'abonné pour les abonnés IMS au S-CSCF. Ce stockage comprend, par exemple, l'abonnement IMS téléchargé à partir du HSS pour chaque abonné, les adresses des fonctions de chargement ;
- **ims_ro_interface** : ce module implémente un mécanisme de chargement en ligne utilisant l'interface IMS DIAMETER Ro. L'interface Ro est destinée à être utiliser dans une configuration Kamailio S-CSCF et liée à un système de chargement en ligne (*OCS*). Actuellement, le module est purement basé sur le temps (c'est-à-dire que la charge de l'unité et les réservations sont en secondes) et utilise l'algorithme SCUR

(*Load Caring-with-Unit-Reservation*) (voir **RFC 4006**). Le module dépend du module **ims_dialog** pour suivre les « boîtes de dialogue » à charger ;

- **AVP** : ce module contient plusieurs fonctions qui peuvent être utilisées pour manipuler le contenu des AVP (*paires Attribute-Value*). Les AVP sont des variables attachées au message SIP en cours de traitement. Chaque variable a son nom et sa valeur. Les AVP peuvent être utilisés pour stocker des données arbitraires ou comme moyen de communication entre modules ;
- **ims_ocs** : ce module fournit un simple module de serveur de charge en ligne pour travailler avec le module ims_charging. Il communique avec le module ims_charging via l'interface DIAMETER-Ro. Il dépend des modules CDP pour communiquer avec un serveur S-CSCF ;
- **ims_registrar_pcscf** : ce module contient toutes les fonctionnalités pour utiliser Kamailio SIP Server comme un Proxy-CSCF. Il dépend des modules USRLOC_PCSCF et PUA si le module REGINFO est utilisé ;
- **ims_registrar_scscf** : ce module contient la logique de traitement REGISTER pour le S-CSCF. Le « moteur de stockage » de ce module est fourni par le module ims_usrloc_scscf ;
- **ims_usrloc_pcscf** : ce module contient la logique de traitement REGISTER pour le S-CSCF. Le « moteur de stockage » de ce module est fourni par le module ims_usrloc_scscf. Il dépend des modules suivants : CDP, CDP_AVP, TM et Ims_usrloc_scscf ;
- **presence_reginfo** : le module permet de gérer un évènement lors de lřenregistrement cřest-à-dire les « Event reg » (tel que défini dans **RFC 3680**) à l'intérieur du module de présence. Cela peut être utilisé pour distribuer l'état de l'information d'enregistrement aux observateurs inscrits. Le module ne met actuellement en œuvre aucune règle d'autorisation. Il suppose que les demandes de publication ne sont délivrées que par une demande autorisée et ne sont soumises que par des utilisateurs autorisés. L'autorisation peut donc être facilement effectuée dans le fichier de configuration Kamailio avant d'appeler les fonctions handle_publish () et handle_subscribe (). Ce module active uniquement le traitement du « reg » dans le module de présence ;
- **rabbitmq** : ce module offre une communication amqp en utilisant librabbitmq. Ce module a été créé en utilisant le client rabbitmq-c. Une nouvelle connexion amqp est

configurée par défaut, lorsque Kamailio démarre. Si la connexion est perdue, le processus tente de le rétablir lorsqu'une nouvelle action amqp est requise. Actuellement, librabbitmq n'offre aucune API asynchrone, mais une API de synchronisation, avec un délai d'attente ;

- **usrloc** : cřest un module d'emplacement de l'utilisateur. Il conserve une table de localisation d'utilisateur et permet d'accéder à la table pour d'autres modules. Le module n'exerce aucune fonction pouvant être utilisée directement à partir de scripts de routage ;
- **websocket** : ce module implémente les fonctionnalités dřun serveur WebSocket (***RFC 6455***) et fournit l'établissement de la connexion, la gestion et l'encadrement des sous-protocoles SIP et MSRP WebSocket **[41].** Le module prend en charge le transport en WS et WSS ;
- **xmlrpc** : ce module implémente l'interface de transfert et de codage XML-RPC pour les RPC Kamailio. Le protocole XML-RPC code le nom de la méthode à appeler avec son paramètre dans un document XML qui est transmis à l'aide du protocole HTTP au serveur. Le serveur extrait le nom de la fonction à appeler avec ses paramètres à partir du document XML, exécute la fonction et encode toute donnée renvoyée par la fonction dans un autre document XML qui est ensuite renvoyé au client dans le corps d'un code réponse 200 OK répond à la requête HTTP. XML-RPC est similaire au **SOAP** plus populaire (*Simple Object Access Protocol*), qui est un framework de messagerie basée sur XML utilisé dans les services Web développé dans le W3C. Les deux protocoles utilisent HTTP comme protocole de transport pour les documents XML, mais XML-RPC est beaucoup plus simple et plus facile à mettre en œuvre que SOAP **[52], [53].**

- **Clearwater**

Le Clearwater est une implémentation open source de lřIMS (*the IP Multimedia Subsystem*) conçue dès le départ pour un déploiement massivement évolutif dans Cloud pour fournir des services de messagerie vocale, vidéo et messagerie à des millions d'utilisateurs.

Le Clearwater combine l'économie des plates-formes de service de style haut de gamme avec la conformité aux normes des solutions de réseau de communication de qualité télé, et sa conception orientée vers le Cloud rend extrêmement adapté au déploiement dans un environnement de virtualisation des fonctions réseau (*NFV*).

Le Clearwater est lřIMS dans le Cloud. LřIMS (*IP Multimedia Subsystem*) est l'architecture basée sur les normes qui a été adoptée par la plupart des grands dans les télécommunications comme base de leurs services de messagerie vocale, vidéo et de messagerie IP, remplaçant les systèmes de commutation de circuits existants et les systèmes VoIP de génération précédente basés sur le softswitching. Le Clearwater suit les principes d'architecture IMS et prend en charge toutes les interfaces standard normalisées attendues d'un réseau de base IMS. Mais contrairement aux implémentations traditionnelles de l'IMS, le Clearwater a été conçue dès le début pour Cloud. Le Clearwater fournit un contrôle d'appel basé sur le SIP pour les communications vocales, vidéo et pour les applications de messagerie SIP. Vous pouvez utiliser le Clearwater comme une solution autonome pour les services VoIP de masse

Lorsqu'il est déployé en tant que noyau IMS, le Clearwater effectue tout ce que l'on attend d'un noyau IMS, en incorporant le Proxy CSCF (*Call Session Control Function*), interrogating-CSCF et Serving-CSCF, ainsi que la fonction de contrôle Breakout Gateway. Le Clearwater comprend également une passerelle WebRTC et prend en charge de manière native l'interfonctionnement entre les clients WebRTC et les clients SIP standard, en utilisant le SIP sur la signalisation WebSocket. Pour relier le ClearWater (figure 4.2) avec d'autres fournisseurs de services sur des troncs SIP, un contrôleur de bordure de session tel que le SBC est recommandé de fournir une sécurité au point de démarcation **[54]**.

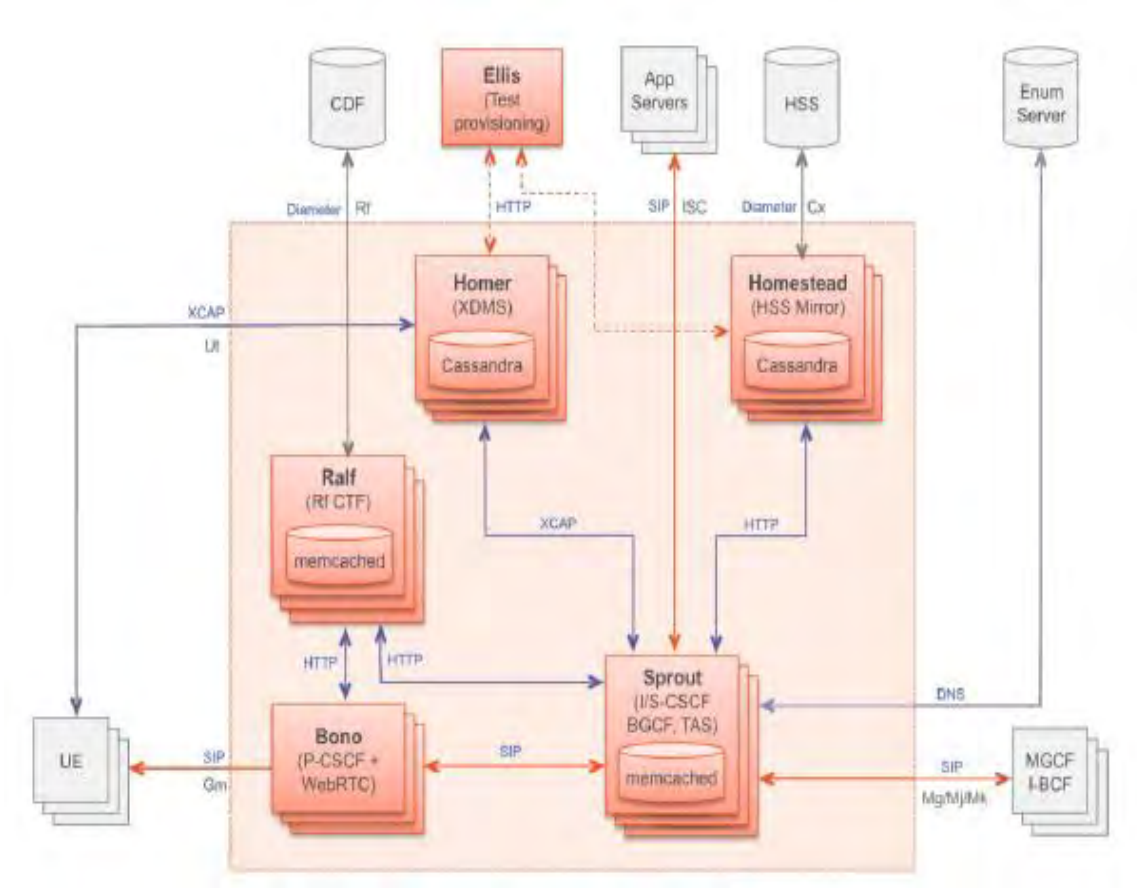


Figure 4.2. Architecture ClearWater

- **OpenIMSCORE**

L'IMS est l'architecture standardisée du NGN (*Next Generation Network*) pour fournir des services multimédias quel que soit le type de réseau d'accès. L'IMS est définie par 3GPP, 3GPP2, ETSI et PacketCable. LřIMS est basée sur un cœur de réseau Tout IP, utilise le protocole SIP (*Session Initiation Protocol*) pour la gestion des sessions de communication entre utilisateurs.

OpenIMSCore est lřimplémentation dřun cœur de réseau IMS basé sur la solution open source SIP Express Router (*SER*) (figure 4.3). Développé par l'institut de recherche allemand FOCUS, ses premières versions compatibles Linux sont apparues en 2006. Cřest une implémentation des CSCF et du HSS. Cette solution fournit toutes les fonctions élémentaires dřun cœur de réseau IMS **[36]**. Les principaux éléments de la couche sont : les serveurs d'abonnés à domicile (*HSS*) et différents serveurs de fonctions de commande d'appel / session (*CSCF*). La couche de contrôle se connecte aux serveurs d'application (*AS*) dans la couche de service et à l'équipement utilisateur (*UE*) via la couche de transport. Le Proxy-CSCF (*P-*

CSCF) agit comme le point de contact avec l'UE pour l'accès au service réseau principal ; Interrogatoire-CSCF (*I-CSCF*) [33].

Né du domaine de la Recherche & Développement, le projet OpenIMSCore, initié par lřinstitut de recherche allemand FOKUS a pour but de combler le vide dans le monde open source de lřIMS. Il a aussi pour but de fournir une implémentation de référence du noyau IMS pour tester cette technologie et mettre en œuvre des concepts qui entourent lřIMS dans le cadre des travaux de recherche. A travers ce projet, tous les développeurs potentiels des services IMS devraient avoir une interface complète de contrôle IMS, conforme à 3GPP, ce qui va leur permettre de sřen servir pour développer et tester leurs services. Cependant, aussi au niveau de la couche accès, lřOpenIMSCore, vise à susciter le développement de composants et concepts qui relient le noyau IMS aux divers réseaux dřaccès.

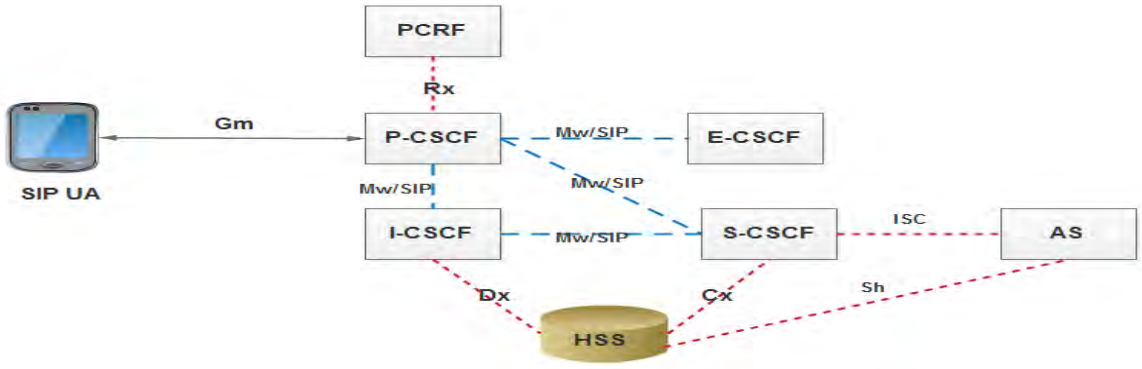


Figure 4.3. Entités du cœur du réseau IMS

- ✓ Lřentité P-CSCF est le point dřentrée dans le réseau IMS pour tout ce qui concerne la signalisation dřune session dřun utilisateur. Il est le point de contact entre lřutilisateur et le serveur central.
- ✓ Lřentité I-CSCF constitue, pour une session dřun utilisateur, le point dřentrée dans le réseau de lřopérateur auquel lřutilisateur a souscrit un contrat de service (*SLA*). Il sert dřintermédiaire entre le serveur proxy et le serveur dřauthentification. Il permet de rediriger les requêtes dřun utilisateur vers son opérateur dřorigine. Lřentité I-CSCF assigne une entité S-CSCF à lřUE et transfert la requête à lřentité S-CSCF sélectionnée. Pour effectuer cette fonction, un échange de DIAMETER avec lřentité HSS est nécessaire. Elle génère aussi les informations nécessaires à la génération des tickets de taxation.

- ✓ Lřentité S-CSCF est chargée de lřauthentification de lřutilisateur et de lui fournir les services opérationnels. Il fournit des informations de routage, de facturation et maintient lřétat de la session en contrôlant un minuteur (temps), interroge le HSS pour vérifier les droits utilisateurs vis-à-vis dřun service. Parallèlement, le S-CSCF enregistre dans le HSS la position de lřabonné dans le réseau et indique au HSS son adresse, afin quřune entité cherchant à joindre lřabonné sache à quel S-CSCF sřadresser.
- ✓ Lřentité HSS est une base de données assurant le stockage des données propres à chaque utilisateur [55] [56] [57].

- **Kurento**

Le Kurento est un serveur de media pour la convergence Web/mobile des communications multimédia temps réel supportant le WebRTC. Les expériences menées dans **[58]** décrivent la technologie WebRTC comme moyen pour parvenir à une convergence réelle entre le web et les mobiles pour les services de communications multimédias temps réel. Elle contribuera à vaincre la fragmentation et doit fournir des avantages significatifs aux utilisateurs et aux développeurs. En suivant cette vision, les auteurs décrivent Kurento, comme une technologie de serveur de médias en mettant en place un prototype à travers une architecture pour démontrer comment cette convergence est possible en combinant un plan de signalisation SIP/HTTP.

Lřavantage de cette technologie est quřelle est bien adaptée pour l'envoi et la réception puis le stockage des flux multimédia en temps réel à travers différents formats de protocoles. Elle est capable dřoffrir des capacités avancées de traitement de différents flux médias, le transcodage et le filtrage. Ceux-ci estiment que le Kurento pourrait pousser les capacités de WebRTC actuelles au-delà dřune simple communication pair-à-pair. Les auteurs ont estimé que les solutions propriétaires ne favorisent pas la convergence que la standardisation dřune norme.

Dřaprès les auteurs du **[58]**, le WebRTC apporte tous les ingrédients nécessaires pour parvenir à une convergence efficace web/mobile.

En conclusion de ces travaux, les auteurs ont introduit le Kurento : une technologie de serveur multimédia compatible avec les clients WebRTC et capable de démontrer comment les applications WebRTC peuvent interagir avec d'autres services de communication en temps réel mobiles et de bureau de manière transparente et simple. Leur expérience permet de montrer comment Kurento pourra contribuer à la consolidation de l'écosystème WebRTC en

montrant une voie vers des services de communication en temps réel plus avancés et universels [59] [60] [61].

- **WebRTC**

Le WebRTC est une technologie en voie de standardisation. C'est une plateforme qui permet d'effectuer des communications temps réel de façon pair-à-pair au moyen des navigateurs en utilisant les API JavaScript. Elle permet de rendre effectifs les services temps réel tels que les appels vocaux, la vidéoconférence, le chat, et même les services de partages de ressources (fichiers, écrans…) au moyen des navigateurs en temps réel sans passer nécessairement par des protocoles propriétaires et ne nécessite pas dřinstallation de plugins additionnels **[39]**.
Cřest un projet initié par le groupe de travail RTCWeb de l'IETF (*Internet Engineering Task Force*) qui vise à intégrer dans les navigateurs des plugins permettant des communications en temps-réel. Il sřagit en effet de lřimplémentation dřun standard ouvert en cours de normalisation par IETF [62] [63] [64] [65] [66] [67] [68].

- **OpenEPC**

Le projet OpenEPC a été développé par Fraunhofer FOKUS depuis 2008. Il couvre tous les éléments fonctionnels dans les spécifications 3GPP Evolved Packet System (*EPS*), anciennement connues comme évolution de l'architecture système (*SAE*). Comme le Fraunhofer FOKUS avance maintenant vers le Système 5G, le projet OpenEPC a été repris par Core Network Dynamic, un spin off société de Fraunhofer FOKUS, qui poursuit le développement et la maintenance du Projets OpenEPC (Core Network Dynamic, 2015). L'avenir de la technologie sans fil réside dans le réseau mobile de nouvelle génération (*NGMN*).
LřOpenEPC peut être utilisé pour créer des bancs de test NGMN qui sont ensuite utilisés pour prototyper, mesurer, surveiller, tester et effectuer des travaux de recherche et de développement pour les réseaux NGMN. Le futur massif, la communication à large bande sera réalisée grâce à un support multi-accès (LTE, 2G, 3G, WiFi, réseaux fixes, etc.) et multi-applications (OTT, IMS, P2P, M2M, Cloud, etc.). EPC est la plate-forme centrale de contrôle de la connectivité IP des technologies à large bande sans fil pour les réseaux NGMN.
Le Core Network Dynamic développe OpenEPC, permettant dřintégrer différents réseaux technologies et plates-formes dřapplication en un seul banc de test (Vlad & Magedanz, 2013).

Cette plate-forme est un ensemble de composants logiciels offrant des schémas de mobilité IP avancés, basés sur des règles Contrôle de la qualité de service et intégration avec différentes plates-formes d'applications dans un réseau convergent environnements. En plus de favoriser la recherche et le développement, lřOpenEPC toolkit permet aux chercheurs universitaires et industriels à réaliser rapidement une infrastructure NGMN de pointe et les bancs d'essai des applications (*FOKUS Fraunhofer Institute for Open Communication System, 2010*).

Le LTE est une nouvelle technologie sans fil, les fonctionnalités avancées dřEPC nécessitent encore beaucoup de recherches et dřessai. Après le développement réussi dřOpenIMS, Fraunhofer FOKUS a lancé lřOpenEPC en utilisant les connaissances acquises du projet OpenIMS Core. LřOpenEPC est une implémentation de prototype du EPC (*Evolved Packet Core*) 3GPP. Ce n'est pas un remplacement de lřOpenIMS core mais il s'intègre bien avec lui, offrant des services optimisés pour les opérateurs et autre fournissant la connectivité haute performance. Donc, aujourd'hui dans chaque déploiement et banc d'essai du projet OpenEPC comprend la plate-forme de lřOpenIMS Core (*Fraunhofer FOKUS, 2015*).

Les composantes de l'OpenEPC :

LřOpenEPC comprend tous les composants et une partie majeure des fonctionnalités du EPC normes 3GPP.

- ✓ **Les passerelles** : une variété de passerelles sont utilisées dans EPC pour transférer les données trafic d'appareils mobiles et assurer le contrôle d'accès, la qualité de service et la gestion de la mobilité. Serving Gateway (*SGW*) est une passerelle spécifique au réseau dřaccès utilisée pour gérer la mobilité des utilisateurs. Il agit comme un routeur et maintient le chemin de données entre eNodeBs et la passerelle de réseau de données par paquets (*PDN-GW*). Tous les paquets sont transférés à travers elle. Lorsque les terminaux se déplacent entre les eNodeB, le SGW sert d'ancre de mobilité locale. La passerelle de date de paquet (*ePDG*) évoluée et le réseau d'accès générique Gateway (*ANGW*) assurent lřinterconnexion avec les différents accès radio, Technologies (*RAT*). Le PDN-GW agit comme une interface entre l'EPC et les réseaux de données par paquets et achemine les paquets vers et depuis les PDN. Le PDN-GW effectue aussi diverses fonctions telles que l'attribution d'une adresse IP pour l'équipement utilisateur, l'application de la qualité de service, le contrôle des politiques et la facturation basée sur le flux. (Firmin, 2016).
- ✓ **Le moteur de stratégie et les entités de contrôle** : il est constitué de la fonction de stratégie et de règles de facturation (*PCRF*), l'entité de gestion de la mobilité (*MME*),

le nœud de prise en charge GPRS (*SGSN)* et la fonction de découverte et de sélection du réseau dřaccès (*ANDSF*). Les décisions sont basées sur des règles pour la connectivité, le contrôle d'accès et la ressource allouée aux appareils mobiles (*Core Network Dynamics, 2016*).

- ✓ **Les entités de données d'abonnement :** le serveur **HSS** (*Home Subscriber Server*) et le serveur AAA ont remplacé les concepts de lř**HLR** (*Home Location Register*) utilisés dans les précédentes technologies. Le HSS est la principale base de données d'informations sur les abonnés qui stocke, met à jour et transmet des notifications sur le profil d'abonnement des utilisateurs. Le serveur AAA fournit autorisation et authentification des appareils mobiles [69] [70] [71].

4.3. Logiciels libres dans le domaine connexe de télécommunications (Base données)

Le RabbitMQ est une implémentation logicielle du protocole AMQP (*Advanced Message Queing Protocol*). Développé par Rabbit Technologies Ltd en 2006 et racheté par une branche de VMware en 2010, le RabbitMQ est une solution de messagerie orientée message ou une solution encore appelée solution Message-Oriented Middleware (*MOM*). Un middleware est un logiciel qui permet de créer un réseau dřéchange dřinformations entre applications. La technique dřéchange dřinformations utilisées par le RabbitMQ qui est lřéchange de messages. Le fonctionnement de RabbitMQ repose sur le protocole AMQP. Lř**AMQP** est un protocole Internet ouvert pour la messagerie dřentreprise. LřAMQP est composé de plusieurs sous couches. Le niveau le plus bas définit un protocole efficace, binaire, pair-à-pair pour transporter les messages entre deux processus sur un réseau **[52]**. LřAMQP est similaire aux protocoles HTTP et TCP car c'est un protocole wire-level, à la différence qu'il permet un transport asynchrone. Le RabbitMQ a choisi d'implémenter lřAMQP pour plusieurs raisons. La première raison est que ce protocole est décrit comme un standard pour les middlewares, contrairement à JMS qui définit une API. La seconde raison est l'interopérabilité de ce protocole, qui permet à n'importe quelle application implémentant lřAMQP de communiquer avec un broker AMQP lui aussi.

Domaines d'applications :

- ✓ **Réseaux**

Le réseau est la base de l'utilisation de RabbitMQ (figure 4.4) car c'est utile pour gérer la distribution des paquets et autres. En d'autres termes, c'est dans ce domaine qu'il y a le plus d'échanges d'information entre les machines.

- ✓ **Développemment**

Mise en place d'un scheduler ;

Mise en place d'une messagerie instantanée.

- ✓ **Extras**

Les fonctionnalités supplémentaires de RabbitMQ : support TLS ; Troubleshooting, clustering, haute disponibilité, liste de contrôle de production.

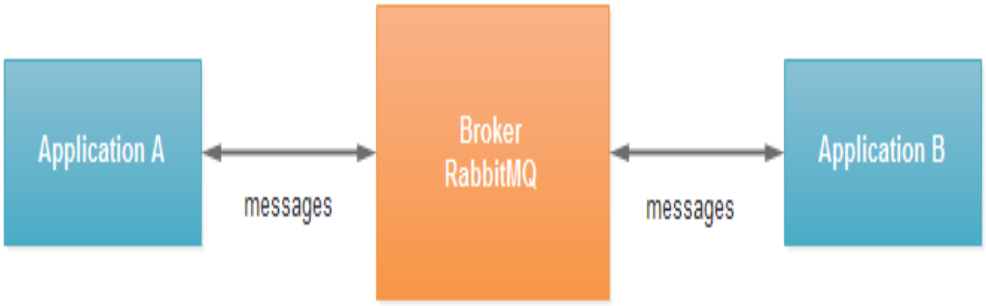


Figure 4.4. Intégration du Broker RabbitMQ au réseau

Le RabbitMQ a de nombreux points forts, ce qui en fait une solution utilisable sur tous types/tailles de projet. En voici quelques-uns :

- Utilise le protocole AMQP (courante : 0.9.1) ;
- Développé en Erlang ce qui en fait un logiciel très robuste ;
- Système de *clustering* pour la haute disponibilité et la scalabilité ;
- Un système de plugins qui permet dřapporter dřautres fonctionnalités (management, ldap, shovel, mqtt, stomp, tracing, AMQP 1.0) ;
- Les vhost permettent de cloisonner des environnements (mutualiser le serveur, env dev/preprod/prod) ;
- *Quality Of Service* (QOS) permet de prioriser les messages.

Afin de pouvoir utiliser efficacement le RabbitMQ, il faut comprendre le fonctionnement du protocole AMQP.

LE BROKER : le RabbitMQ est un message broker, son rôle est de transporter et router les messages depuis les publishers vers les consumers. Le broker utilise les exchanges et bindings pour savoir sřil doit délivrer, ou non, le message dans la queue. Voici le fonctionnement global du broker :

Le publisher va envoyer un message dans un exchange qui va, en fonction du binding, router le message vers la ou les queues. Ensuite un consumer va consommer les messages.

Nous allons donc détailler les différents éléments qui composent le broker.

LE MESSAGE : le message est comme une requête HTTP, il contient des attributs ainsi quřun payload. Parmi les attributs du protocole, vous pouvez y ajouter des headers depuis votre publisher.

Liste des properties du protocole content_type, content_encoding, priority, correlation_id, reply_to, expiration, message_id, timestamp, type, user_id, app_id, cluster_id

Les headers seront disponibles dans attributes [headers].

Lřattribut routing_key, bien quřoptionnel, nřen est pas moins très utile dans le protocole.

LES BINDINGS : les bindings, ce sont les règles que les exchanges utilisent pour déterminer à quelle queue il faut délivrer le message. Les différentes configurations peuvent utiliser la routing key (direct/topic exchanges) ainsi que les headers (header exchanges). Dans le cas des exchanges fanout, les queues nřont quřà être bindées pour recevoir le message.

Nous allons détailler leurs utilisations.

LES EXCHANGES : un exchange est un routeur de message. Il existe différents types de routages définis par le type dřexchange.

Vous publiez dans un exchange. Vous ne consommez pas un exchange !

Important à savoir : l''exchange amq.default est l''exchange par défaut de rabbit. Vous ne pouvez ni le supprimer ni vous binder dessus.

Cet exchange est auto bindé avec toutes les queues avec une routing key égale au nom de la queue.

L'EXCHANGE TYPE FANOUT : lřexchange fanout est le plus simple. En effet, il délivre le message à **toutes** les queues bindées.

L'EXCHANGE TYPE DIRECT : lřexchange direct nřautorise que le binding utilisant strictement la routing key. Si la routing_key du message est strictement égale à la routing_key spécifiée dans le binding alors le message sera délivré à la queue.

binding.routing_key == message.routing_key

L'EXCHANGE TYPE TOPIC : lřexchange topic délivre le message si routing_key du message matche le pattern défini dans le binding.

Une routing key est composée de plusieurs segments séparés par des points. Il y a également 2 caractères utilisés dans le matching.

* nřimporte quelle valeur de segment

nřimporte quelle valeur de segment une ou plusieurs fois

Par exemple pour la routing key foo.bar.baz

- foo.*.baz match
- foo.*.* match
- foo.# match
- foo.#.baz match
- *.*.baz match
- #.baz match
- #.bar.baz match
- # match
- foo.* **non trouvé**

match(binding.routing_key, message.routing_key)

L'EXCHANGE TYPE HEADERS : lřexchange headers délivre le message si les headers du binding matchent les headers du message.

Lřoption x-match dans le binding permet de définir si **un seul** header ou **tous** doivent matcher.

X-MATCH = ANY : avec le x-match = any, le message sera délivré si un seul des headers du binding correspond à un header du message.

binding.headers[attrName1] == message.headers[attrName1] OU binding.headers[attrName2] == message.headers[attrName2]

Le message sera délivré si le header attrName1 (configuré au moment du binding) est égal au header attrName1 du message

OU

si le header attrName2 est égal au header attrName2 du message.

X-MATCH = ALL : avec le x-match = all le message sera délivré si **tous** les headers du binding correspondent aux headers du message.

binding.headers[attrName1] == message.headers[attrName1] ET binding.headers[attrName2] == message.headers[attrName2]

Ici le message sera délivré seulement si les headers attrName1 ET attrName2 (du binding) sont égaux aux headers attrName1 et attrName2 du message.

LES QUEUES : une queue est lřendroit où sont stockés les messages. Il existe des options de configuration afin de modifier leurs comportements.

Quelques options :

- durable, (stockée sur disque) la queue survivra au redémarrage du broker. Attention seuls les messages *persistants* survivront au redémarrage.
- exclusive, sera utilisable sur une seule connexion et sera supprimée à la clôture de celle-ci.
- auto-delete, la queue sera supprimée quand toutes les connexions sont fermées (après au moins une connexion).

Vous publiez dans un exchange. Vous ne consommez pas un exchange ! (quand vous croyez publier dans une queue en réalité le message est publié dans l''exchange amq.default avec la routing key = queue name)

CONSUMER : le rôle du consumer est dřexécuter un traitement après avoir récupéré un ou plusieurs messages.

Pour ce faire, il va réserver (prefetching) un ou plusieurs messages depuis la queue, avant dřexécuter un traitement. Généralement, si le traitement sřest correctement déroulé, le consumer va acquitter le message avec succès (basic.ack). En cas dřerreur, le consumer peut également acquitter négativement le message (basic. nack). Si le message nřest pas acquitté, il restera à sa place dans la queue et sera refetch un peu plus tard [72] [73] [74] [75].

4.4. Conclusion

Aujourdřhui, les technologies de lřinformation et de la communication (*TIC*) prennent de plus en plus dřampleur au sein de toutes les entreprises, de la plus petite à la plus grande.

Nous avons une panoplie de logiciels libres énumérés ci-dessus, qui existent et sont largement utilisés dans le domaine de la recherche parmi lesquels nous ferons bon usage de quelques uns pour mener à bien nos travaux. Grace à lřouverture du code et au respect des normes, les scientifiques utilisent les logiciels libres, eu égards aux différents outils présentés dans ce chapitre. Le monde libre contribue efficacement dans le domaine de télécommunications.

Fort de cela, nos propositions de solutions qui sřappuient sur les logiciels libres et nous ont permis de contribuer à lřamélioration de la fiabilité du réseau IMS. Les chapitres suivants présentent les propositions de solutions dans lřamélioration de la fiabilité de lřIMS et de lřutilité de lřIMS dans le domaine e-santé pour aider la population des zones rurales.

Chapitre 5 : Propositions de solution d'amélioration de fiabilité des réseaux convergents

Ce chapitre considére lřIMS comme une architecture unique pour distribuer les services dans de réseaux Tout IP et quelle que soit la nature du réseau dřaccès. Le réseau IMS est lřélément fédérateur qui rend possible la convergence des réseaux de télécommunications. Il doit permettre de déployer tous les services tels que : la voix sur IP, la présence, la messagerie instantanée, le push to talk, la conférence, la distribution des services vidéo et la télévision.

Un réseau est composé de plusieurs entités, il ne peut être fiable que si chaque entité qui le compose est fiable.

Le thème de notre thèse porte sur la fiabilité, nous abordons la notion de fiabilité qui nous parait important dřen parler dans ce chapitre.

La **Fiabilité,** appelé en Anglo-saxon **Reliability**, exprime la confiance de lřutilisateur dans lřappareil quřil utilise ou qui lui est proposé. Ce nřest que le 9 avril 1962 que ce néologisme a été admis par lřAcadémie des sciences qui en a donné la définition suivante : « **Grandeur caractérisant la sécurité de fonctionnement, ou mesure de la probabilité de fonctionnement d'un appareillage selon des normes prescrites** [76] ». Cette définition fait intervenir plusieurs concepts : la probabilité de bon fonctionnement, les performances à accomplir, les conditions dřopérations et enfin la durée de vie.

La fiabilité est une composante essentielle da la surêté de fonctionnement dřun système. La continuité de service sans coupure avec une qualité de service de bout en bout de façon transparente justifie cette fiabilité alors que tout lřenvironnement est en mouvement. Par ailleurs, nous pourrons aussi définir la fiabilité dřun dispositif comme étant sa probabilité de fonctionner correctement pendant une durée donnée, autrement dit cřest la probabilité quřaucune défaillance ne se produise pendant cette durée.

Parmi les critères de la QoS, notons la performance, la disponibilité, la sécurité et la fiabilité en fait partie [33]. Par conséquent, la **fiabilité est l'un des paramètres clé de la qualité du service** dans lřétude de la plupart des composants électroniques et informatiques. De nombreux industriels et chercheurs travaillent à lřévaluation et lřamélioration de la fiabilité de leurs produits au cours de leur cycle de développement, de la conception à la mise en service (*conception, fabrication et exploitation*) afin de développer leurs connaissances sur le rapport Coût/Fiabilité et maîtriser les sources de défaillance.

La disponibilité, le débit, le délai de transmission, la gigue, le taux de perte de paquets constituent les paramètres de la QoS. Le but de la qualité de service (QoS) est donc dřoptimiser les ressources du réseau et de garantir de bonnes performances aux applications pour les utilisateurs. La QoS permet ainsi aux fournisseurs de services de sřengager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leurs infrastructures IP.

La fiabilité est la clé de la QoS qui mérite d'être maitrisée. Au sein dřun réseau donné, la fiabilité de celui-ci est évaluée en fonction des différents équipements qui le composent, ainsi que du trafic qui y circule, etc. Des applications multimédias et les applications classiques sont de plus en plus utilisées dans ce type de réseaux. Elles nécessitent un niveau minimal de qualité de service en termes de bande passante, de délai, de gigue ou de taux de pertes de paquets dont définir leur sens nous parait important :

- ✓ **Le Débit :** il définit le volume maximal pouvant être atteint pour la transmission de lřinformation (bits) par unité de temps (s) dans une communication entre un émetteur et un récepteur.
- ✓ **La perte de paquets :** elle correspond aux octets perdus lors de la transmission des paquets. Elle sřexprime en taux de perte comme le rapport entre le nombre de paquets perdus et le nombre total de paquets émis.
- ✓ **Le délai de transit (latence) :** Cřest le délai de traversée du réseau, dřun bout à lřautre, par un paquet. La latence dépend du temps de propagation (*fonction du type de média de transmission*), du temps de traitement (*fonction du nombre d''équipements traversés*) et de la taille des paquets (*temps de sérialisation*).
- ✓ **La gigue :** elle désigne les variations de latence des paquets. La présence de gigue dans les flux peut provenir des changements dřintensité de trafic sur les liens de sorties des commutateurs. Plus globalement, elle dépend du volume de trafic et du nombre dřéquipements sur le réseau.
- ✓ **La bande passante :** il existe deux modes de disponibilité de la bande passante, en fonction du type de besoin exprimé par lřapplication :
    - Le mode "**burst**" est un mode immédiat, qui monopolise toute la bande passante disponible (*par exemple lors d''untransfert de fichier*).
    - Le mode "**stream**" est un mode constant, plus adapté aux fonctions audio/vidéo ou aux applications interactives.

Dans le cadre de nos travaux, nous traiterons la fiabilité au niveau des composants du réseau notamment sur les paramètres de fiabilité suivants : le transfert de données, le retard de transmission des messages Diameter échangés sur les interfaces Cx et Dx et la connectivité qui sont liés au composant HSS qui est un élement central des communications dans lřIMS dans la gestion de profils des utilisateurs.

Nous présentons la gestion de profils des utilisateurs en nous basant sur lřentité HSS. Le HSS est une base de données permettant de stocker toutes les informations relatives aux profils utilisateurs (*l''IMPI et l''IMPU*) qui sont énumérées comme suit :

- ✓ il fournit les autorisations dřaccès aux services proposées par le réseau IMS ;
- ✓ la localisation du HSS est effectuée grâce au SLF (*Subscriber Location Function*) ;
- ✓ il est similaire au HLR (*Home Location Register*) et au AuC (*Authentication Center*) des réseaux mobiles telle que le GSM ;
- ✓ les serveurs HSS et SLF communiquent via le protocole DIAMETER.

Les paramètres de services du HSS sont constitués des élements suivants :

- chaque utilisateur possède un profil ;
- ces services sont définis dans le HSS par les iFC (*Initial Filter Criteria*)
- pour chaque serveur dřapplication (AS), on associe un Trigger (*déclencheur*) en fonction de certains paramètres des messages SIP (*entêtes, types de messages*…).

Nous savons que le profil des utilisateurs dans lřIMS est géré par lřentité HSS et le HSS utilise le protocole DIAMETER pour établir la communication. Durant nos tests, il a été constaté de problème dans les échanges dřinformation entre lřutilisateur et lřentité HSS. De propositions de mise en évidence de ces problèmes ont été faites, des hypothèses ont été posées et de solutions au dysfonctionnement ont été proposées.

En effet, il faut noter que lřIMS est le socle pour la fourniture de services aux utilisateurs. LřIMS se base sur le protocole dřouverture de session multimédia SIP pour lřétablissement de communications. Lřentité HSS est la base de données de lřIMS. Il stocke les données propres à chaque utilisateur telles que les paramètres dřaccès et les règles dřinvocation de services, mais aussi les élements de facturation. Les échanges entre lřentité HSS et les entités CSCF se basent sur le protocole DIAMETER. Cependant, il est important que les mécanismes dřéchange dřinformation dřauthentification basés sur le protocole DIAMETER soient clairs. Un dysfonctionnement de ceux-ci peut impacter négativement la fiabilité du système par ricochet la qualité de service (QoS) car la fiabilité est la clé de la qualité de service ainsi que les profits des opérateurs seront ménacés.

En outre, beaucoup de travaux de recherche sont menés ces dernières années avec les logiciels libres implémentant le cœur de réseau IMS, à lřinstar des plateformes SER telles que : lřOpenIMSCore et le KAMAILIO.

Par ailleurs, différents tests ont été effectués avec la plateforme KAMAILIO couplée avec le HSS dřopenIMSCore pour bâtir un cœur de réseau IMS.

Durant ces tests, les différentes observations sont menées sur lřanalyse des messages dřenregistrement, à la suite desquelles deux problèmes ont été identifiés :

- lřentité HSS affiche sur son interface le **« statut connecté »** des utilisateurs, alors que ces derniers nřarrivent pas à se connecter ;
- lorsquřun utilisateur qui est connecté quitte sa session, lřentité HSS nřaffiche pas sur son interface que lřutilisateur est déconnecté.

5.1. Les hypothèses de recherche

Ce travail a pour resultat de mettre en évidence les problèmes constatés ci-dessus et de faire de proposition de solution en vue dřaméliorer le fonctionnement du système. Enfin, nous terminerons ce chapitre par une conclusion.

Cette démarche laisse émettre des hypothèses suivantes :

- ✓ **Hypothèse 1**

Une analyse des messages échangés depuis la requête de UA (*User Agent*), laisse présager des erreurs liées au message SAR entre le HSS et le S-CSCF. Après diagnostic, il apparait un dysfonctionnement au niveau du serveur de session du S-CSCF.

- ✓ **Hypothèse 2**

Le retard de transmission est une source de dysfonctionnement dans les échanges de communication. Pour ce faire, il faut limiter le retard dans la transmission des messages DIAMETER échangés sur les interfaces Cx et Dx en synchronisant le HSS et le S-CSCF.

- ✓ **Hypothèse 3**

Le HSS comprend le protocole DIAMETER et non le protocole SIP. Il serait important que le HSS puisse comprendre le protocole SIP afin de rendre fiable les informations de stockage. Une alternative serait dřutiliser un gestionnaire de file dřattente capable de comprendre les messages SIP et les messages DIAMETER afin de permettre au HSS de mieux comprendre les transactions qui lui sont destinées en vue de les rendre fiables pendant la phase

dřenregistrement dřun utilisateur. Il faut alors agir sur le diagramme d'enregistrement tout en pensant à modifier le comportement du HSS.

- ✓ **Hypothèse 4**

Lorsque le HSS reçoit le message DIAMETER **SAR** (*Server-Assignment-Request*) du S-CSCF, celui-ci répond par un **SAA** (*Service-Assignment-Answer*). A ce moment, le HSS stocke l'utilisateur qui tente de s'enregistrer, ensuite le S-CSCF envoie la réponse « **SIP 200 OK** » à l'entité I-CSCF qui le transmettra au P-CSCF pour le notifier à l'utilisateur qu'il est connecté alors que ce dernier n'arrive pas à se connecter. Pour cela, il faut modifier le comportement des entités HSS et S-CSCF.

- ✓ **Hypothèse 5**

En supposant que la réponse « OK » envoyée à lřentité I-CSCF par lřentité S-CSCF passe après que celui-ci reçoit le SAA du HSS. Pour cela, on peut modifier le comportement de l'entité I-CSCF de telle sorte qu'il fasse une copie du message « OK » et l'envoyer au HSS avant que ce dernier n'envoie le message SAA au S-CSCF.

- ✓ **Hypothèse 6**

Etendre les rôles du serveur KAMAILIO pour lřutiliser en tant que le P-CSCF, lřI-CSCF et le S-CSCF pour bâtir le cœur du réseau IMS, mais aussi de le coupler à un serveur SEMS.

- ✓ **Hypothèse 7**

Etendre les rôles de lřentité P-CSCF du réseau IMS pour assurer lřinteropérabilité entre les clients et les clients UE 3GPP existant **[43]**.

- ✓ **Hypothèse 8**

Le **WebRTC**, une solution pour bénéficier de nouveaux services dans le contexte des réseaux convergents. Lřutilisation du WebRTC comme plateforme de développement de services pourrait ouvrir la voie à une interopérabilité avec le protocole SIP. Le protocole SIP sera utilisé comme protocole de signalisation.

- ✓ **Hypothèse 9**

Bâtir une architecture reposant sur le WebRTC permettant un accès aux réseaux IMS pour les clients sur un UE 3GPP en itinérance au niveau d'accès pour les scénarios suivants :

- lorsque l'accès 3GPP ou non 3GPP est utilisé (IMS commun) ;
- lorsque l'UE n'est pas en itinérance au niveau d'accès ou lorsque l'accès en ligne est utilisé **[43].**

Au cours de nos travaux de recherche, nous allons tenter de confirmer ou dřinfirmer les hypothèses ci-dessus citées par des propositions de différentes plateformes ou solutions utilisées. Nous procéderons à la présentation des différentes solutions et architectures proposées ainsi que les éventuels tests effectués et les résultats obtenus. Enfin, il faut terminer par une discussion sur les différents cas de figure constatés.

Ce chapitre justifie nos choix technologiques pour la mise en place de lřenvironnement de travail. Nous avons retenu IP Multimedia Subsystem (*IMS*) comme infrastructure NGN car cřest la plus aboutie actuellement. Un réseau IMS est composé de plusieurs éléments :

- le cœur de réseau qui concentre les fonctions vitales du réseau (base dřutilisateurs, authentification, contrôle dřaccès, etc.) ;
- les services numériques ;
- les terminaux des utilisateurs.

Les logiciels libres vont nous permettre dřimplémenter le cœur de réseau IMS, à lřinstar des plateformes SER telles que : lřOpenIMSCore et le KAMAILIO. Par ailleurs, les différents tests ont été effectués avec la plateforme KAMAILIO couplée avec le HSS dřopenIMSCore pour bâtir un cœur de réseau IMS. Et le WebRTC est dřactualité et a beaucoup dřavenir devant lui pour les services Web. Il est souple, conviviale et offre les mêmes services que lřIMS.

5.2. Simulation 1 : Kamailio utilisé comme cœur du réseau IMS

5.2.1. Architecture

Dans lřarchitecture de la figure 5.1, le serveur Kamailio IP est choisi. Il est un logiciel Open Source de premier plan pour la création de services SIP, tels quřun proxy SIP, un serveur SIP Présence, un serveur de localisation SIP, etc. avec un langage de configuration riche, une modularité et un développement continu, le Kamailio est le choix idéal pour la création de solutions dřentreprise et dřopérateurs. Le Kamailio fonctionne sur des systèmes Unix et Linux, allant des systèmes intégrés aux serveurs multicœurs à grande échelle. Le serveur Kamailio est capable de fonctionner en mode sans état et avec état, fournit une traversée NAT, prise en charge du trafic SIP et RTP. Le Kamailio vérifie lřauthenticité des utilisateurs

sur la base de cette base de données. Une fois inscrits, les utilisateurs peuvent téléphoner selon les privilèges fournis par leur abonnement et accord avec le prestataire de services. Le départ et la configuration de l'appel iront sur le serveur Kamailio, qui détermine ensuite le type dřappel demandé et effectue les contrôles d'authentification. En fonction du type dřappel, la décision de routage est alors prise.

Un contrôleur SBC est aussi déployé. Il est situé à la limite logique de deux réseaux, dans notre cas entre deux machines virtuelles et contrôle la communication entre eux. Il résout les problèmes de compatibilité liés à une des différences dans lřadministration et les protocoles des réseaux frontaliers, fournissant de lřinteropérabilité malgré le déséquilibre. Il peut également fournir des fonctionnalités de sécurité, en gardant un œil sur le volume de trafic entrant dans le réseau et masquant sa topologie aux réseaux environnants.

Certaines des fonctions qu'un SBC peut exécuter sont énumérées ci-dessous :

- ✓ protection contre les accès non autorisés à un réseau ;
- ✓ résolution des problèmes de traduction d'adresses réseau (*NAT*) ;
- ✓ conversion du protocole ;
- ✓ transcodage du trafic multimédia ;
- ✓ l'enregistrement multimédia ou la conversion DTMF ;
- ✓ traduction de formats de numéros de téléphone ;
- ✓ fournir des fonctionnalités de qualité de service (QoS) pour surveiller les appels et améliorer la qualité globale du service.
- ✓ Enfin, il offre des fonctions de sécurité utiles pour protéger le réseau.

Ainsi, le serveur Kamailio a été choisi dans notre architecture de test que nous avons mise en place, representée par la figure 5.1.

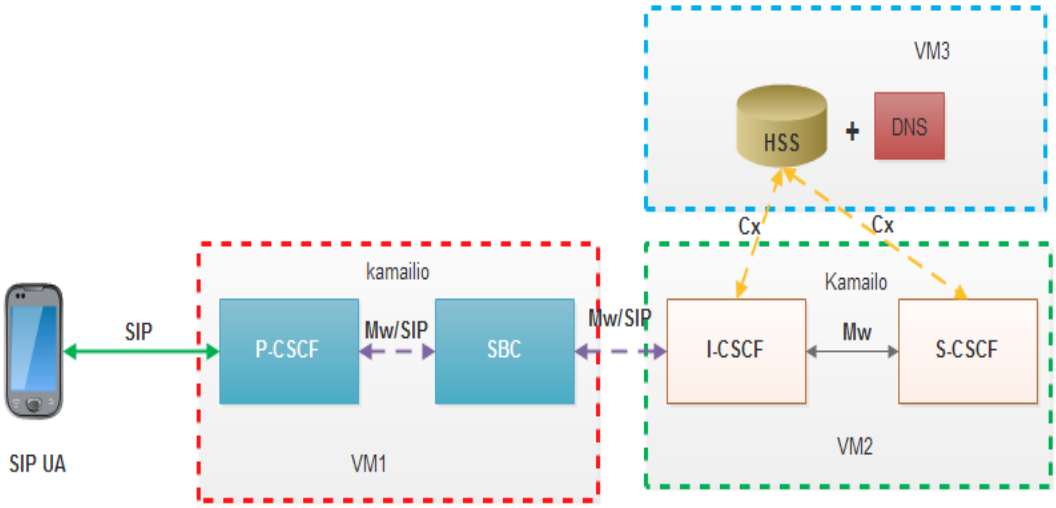


Figure 5.1. Utilisation de Kamailio comme serveur P/I/S-CSCF avec SBC

Lřarchitecture de la figure 5.1 décrit les fonctionnalités dřun cœur de réseau IMS bâti sur la plateforme Kamailio. Le serveur Kamailio est utilisé dans cette architecture comme un Proxy-CSCF, un Interrogating-CSCF, un Serving-CSCF mais aussi comme un SBC. Le SBC établit un pont entre le serveur P-CSCF et le serveur I-CSCF.

Le Kamailio-SBC est configuré de telle sorte que toutes les requêtes (*enregistrement, désenregistrement et ouverture de session*) sont exécutées. Lřentité P-CSCF est reliée au SBC sur lřinterface Mw/SIP qui est à son tour aussi connecté au I-CSCF sur lřinterface Mw/SIP. Les entités I-CSCF et S-CSCF sont reliées au serveur HSS par le protocole DIAMETER sur les interfaces Cx. Le serveur DNS est utilisé pour gérer la résolution du nom de domaine, les URI SIP des serveurs ainsi que les identités publiques et privées des utilisateurs.

5.2.2. Procédure d'enregistrement avec Kamailio IMS SBC

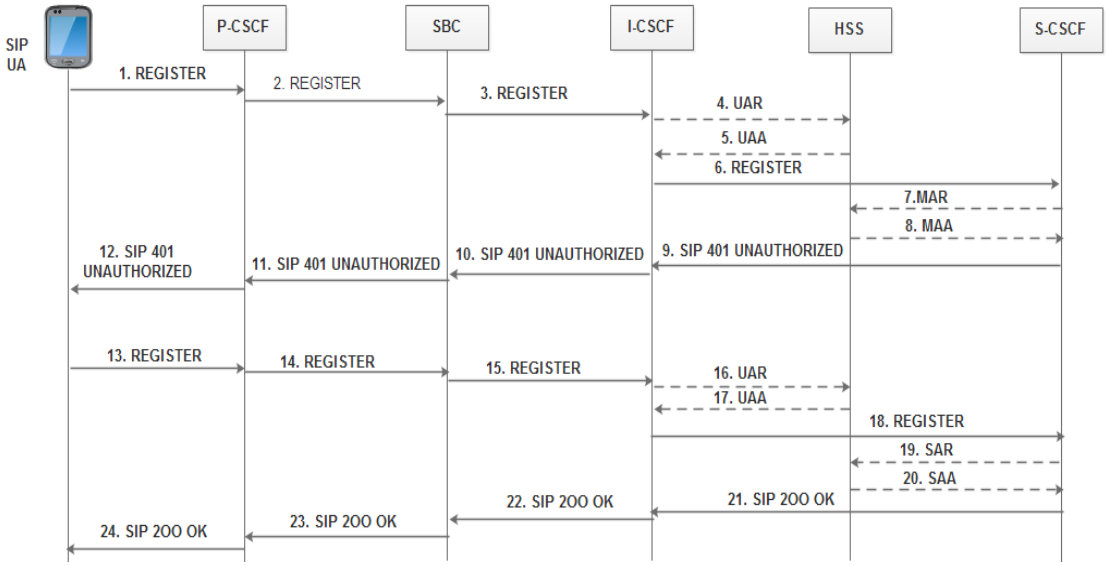


Figure 5.2. Procédure d'enregistrement Kamailio IMS avec SBC

5.2.2.1. Tests d'enregistrement et résultats

Les résultats présentés ci-dessus visent à décrire la procédure dřenregistrement des utilisateurs dans le réseau IMS. Ils sont basés sur les tests effectués et lřanalyse des différents messages DIAMETER échangés entre les entités HSS, lřI-CSCF et le S-CSCF en vue de mettre en évidence le problème de fiabilité des données du HSS. Le HSS est la base de données utilisateur du réseau (figure 5.3). Cette entité est lřéquivalente du HLR (Home Location Register) présent dans les réseaux GSM. Elle contient toutes les données nécessaires pour lřaccès au réseau et aux services. Ces informations sont utilisées par les utilisateurs et les équipements (informations dřauthentification, dřautorisation, profils dřaccès). Les informations indispensables pour lřIMS sont :

- ✓ les abonnements de lřutilisateur en termes de sessions autorisées ;
- ✓ la localisation ;
- ✓ lřauthentification et lřautorisation ;
- ✓ les abonnements aux services de réseau ;
- ✓ le serveur de service S-CSCF alloué à lřutilisateur.

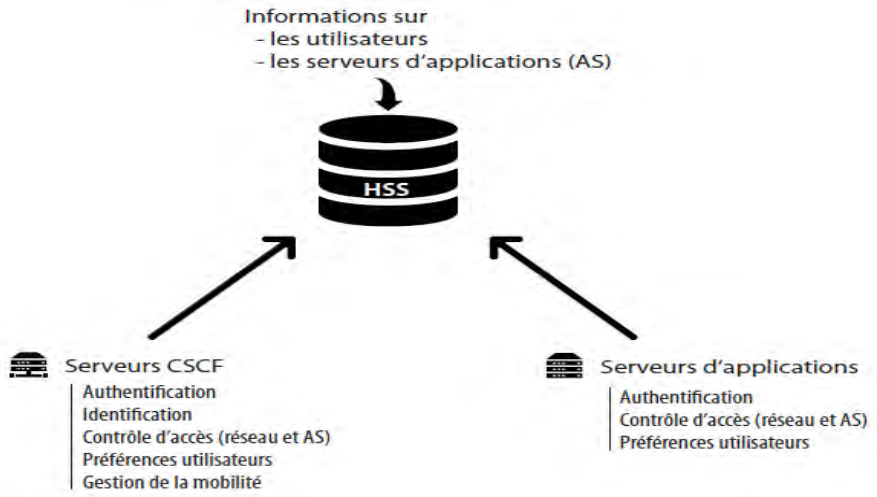


Figure 5.3. Fonction HSS et son environnnement

Cette base de données utilisateurs est accessible uniquement par les entités de contrôle du réseau et dans certaines situations par les serveurs dřapplications. Cřest un élément clé de lřIMS, il sert de support pour les fonctions dřauthentification, de mobilité, dřidentification et dřaccès aux services.

Nous avons enregistré un utilisateur à partir dřun client IMS Boghe. Lřentité HSS arrive à associer à lřutilisateur, lřentité S-CSCF approprié (voir figure 5.4).

A lřétape 16 (figure 2.11. *Localisation et établissement de session dans le réseau IMS avec SIP DIAMETER Application*), le HSS associe déjà le Serving-CSCF (*identité fournie dans le message DIAMETER SAR*) qui dessert lřutilisateur.

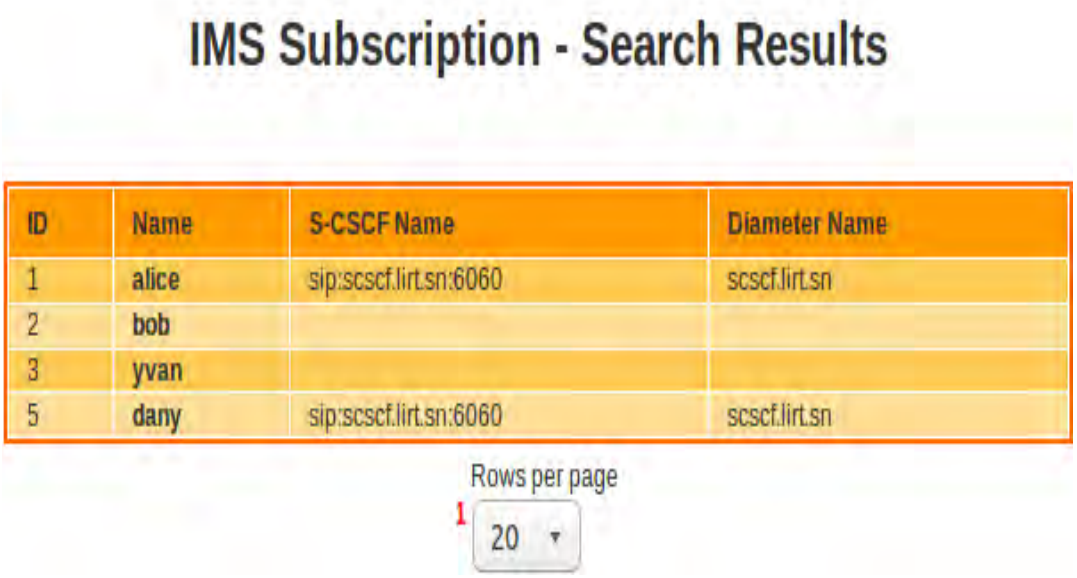


Figure 5.4. Sélection de l'entité S-CSCF par HSS d'un utilisateur

Il sřagit de lřétape 17 (Figure 2.11) où lřentité HSS a reçu le message SAR dans lequel lřentité S-CSCF lui a envoyé ses paramètres en demandant de lui envoyer une partie ou tout le profil de lřutilisateur dans le message DIAMETER SAA. En ce moment, lřentité HSS affiche déjà sur son interface que lřutilisateur est connecté (voir figures 5.5, 5.6 et 5.7).
La figure 5.5 montre lřétat dřenregistrement de trois utilisateurs qui ont tenté de se connecter. Alice et Bob ne sont pas enregistrés cependant dany est enregistré.

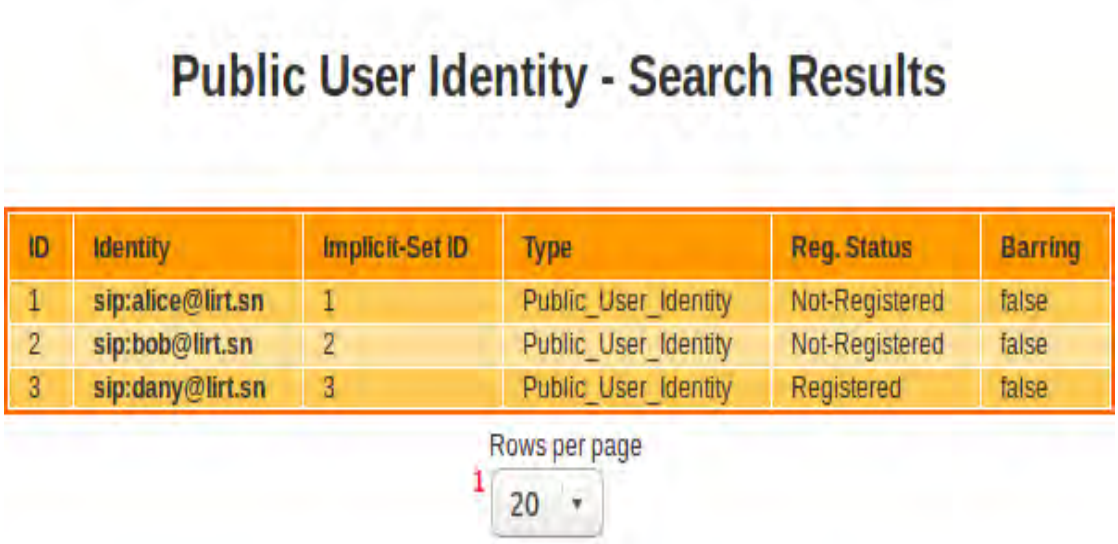


Figure 5.5. Affichage des utilisateurs connectés au niveau du HSS

La figure 5.6 montre la création dřune IMPU (*Public User Identity*) qui est décrit ci-dessous :

- Lřidentité de lřutilisateur doit absolument respecter cette syntaxe : sip:utilisateur@domaine. Soit dans notre cas, pour le domaine lirt.sn et pour un utilisateur dany : sip:dany@lirt.sn;
- Selectionner le service profile par defaut (defaut_sp). Note : le service profile permet de lier un utilisateur à une liste dřiFC (*initial Filter Criteria*). Par defaut, ce service profile va donner à un utilisateur les droits dřutiliser un ensemble de service (résolus via des serveurs dřapplication) ;
- Ne pas oublier de cocher la case « Can Register » pour autoriser lřenregistrement dřun abonné (utile avec un serveur de présence) ;
- Modifier les autres informations comme sur la capture suivante ci-dessous et sauvegarder ; le champ « **User-Status** » est marqué : « **REGISTERED** » cřest-à-dire lřutilisateur est bien enregistré :

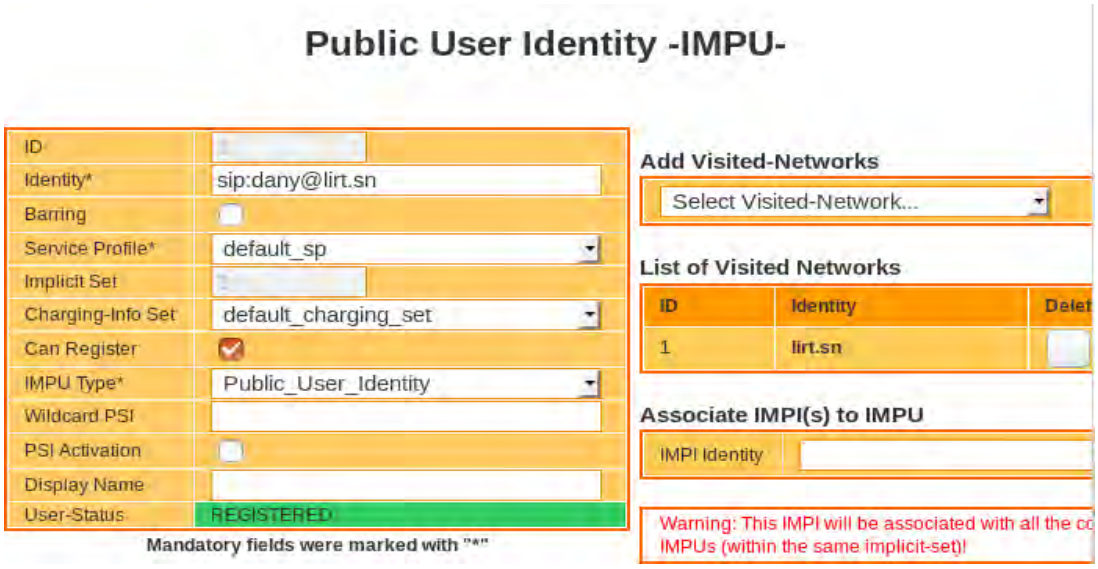


Figure 5.6. Affichage du profil de l'utilisateur (IMPU)

La figure 5.7 ci-dessous montre l'utilisateur dany ayant une identité publique et les identités envoyées implicitement correspondantes sont enregistrées dans le HSS.

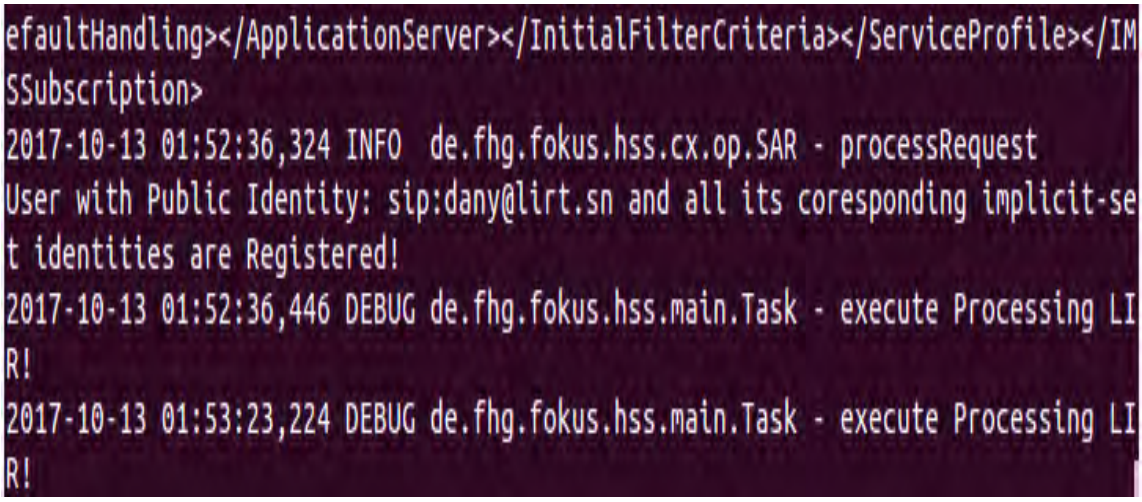


Figure 5.7. Souscription de l'utilisateur au niveau de HSS

Or, sur lřinterface du journal système de lřentité HSS, nous constatons quřelle nřa pas envoyé la réponse SAA attendu du message SAR. Nřayant pas reçu le profil de lřutilisateur (*transmis dans le message SAA*), lřentité S-CSCF nřa pas pu stocker le profil de lřutilisateur.

Par conséquent, elle nřa pas envoyé la réponse attendue « **SIP 200 OK** » pour notifier à lřutilisateur quřil sřest connecté. Sur lřinterface du client, nous constatons que lřutilisateur nřest pas connecté. La Figure 5.8 montre lřinterface du terminal de lřutilisateur nommé dany qui est configuré par lřapplication Boghe-IMS/RCS client. Boghe est un client open source similaire au client propriétaire Mercuro qui est une des toutes solutions commerciales dřun client IMS.

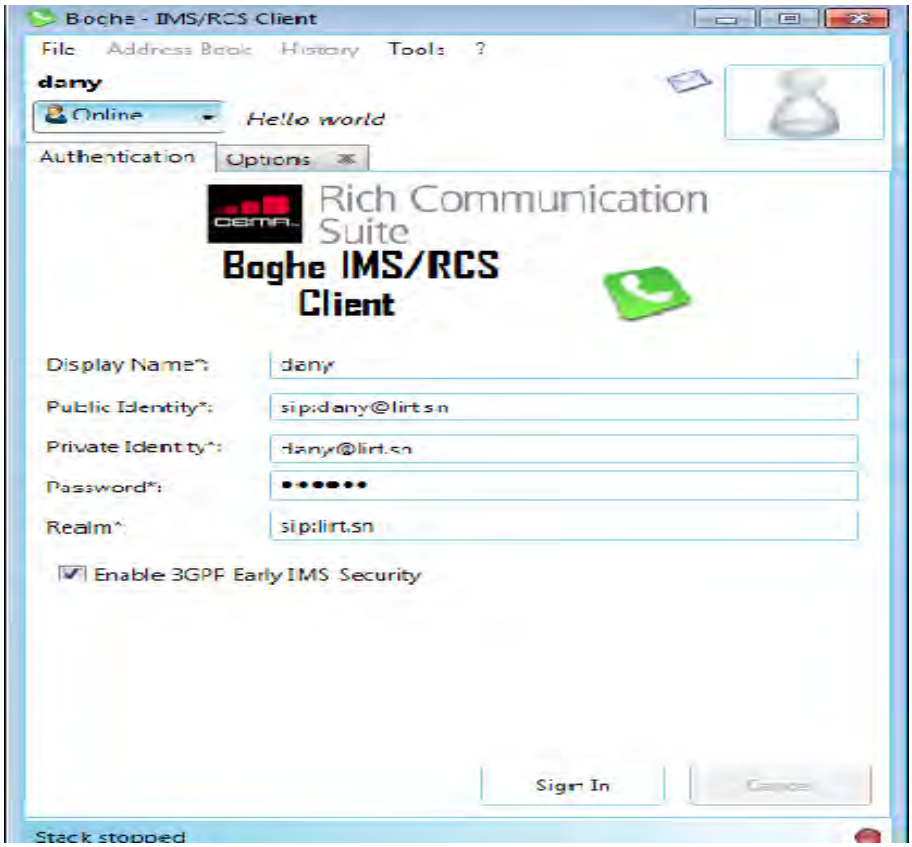


Figure 5.8. Enregistrement du client à partir du SIP UA Boghe

5.2.2.2. Analyse sur Wireshark

Nous avons analysé les trames de la figure 5.9 pour observer les échanges entre les différentes entités pendant la procédure dřenregistrement utilisant la methode REGISTER du protocole SIP. Nous remarquons que sur « Status-Line », il est mentionné « SIP/2.0 403 Forbidden Ŕ HSS Identity not registered ». Ce qui veut que le SIP / 2.0 403 Interdit - Identité HSS non enregistrée, cette information indique que le serveur comprend la demande mais refuse dřy

satisfaire. Lřautorisation nřy fera rien et la demande ne devrait pas être repetée. Le champ dřen-tête « **Via** » indique le transport utilisé (*UDP*) pour la transaction et identifie la localisation où la reponse doit être envoyée. Le champ dřen-tête « **From** » indique lřadresse de lřentité ayant initié lřenregistrement qui peut être lřadresse-dřenregistrement de lřutilisateur. Le champ dřen-tête « **To** » indique lřadresse de lřutilisateur enregistré. Le champ dřen-tête « **To** » specifie avant tout le receveur "logique" souhaité de la demande, ou lřadresse-dřenregistrement de lřutilisateur ou de la ressource qui est la cible de cette requête. Les champs dřen-tête **From** et **To** ont la même valeur si lřutilisateur sřenregistre lui-même, cřest notre cas. Le champ dřen-tête « **Call-ID** (*identifiant d''appel*) » agit comme un identifiant unique pour grouper ensemble une série de messages. Il dit être le même pour toutes les demandes et reponses envoyées par lřun ou lřautre UA dans un dialogue. Le champ dřen-tête « **CSeq** » sert de moyen dřidentifier et dřordonner les transactions. A chaque nouvel enregistrement pour le même User Agent (*UA*), le numéro Cseq est incrémenté.

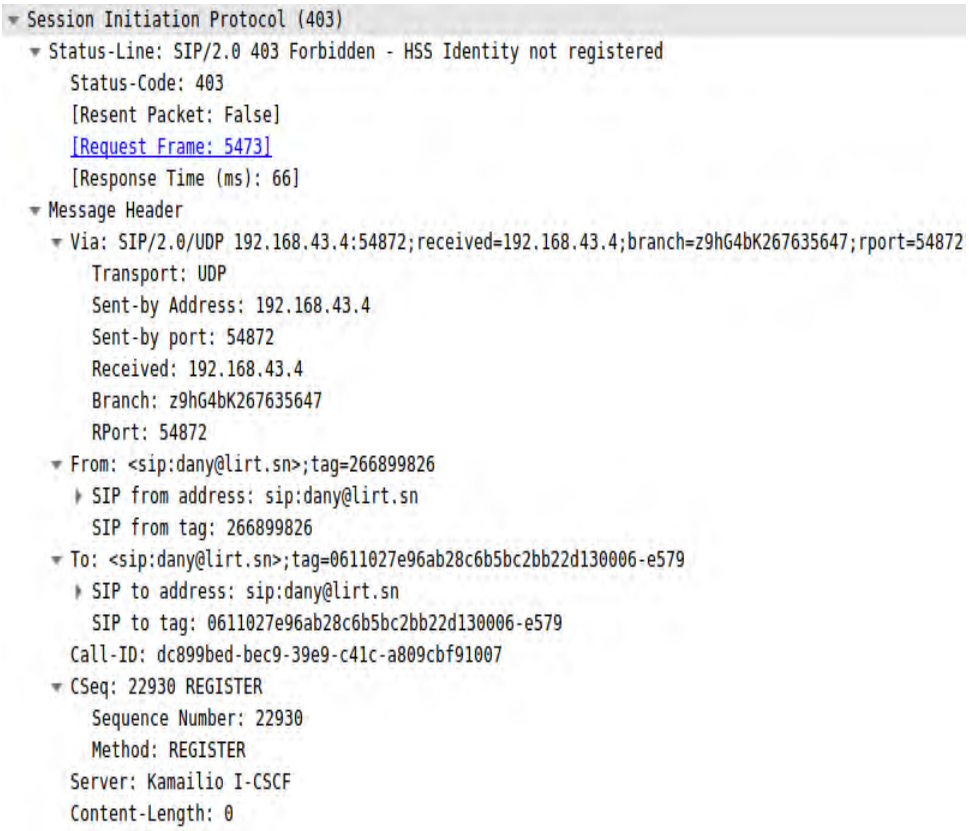


Figure 5.9. Capture message SIP REGISTER (au niveau de l'entité I-CSCF)

La figure 5.10 montre la capture du message **SIP SUBSCRIBE** qui notifie que lřutilisateur est bien enregistré dans la base du S-CSCF par lřinformation de « Status-Line », qui mentionne SIP/2.0 200 Subscription to REG saved. Les différents champs dřen-tête ont les mêmes explications que la figure 5.9.

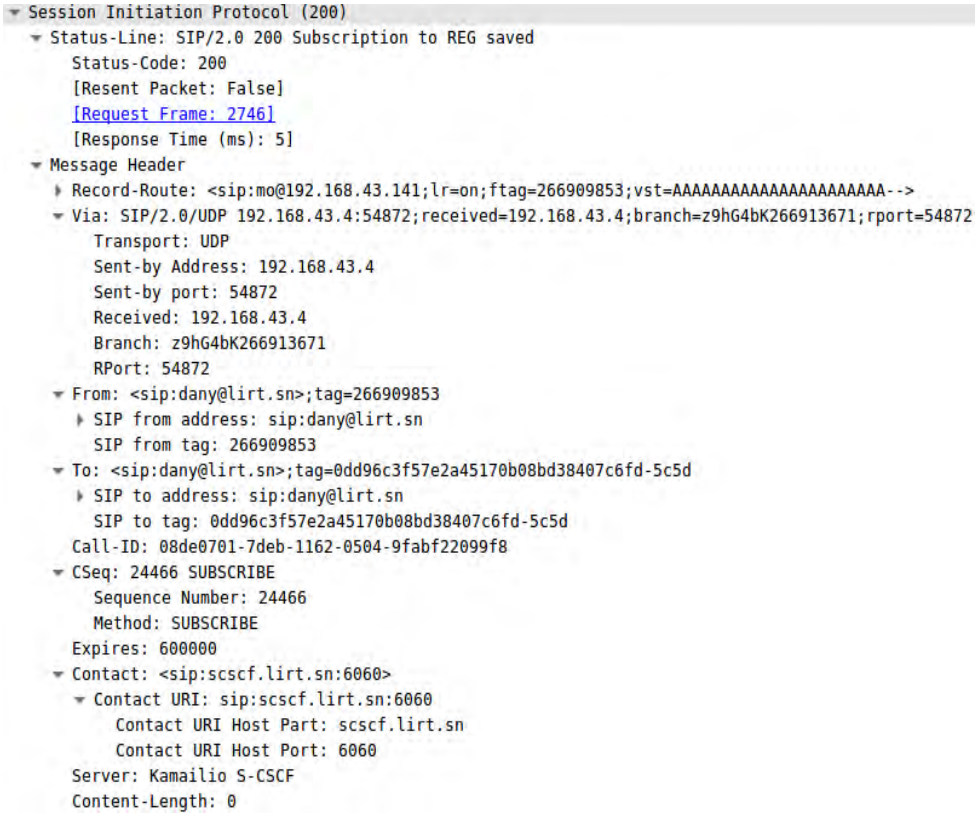


Figure 5.10. Message SIP SUSCRIBE capturé lors de l'enregistrement

5.2.2.3. Discussion

Deux versions différentes de Kamailio (4.4 et 5.0) à partir des codes sources ont été utilisées pour les tests. Les seuls résultats obtenus étaient les connexions entre les différents nœuds (sur les interfaces DIAMETER) de cœur du réseau. Les utilisateurs nřarrivaient pas à sřenregistrer alors que le HSS affiche sur son interface que lřutilisateur est connecté.

Dřautres essais ont été réalisés à la suite cette fois ci, en introduisant un SBC dans lřarchitecture.

A lřétape 16 (figure 2.11), le HSS associe déjà le Serving-CSCF (*identité fournie dans le message DIAMETER SAR*) qui dessert lřutilisateur et affiche quřil est enregistré avant

dřenvoyer une partie ou tout le profil de lřutilisateur dans le message DIAMETER SAA. En analysant le diagramme, nous remarquons que le S-CSCF envoie la réponse SIP 200 OK pour notifier à lřutilisateur quřil est connecté. Or, le HSS affiche déjà sur son interface que lřutilisateur est connecté. Nřayant pas la table location dans laquelle il faut stocker les profils dřutilisateurs qui se connectent, le HSS nřa pas répondu au message SAR. Il fallait dans un premier temps mettre à jour la base de données sur HSS par exécution du script SQL de mise à jour et de mise à niveau. Ensuite, lřidée est dřintroduire un gestionnaire de file dřattente afin de modifier un peu le comportement du HSS. Nous proposons ici une solution basée sur le protocole AMQP en intégrant deux Brokers Rabbitmq qui vont interfacer entre lřentité I-CSCF et le HSS dřune part puis entre le S-CSCF et le HSS dřautre part. Le diagramme de la figure 5.11 montre la procédure dřenregistrement avec les Broker Rabbitmq.

5.3. Simulation 2 : utilisation de RabbitMQ pour modifier le comportement du HSS

Dřaprès lřarchitecture proposée dans **[52],** les fonctions de lřentité HSS du cœur du réseau sont combinées à celle de **SLF** (*Suscriber Location Function*). Dans lřhypothèse 4, la proposition de modifier le comportement du HSS a été émise suite au dysfonctionnement constaté lors de la procédure dřenregistrement. Cependant, la dernière version de Kamailio (5.0) supporte le protocole AMQP (*protocole de base de RabbitMQ*).

Le RabbitMQ est un broker de messages se basant sur le standard AMQP afin dřéchanger avec les différents clients. Nous pouvons comparer le broker à la poste, cřest-à-dire quřil reçoit un message dřune application et le délivre à une autre. LřAMQP est le protocole qui a pour but dřoffrir un système dřéchange totalement interopérable entre les différents acteurs. LřAMQP est un système très souple qui en plus de sa capacité à être utilisé dans nřimporte quel environnement, gère la communication avec simplicité grâce aux différents systèmes dřéchanges applicables.

En se basant sur le diagramme dřenregistrement de la figure 5.2, nous proposons le diagramme dřenregistrement de la figure 5.11 ci-dessous en intégrant dans celui-ci deux serveurs Rabbitmq qui vont interagir avec les entités I-CSCF, S-CSCF et le HSS.

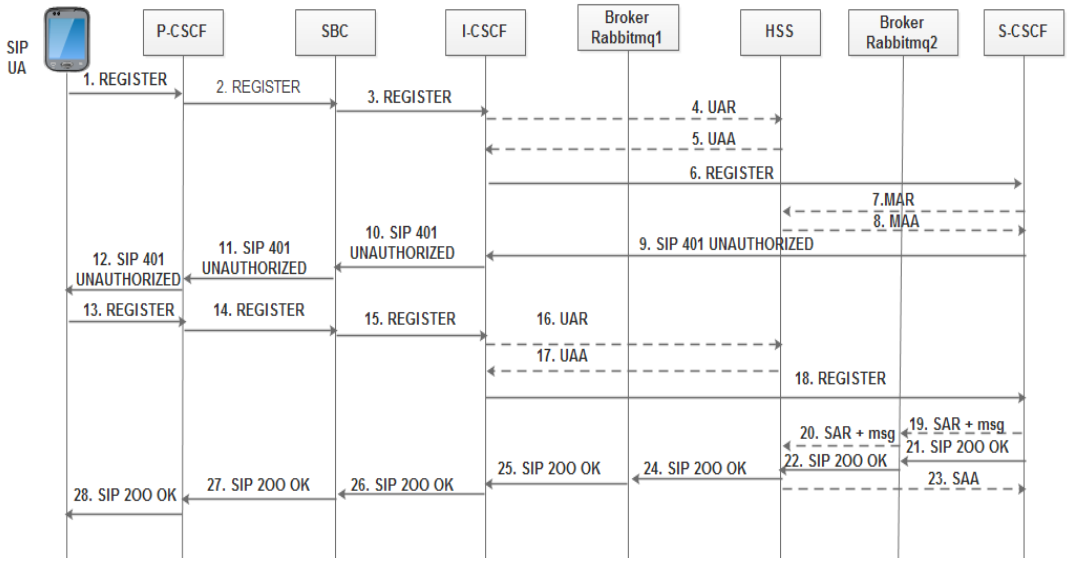


Figure 5.11. Procédure d'enregistrement avec le Broker RabbitMQ

En se reportant à la figure 2.11, les étapes 1 jusqřà 18 sont identiques. Lorsque le S-CSCF reçoit le message REGISTER, il déclenche lřenvoi dřun message DIAMETER SAR plus un autre message pour indiquer au HSS dřattendre la réception du message SIP 200 OK avant dřenvoyer le message SAA. Le S-CSCF déclenche aussi lřenvoi du message SIP 200 OK (étape 21) qui va être transmis au Broker Rabbitmq2 qui sera ensuite envoyé au HSS. Le HSS retransmettra le message SIP 200 OK au Broker Rabbitmq1 qui le transmet à lřI-CSCF pour lřutilisateur. A la réception du message SIP 200 OK, le HSS répond en envoyant le message DIAMETER SAA comportant une partie ou le profil de lřutilisateur. En ce moment, il peut associer au profil de lřutilisateur lřURI du S-CSCF qui le dessert et affiche en même temps le « **statut connecté** ». Le S-CSCF va alors stocker dans sa table location le profil de lřutilisateur qui souhaite sřenregistrer.

Lřarchitecture physique de la solution HSS avec Rabbitmq est representée par la figure 5.12 ci-dessous :

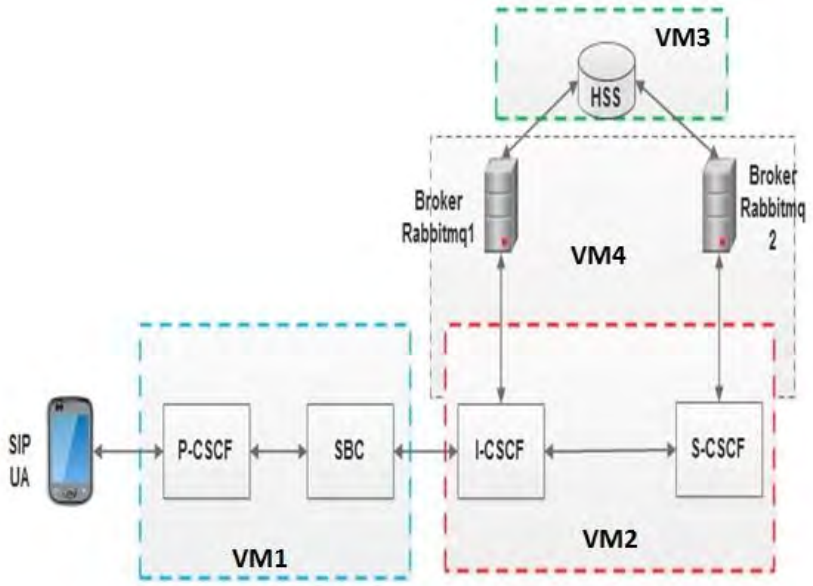


Figure 5.12. Architecture de la solution HSS avec Rabbitmq

La description de lřarchitecture virtuelle de la solution avec Rabbitmq de la figure 5.12 est décrite comme suit :

Cette architecture proposée de la figure 5.12 découle du diagramme de la figure 5.11 qui explique les connexions logiques ainsi que le fonctionnement de lřarchitecture. Elle est déployée, conçue dans un environnement virtuel et est constituée de quatre (4) machines virtuelles respectivement :

- ✓ **La machine virtuelle N° 1 (VM1)** : elle contient lřentité logique **P-CSCF** et le nœud **SBC**. Le P-CSCF est le nœud dřentrée cœur du réseau IMS. Sa fonction principale consiste à transférer les messages SIP REGISTER venant du SIP UA vers le I-CSCF. Il permet aussi au SIP UA dřêtre localisé dans le réseau visiteur. La fonction logique SBC agit en tant que le P-CSCF dans le cas de cette expérimentation et non comme un pare-feu (Firewall) ou pour relier un réseau IMS à un autre réseau IMS ou réseau IP ;
- ✓ **La machine virtuelle N° 2 (VM2) :** elle contient les entités **I-CSCF et S-CSCF**. En effet, lřInterrogating-CSCF (I-CSCF) a comme principales fonctions de déterminer le S-CSCF auquel lřabonné peut se connecter et transmettre les messages entre le P-CSCF et le S-CSCF, un peu comme une passerelle. Les fonctions réalisées par cette entité I-CSCF sont :

- la localisation du S-CSCF concerné par la session par consultation de la base HSS (load balancing de S- CSCF) ;
- la garantie de sécurité entre le Visited network et le Home network.

Le Serving-CSCF (*S-CSCF*) est lřéquipement qui a pour rôle de finaliser lřauthentification de lřutilisateur et lui fournir les services opérationnels. Il fournit des informations de routage, de facturation, maintient lřétat de la session en contrôlant un timer, interroge le HSS pour vérifier les droits utilisateurs vis-à-vis dřun service, etc. Ces entités I-CSCF et S-CSCF vont ensuite être reliées à la machine VM4 sur laquelle sont installés les nœuds Broker Rabbitmq 1 et Broker Rabbitmq 2. Les deux brokers, par leurs mécanismes, vont introduire un temps dřattente au niveau du HSS qui ne pourra envoyer ses informations quřaprès réception du message SIP de confirmation d'ouverture de session. Ainsi, ces brokers règlent le problème de synchronisation des connexions au niveau du HSS

- ✓ **la machine virtuelle N° 4 (VM4)** : elle est enfin reliée à la station machine virtuelle N° 3 (**VM3)** sur laquelle est installée la base de données HSS qui stocke le profil des utilisateurs et des services associés (*à l''instar du HLR pour les réseaux mobiles*).
- ✓ les **clients SIP UA** peuvent être un terminal mobile ou sur une autre station de travail.

5.4. Simulation 3 : Cœur du réseau IMS avec clearwater relié à un HSS externe et interconnecté à un serveur Kamailio

5.4.1. Architecture

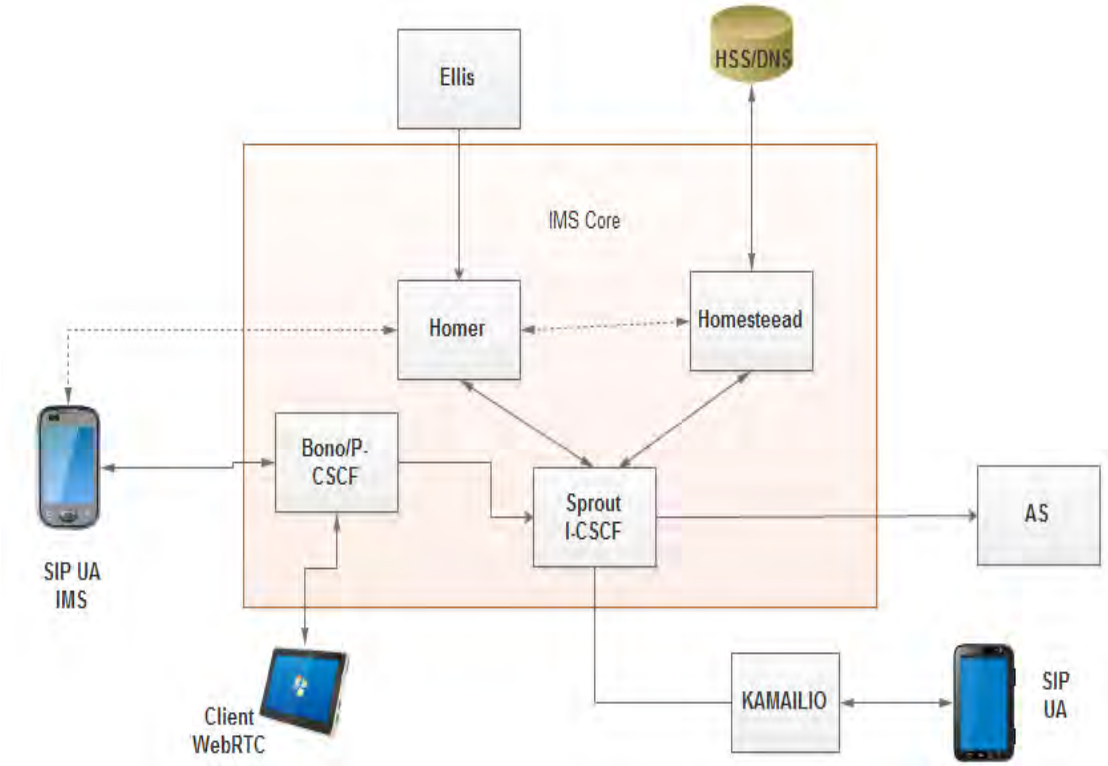


Figure 5.13. Clearwater avec HSS externe

Lřarchitecture proposée de la figure 5.13, décrit le fonctionnement dřun cœur de réseau IMS bâti avec Clearwater. A la base, la plateforme Clearwater vient avec une base de données HSS intégrée qui tourne avec Cassandra. Lřinterface du HSS de Clearwater ne présente pas assez de fonctionnalités. Pour ce faire, lřidée est dřutiliser un serveur HSS externe celui dřOpenIMSCore qui fournit plus de fonctionnalités et une interface assez souple à administrer. La signalisation est assurée par le protocole SIP over SCTP. LřIMS permet le transport SCTP au cœur du réseau, mais pas entre le P-CSCF et lřUE. Clearwater ne prend pas en charge le transport SCTP (ni PJSIP).

5.4.2. Utilisation de IMS-SBC comme passerelle

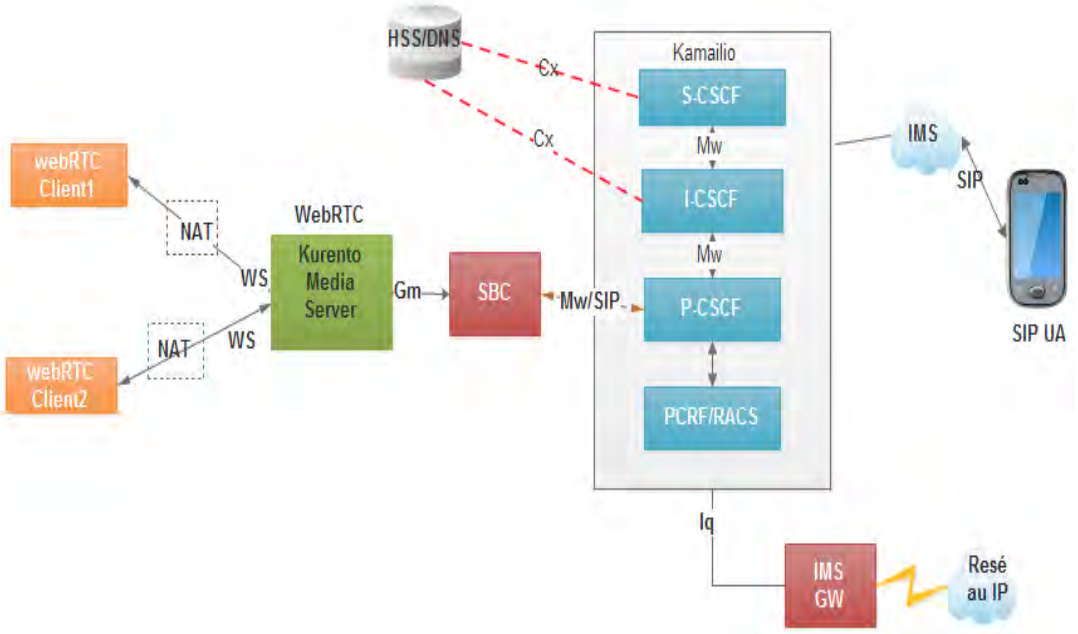


Figure 5.14. Interconnexion IMS WebRTC par IMS-SBC

Lřarchitecture de la figure 5.14 est composée dřun cœur de réseau IMS bâti sur Kamailio, dřun serveur de media Kurento qui combine les fonctionnalités dřun serveur de média (pour le stockage des vidéos) et celles dřun serveur de signalisation WebRTC. LřIMS-SBC est utilisé comme passerelle. Ci-dessous, le descriptif de la figure 5.14.

- lřinterconnexion entre le serveur WebRTC et le cœur du réseau IMS est effectuée par un SBC (IMS-SBC) ;
- les échanges entre les entités I/S-CSCF et le serveur DIAMETER (HSS) sont effectués sur le support DIAMETER SIP Application ;
- la signalisation entre les clients WebRTC et le serveur WebRTC est effectuée grâce au protocole WebSocket (WS) ou WebSocket Secure (WSS) pour une connexion sécurisée ;
- pour le réseau IMS, la signalisation est assurée par le protocole SIP ;
- le transport des flux media entre les clients SIP est assuré par le protocole RTP et RTCP et SRTP pour le transport sécurisé ;
- le DNS est utilisé pour lřadressage SIP ;
- les protocoles SIP et SDP seront utilisés pour la signalisation et les capacités média ;

- les protocoles ICE ainsi que les serveurs STUN et TURN seront utilisés pour la traversée de NAT et pare-feu.

5.5. Conclusion

Ce chapitre a fait lřobjet des différentes propositions de solution partant de lřamélioration de la fiabilité de lřentité HSS à la proposition des plateformes de développement des services. La proposition apportée à la problématique évoquée, est en rapport avec lřhypothèse 3 évoquée ci-dessus.

En effet, lřentité HSS est un élément central dans le système de télécommunications convergent. Il est important que celui-ci fonctionne normalement afin que les échanges des données utilisateurs avec les autres entités du réseau IMS soient fiables. Les résultats obtenus dans la plateforme de tests visent à décrire la procédure dřenregistrement des utilisateurs dans le réseau IMS. Ces résultats sont basés sur les tests effectués et lřanalyse des différents messages DIAMETER échangés entre les entités HSS, I-CSCF et S-CSCF ont montré lřévidence du problème au niveau du HSS. La plateforme IMS KAMAILIO et OpenIMSCore déployée a permis de mettre en évidence le dysfonctionnement du HSS. Pour résoudre ce dysfonctionnement, nous avons introduit le gestionnaire de file dřattente Rabbitmq pour améliorer les échanges dřinformation. Cette proposition de solution a valu un article dont le thème est : « ***Proposed solution for improving the reliability of HSS data by integrating a queue manager*** ». 20th International Conference on Advanced Communication Technology (ICACT), 11-14 Feb.2018, Pages: 685Ŕ693. IEEE, 2018 DOI : 10.23919/ICACT.2018.8323884.

Après avoir traité lřamélioration de la fiabilité des systèmes convergents, nous allons aborder les propositions des applications dans les systèmes convergents.

Chapitre 6 : Proposition de solutions de e-santé basées sur les réseaux convergents

Nous présentons dans ce chapitre, les applications des réseaux convergents pour lřamélioration de lřaccès aux soins de santé des populations en zone rurale. La population africaine est confrontée à de nombreux enjeux en termes dřaccès à la santé. Les patients sont obligés de se déplacer pour accéder aux services de santé mais lřaccès est rendu difficile par les problèmes de transports et lřétat des routes. Par faute de ressources financières, beaucoup nřont pas accès aux moyens de diagnostics et de prise en charge. Cela est dřautant plus vrai que lorsque le patient est hospitalisé dans une structure de santé localisée dans une ville où il nřa pas dřattache familiale, ceci occasionne ainsi des coûts additionnels inhérents à lřhospitalisation.

La quasi-totalité des hôpitaux régionaux ne disposent que dřun ou deux spécialistes voire trois spécialistes. Les spécialités que nous rencontrons fréquemment dans ces hôpitaux sont pour la plupart, les chirurgiens généralistes et les gynécologues. Les quelques rares hôpitaux qui disposent dřautres spécialistes, couvrent la cardiologie et lřorthopédie. En outre, même si ces spécialistes existent, ils ont besoin dřéchanger avec des confrères plus expérimentés pour le diagnostic et/ou la prise en charge des cas de pathologies peu fréquentes ou compliquées. Dans les pays développés, la télémédecine se définit comme « *une coopération médicale à distance* », capable dřaugmenter lřefficacité et de réduire le coût de la télémédecine traditionnelle. Dans les pays en développement, elle représente un vrai remède au manque de médecins experts et spécialisés en zone rurale. La télémédecine présente lřavantage de pouvoir sřadapter aux besoins, aux moyens technologiques et humains de chaque structure.

Le resutat attendu est dřoffrir lřaccès aux soins de qualité au plus grand nombre, et de réduire les inégalités en termes de facilitation dans les secteurs de santé entre les grands centres urbains et les zones rurales les plus isolées. Enfin, nous terminerons ce chapitre par une conclusion.

6.1. Résultat escompté

En Afrique plus particulièrement au Sénégal, les populations rurales accèdent difficilement aux services de santé dans le cas des maladies vitales telles que : lřhypertension artérielle, le

diabète, les maladies rénales, la maladie du foie, la maladie pulmonaire etc…. La plupart des structures de référence sont implantées à Dakar et au niveau des capitales régionales. Le coût de la prise en charge déjà élevé est majoré par les frais liés au déplacement et à lřhébergement, ce qui rend la tâche insupportable aux patients qui sont dans les zones isolées. Par manque de moyens financiers et de prise en charge par des médecins, beaucoup de patients meurent dans les zones rurales.

Pour ce faire, un système portatif à base de capteurs pour la surveillance continue des paramètres physiologiques est essentiel pour les patients atteints de maladies chroniques, se situant dans les zones rurales et dépourvues de médecins spécialistes.

Les récents travaux de recherches dans le domaine des e-Heath ont conclu que plusieurs paramètres vitaux peuvent être monitorés en utilisant lřArduino, la raspberry pi et les capteurs biométriques [77] [78] [79]. Pour répondre à ce besoin des milieux ruraux et afin de permettre à la population dřavoir un accès universel aux soins de qualité et à moindre coût, une solution de monitoring portatif est proposée. Le système permet à lřinfirmier (e) de choisir un spécialiste si une valeur anormale est décelée des paramètres physiologiques des maladies chroniques à savoir lřhypertension artérielle, le diabète. Il permet aussi aux spécialistes dřavoir une idée sur la température corporelle et lřélectrocardiogramme du patient, indiquée par les capteurs biométriques. Cela aide à prendre les mesures appropriées instantanées, et dřanticiper sur les éventuels risques de maladies qui peuvent subvenir à lřavenir. Un tel système peut aider à réduire les factures des hôpitaux découlant de l'admission du patient à l'hôpital et de lřaccès aux soins de qualité tout en restant dans sa localité.

6.2. Mise en œuvre de la solution

Depuis 2002, lřEtat du Sénégal à travers lřAgence de lřinformatique de lřEtat (ADIE) a bâti une infrastructure de fibre optique de 1 500 km, interconnectant 12 des 14 capitales régionales du pays en vue de permettre aux différentes structures de lřEtat dřéchanger des informations comme le montre la figure 6.1 [80]. Depuis 2016, cette interconnexion sřest améliorée grâce au partenariat entre ADIE et la société nationale dřélectricité du Sénégal (*SENELEC*) dont le réseau de fibre optique couvre les deux régions manquantes du Sénégal. Donc, à présent le réseau fibre optique ADIE-SENELEC couvre la totalité des capitales régionales du Sénégal. Concernant le transport des données, si lřhôpital est loin des points de présence (*POP*), nous

mettrons de faisceau hertzien de part et dřautre pour desservir cet hôpital. Nous voyons bien que lřinfrastructure de fibres optiques de lřADIE suit la répartition de la population concentrée sur le littoral :

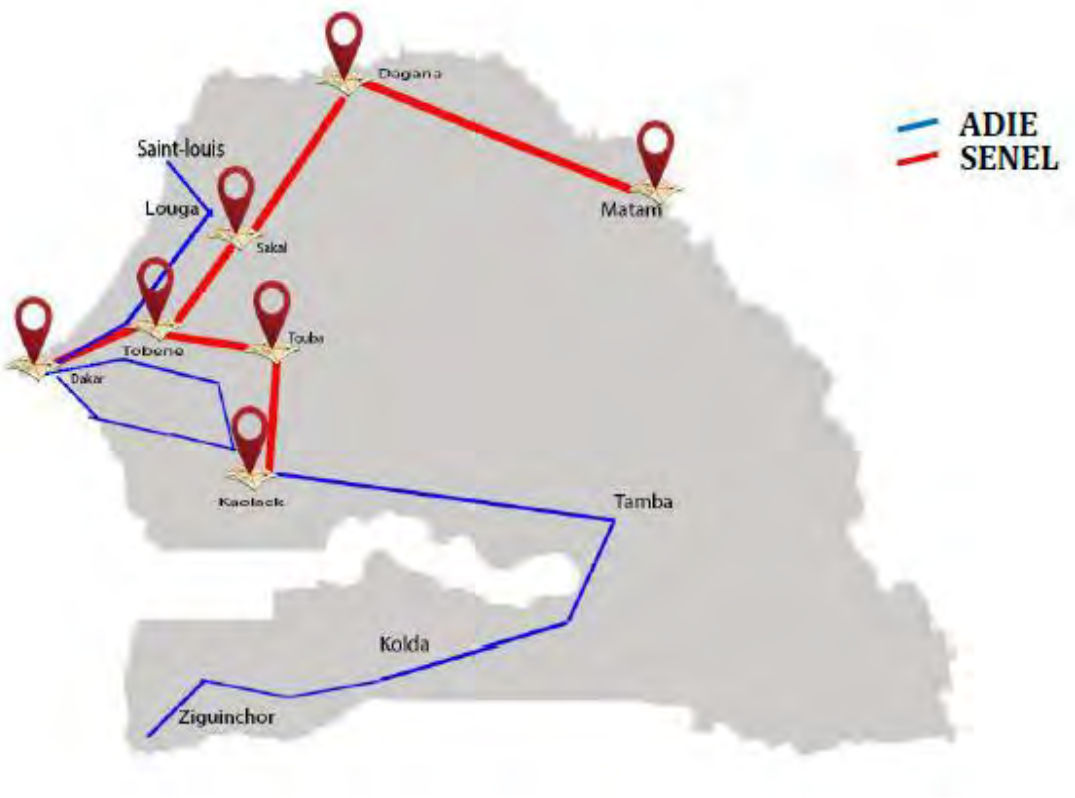


Figure 6.1. Réseau FO de l'ADIE 2016

Ainsi, le système proposé sřappuie sur ce réseau pour interconnecter les structures sanitaires des zones rurales avec celles où se trouvent les médecins spécialistes du domaine comme le diabète, lřhypertension artérielle, lřECG et la température corporelle.

6.2.1. Système de monitoring des patients

Les différents paramètres vitaux du patient sont surveillés par ce système. Les résultats sont affichés et observés par les médecins. Nous constatons :

- ✓ dřune part, le nombre de personnes souffrant de différentes maladies chroniques est assez élevé ;

- ✓ dřautre part, le nombre limité dřétablissement de santé et le manque de médecin spécialiste dans les structures sanitaires des zones rurales est à relever. Certaines maladies chroniques nécessitent un suivi régulier. Parmi ces maladies on peut citer : le diabète, lřhypertension artérielle, les maladies rénales, la maladie du foie et la maladie pulmonaire.

Le système proposé est basé sur une architecture client-serveur. Le serveur dřapplication est responsable du stockage des données du patient, du traitement des données et de lřenvoi sur le serveur dédié aux médecins.

Les paramètres physiologiques basiques qui sont :

- **La tension artérielle**

La tension artérielle résulte de la force créée par l'action de pompage du cœur qui conduit le sang dans les artères, puis dans le système circulatoire. Comme le sang coule dans les artères, ils offrent une certaine résistance à l'écoulement du sang. Près de vingt-quatre pour cent (24%) de mort au Sénégal sont causés par l'hypertension. Le dépistage précoce et le contrôle de l'hypertension peut réduire le risque de maladies cardiaques et d'insuffisance rénale [81].
La pression artérielle normale pour une personne saine est de 120/80 mmhg. Si la tension artérielle est supérieure à 140/90, on l'appelle l'hypertension artérielle [81]. La surveillance quotidienne de la tension artérielle aiderait à la contrôler et de prendre des mesures nécessaires une fois que la valeur de cette pression artérielle est anormale.

- **Le taux de sucre dans le sang**

Le glucomètre est un dispositif médical destiné à déterminer la concentration approximative de glucose dans le sang. Une petite goutte de sang obtenue en piquant la peau avec une lancette est placée sur une bande de test jetable que l'appareil de lecture utilise pour calculer le taux de glucose sanguin. Le compteur affiche le niveau en mg / dl ou mmol / l.
Malgré des intervalles très variables entre les repas ou la consommation occasionnelle de repas avec un hydrate de carbone, les niveaux de glucose dans le sang humain ont tendance à rester dans la plage normale. Cependant, peu de temps après avoir mangé, le niveau de glucose dans le sang peut augmenter, chez les non-diabétiques, temporairement jusqu'à 7,8 mmol / L (140 mg / dL) ou un peu plus [82].

- **Le rythme cardiaque**

Le pouls est la pulsation des artères résultant du battement de cœur. L'impulsion peut être généralement ressentie au cou, les poignets, derrière le genou, à l'intérieur du coude. La fréquence du battement de cœur (battements par minute) est normalement indiquée par le pouls. Au repos pour un adulte en bonne santé, le pouls normal varie entre 60-100bpm. Mais pendant le sommeil, sa valeur est à 40 bpm et pendant un exercice physique, il monte à une valeur comprise entre 200-220 bpm [82] [83] [84].

Un rythme cardiaque irrégulier ou rapide montre une anomalie cardiaque. Les étourdissements, les évanouissements, les douleurs thoraciques ou l'essoufflement peuvent être corrélés avec le pouls affecté. Le taux de pouls réduit peut également indiquer un vaisseau sanguin bloqué.

- **La température corporelle**

La température corporelle normale d'un être humain est d'environ 98,6 ° F ou 37,0 ° C. Par contre une température supérieure à 37,8 ° C (100 ° F) est considérée comme celle de la fièvre [85].

6.2.2. Système proposé pour le suivi du patient dans les zones rurales

La pression artérielle (*BP systolique et diastolique*), la fréquence cardiaque, la température corporelle et la détection du taux de sucre dans le sang sont mesurées à l'aide de capteurs biométriques interconnectés avec la raspberry pi. Le système proposé sřarticule autour de 5 entités qui sont : les capteurs, la raspberry Pi et le kit e-Heath, la base de données et lřapplication (figure 6.2).

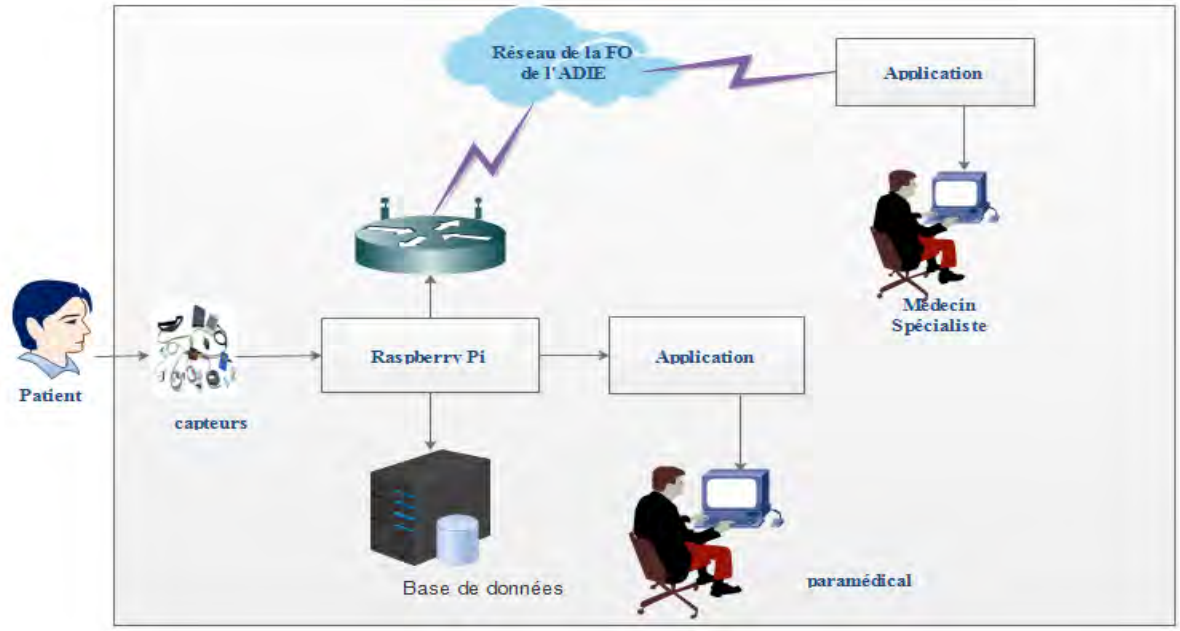


Figure 6.2. Architecture du système proposé

6.2.2.1. Les capteurs

Différents capteurs sont utilisés pour acquérir les signaux vitaux des patients. Sur le kit e-Heath V2.0 [86], qui est une carte qui permet aux utilisateurs dŕArduino et Raspberry Pi dŕeffectuer une surveillance médicale et les applications biométriques utilisant 10 différents capteurs (figure 6.3). Pour le système proposé, les capteurs suivants sont utilisés : le glucomètre, lŕélectrocardiogramme, le thermomètre et le tensiomètre.

Figure 6.3. Plateforme e-Heath

Les capteurs utilisés pour notre système sont décrits ci-dessous :

- **Le glucomètre** : cet appareil permet de mesurer rapidement le taux de glucose (sucre) dans le sang (la glycémie). Une petite piqûre au doigt avec un stylo spécial permet de recueillir une goutte de sang qu'on dépose sur une bandelette où il y a un capteur qui va analyser directement la goutte de sang. Le glucomètre est composé d'un écran à cristaux liquides qui donne des informations et des résultats, et d'une zone où l'on peut introduire la bandelette réactive où déposer la goutte de sang. Il en existe de différents modèles. Il est indispensable de suivre précisément le protocole marqué sur la notice, sinon, l'appareil inscrit une erreur marquée « **Err** ». Il donne la mesure en grammes/litre ou en millimoles/litre. Les 10 derniers résultats sont mémorisés et peuvent être rappelés. Ce système est utilisé en particulier pour la surveillance des diabétiques.

- **L'électrocardiogramme (ECG)** : il désigne un examen visant à évaluer le fonctionnement du cœur. Il est indiqué par un cardiologue en cas de suspicion ou d'antécédents de troubles cardiaques. L'ECG a pour objectif de mesurer le rythme cardiaque en enregistrant l'activité électrique du cœur. Il est indiqué chez les personnes qui se plaignent d'une douleur thoracique, un des premiers symptômes observés dans la plupart des affections cardiaques. L'électrocardiogramme est

particulièrement utile dans la détection des infarctus du myocarde (*crises cardiaques*). Il permet également de mettre en évidence une tachycardie (*rythme cardiaque anormalement élevé*), une bradycardie (*rythme cardiaque anormalement faible*) ou une inflammation du péricarde (*péricardite*). L'électrocardiogramme est également réalisé dans le cadre d'un bilan préparatoire avant une intervention chirurgicale et à titre préventif chez les sportifs, les diabétiques et les hypertendus. L'ECG est essentiellement réalisé au repos (*patient allongé sur le dos*), mais peut aussi être effectué pendant l'effort sur un vélo ou un tapis roulant (*test à l'effort*). L'ECG enregistre cinq ondes au total, respectivement appelées P, Q, R, S et T. La première représente l'activité des oreillettes, les trois suivantes celles des ventricules. La dernière onde (T) indique le moment de la mise au repos des ventricules.

- **Le thermomètre :** cet instrument permet de mesurer la température. Il se compose dřune substance qui se dilate ou se contracte suivant les variations de la température et dřune échelle graduée qui indique le degré de contraction ou de dilatation. Avec le thermomètre, nous mesurons l**a température corporelle**. La mesure de la température corporelle est un acte diagnostique essentiel en médecine générale de premier recours, réalisable par les patients, de surcroit en période de consultation. La température corporelle correspond à la température interne du corps. Chez l'être humain, la température corporelle est constante (*autour de 37 °C, mais elle peut légèrement varier suivant l'heure de la journée de 36,1 °C à 37,8 °C*), quelle que soit la température extérieure. Par définition, lřêtre humain est homéotherme, c'est-à-dire capable de maintenir sa température corporelle dans dřétroites limites quelle que soit la température extérieure. Elle est contrôlée par l'hypothalamus, qui intervient pour maintenir la température constante. S'il est trop chaud, l'organisme va transpirer pour évacuer de la chaleur. S'il est trop froid, des frissons (*correspondant à des contractions musculaires*) permettent de produire de la chaleur.

- **Le tensiomètre :** cřest un appareil de mesure médicale, utilisé pour mesurer la pression artérielle. La prise de la tension au tensiomètre manuel et stéthoscope constitue la méthode de référence. On utilise maintenant souvent des appareils automatiques, dont le brassard se gonfle automatiquement, et qui ne nécessitent plus de stéthoscope, grâce à l'utilisation de capteurs intégrés. Ces derniers sont soit

acoustiques, reproduisant la prise de tension manuelle au stéthoscope mais exigeant un bon positionnement du brassard, soit pléthysmographie, où cřest la pulsation qui est détectée. Le brassard se situe le plus souvent au niveau du poignet. Une nouvelle génération de tensiomètres connectés permet une prise de la tension et un échange de données fiables avec le corps médical.

6.2.2.2. La raspberry Pi et le kit e-Heath

La raspberry Pi est utilisée pour recevoir et analyser les signaux des différents capteurs et les envoyer vers les personnels de santé. Une carte Raspberry (figure 6.4) est en fait un micro-ordinateur. En effet, à lřinverse des cartes dites « programmables » telles que les cartes Arduino, les Raspberry possèdent tous les composants dřun ordinateur classique : sorties audio et vidéo, ports USB, lecteur de carte SD, connexion internet, etc. Ces cartes ont pour avantages dřêtre très compactes, de pouvoir être utilisées dans de nombreux domaines (*ordinateur de poche, serveur de petite taille, domotique*…), tout en étant très économique. Le choix du système dřexploitation de la carte se fait parmi un large choix de distributions Linux spécialement développées pour les Raspberry. Lřoptimisation est donc poussée à son maximum du côté du fabricant [87].

Figure 6.4. Composant basique utilisé pour acquérir les données

6.2.2.3. La base de données et les applications

Une Base de Données Relationnelle (*BDR*) est mise sur place pour stocker les données biométriques des patients, des médecins spécialistes et généralistes. Les paramédicaux et les personnels soignants peuvent accéder sur ces données. Le traitement prescrit et les conseils du médecin généraliste ou le médecin spécialiste est également disponible dans la base de données. Les infirmiers et les médecins peuvent accéder à l'information chaque fois qu'ils seront nécessaires.

Lřapplication basée sur le Web utilisant le PHP et le HTML est responsable de lřarchitecture client-serveur permettant une communication entre les paramédicaux et les médecins spécialistes [88] [89].

Côté Clients : le côté client permet l'interaction entre les infirmiers et les médecins. Les infirmiers sont les acteurs de l'acquisition des données biométriques du corps des patients en utilisant différents capteurs. Ces signaux sont transmis sur le réseau de la fibre optique de lřADIE via un point dřaccès WIFI, par lřEthernet ou le GPRS à des médecins spécialistes ou généralistes de la région du poste de santé. Une application Web est utilisée pour visualiser les signaux biométriques comme le HTA, le taux de sucre dans le sang du patient en temps réel [90].

Les informations des patients sont enregistrées ensuite les données physiologiques aussi (Nom, Prénom, Age, sexe, taille, etc.). Lorsque lřinfirmier inscrit les informations relatives au patient avec un signal, un code unique lui est envoyé pour identifier de manière unique le patient dans le réseau. Lř**Id** lui permettra de se connecter sur son compte plus tard.

Les données sont non seulement surveillées mais également comparées aux valeurs normales déjà définies. Le médecin spécialiste accède à toutes les informations avec lřimage des signaux captée par les capteurs du patient. Par conséquent, le médecin une fois quřil a les informations du patient, il les traite, prodigue des traitements et des conseils à lřinfirmier et au patient.

Coté serveurs : il est utilisé pour rendre disponible et stocker les données du patient. Le serveur dispose également dřune base de données pour stocker toutes les informations du patient et du médecin. Si le médecin, lřinfirmier et le patient veulent se communiquer, le système est capable de leurs fournir une communication par le WebRTC. Pour cela, il faut connecter une caméra sur la raspberry Pi et le médecin spécialiste doit disposer dřun appareil supportant le WebRTC.

6.3. Les paramètres expérimentaux

Le modèle proposé se base essentiellement sur la Raspberry pi pour acquérir les signaux des différents capteurs biométriques du patient et le réseau dřaccès de lřADIE.
Une application Web est développée pour envoyer ces signaux avec les informations requises au médecin spécialiste afin dřobtenir un meilleur traitement si la valeur captée dépasse la normale. Les utilisateurs incontournables du système sont les infirmiers, les médecins spécialistes et le patient. La figure 6.5 nous montre le scénario du système proposé.

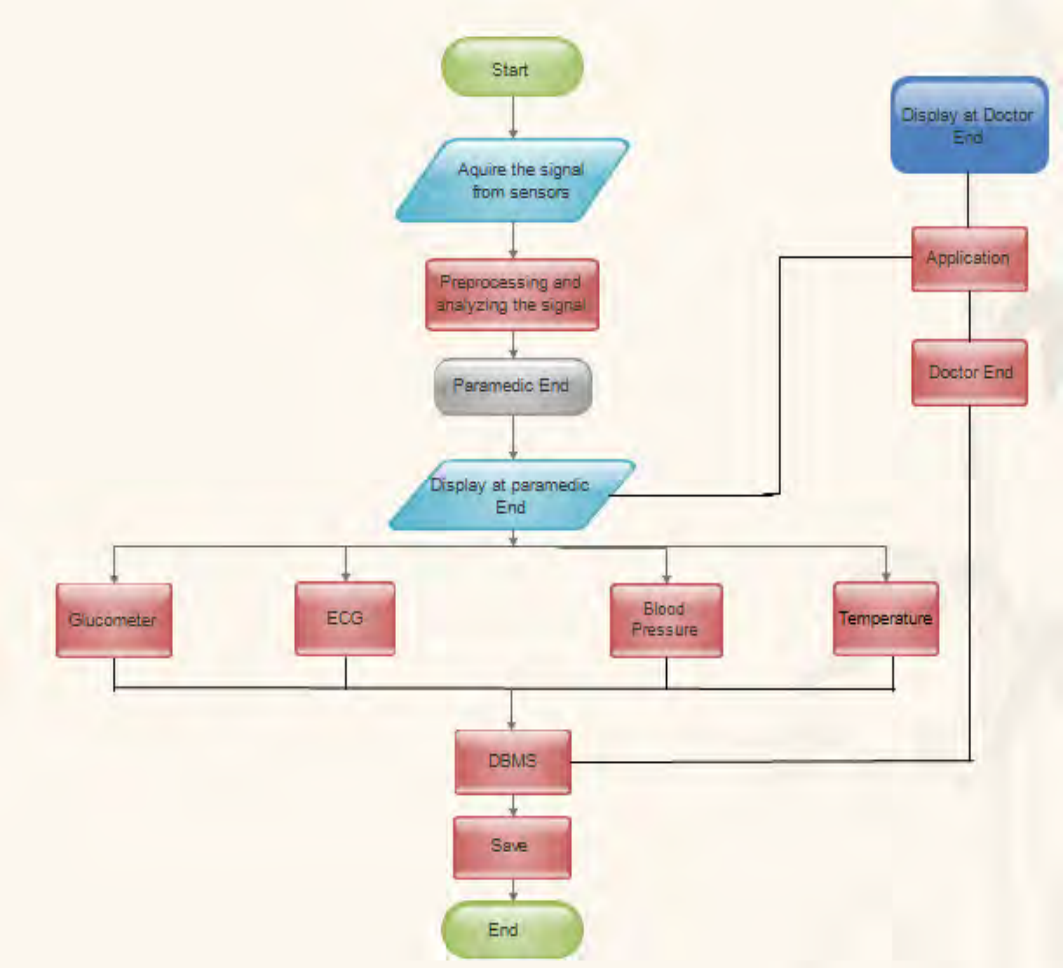


Figure 6.5. Organigramme du modèle proposé

Le paramédical remplit les renseignements des patients tel que : le Nom, Prénom, lřadresse, lřâge, le sexe, le numéro de téléphone, le domaine de la maladie. Il relève aussi lřensemble des données vitales captées par les capteurs : le tensiomètre, le glucomètre, lřECG, le thermomètre.

Une fois ces informations sont collectées, lřensemble est transmis dans la base de données et accessible partout dans le réseau de lřADIE. Après avoir rempli toutes les informations sur le patient, il sera en mesure dřattribuer au patient, un médecin spécialiste.

Pour obtenir un meilleur traitement en un peu de temps, un médecin spécialiste se connecte sur le réseau pour accéder à ces données. Une fois les données reçues, le médecin les analyse et donne des traitements et conseille le patient sur sa maladie. Le personnel paramédical peut maintenant récupérer le fichier qui peut être téléchargeable en version PDF, doc ou xls.

Le système proposé met en œuvre comme décrit précédemment : sur le côté client et serveur une application php et html sont utilisés. Ce système proposé est conçu pour fonctionner entre le médecin et les paramédicaux. La tâche principale sera de surveiller et de recueillir lřétat de santé du patient. Le médecin spécialiste peut prescrire au patient un traitement et lui donner aussi des conseils par vidéoconférence ou par chat. Lřinfirmier télécharge le fichier de traitement suivant le format voulu PDF ou autre. Lřévaluation des données est une question importante dans les systèmes de surveillance des patients. Les données sont non seulement surveillées mais également comparées aux valeurs normales déjà définies (figure 6.6).

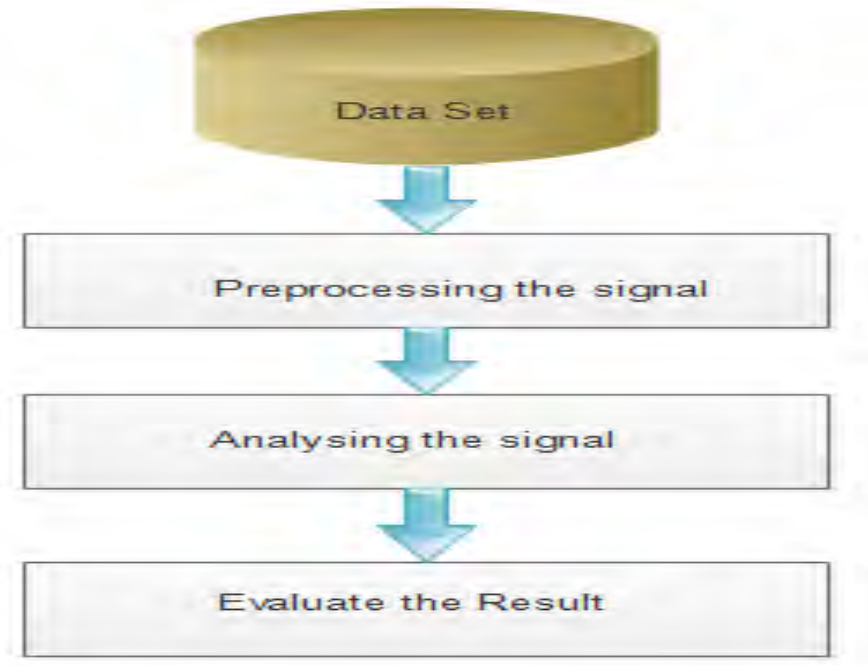


Figure 6.6. Traitement de données et évaluation des résultats

Si les données sont hors de la gamme normale de valeurs prédéfinies, lřinfirmier envoie un message dřalerte au médecin spécialiste de la maladie. Ce dernier peut recevoir un message sur sa boite email et un SMS via un module GSM incorporé dans le système.

Par ailleurs, nous avons aussi collaboré avec les collègues du laboratoire LIRT pour proposer un système de e-santé sřappuyant sur lřIMS, le WebRTC et les objets connectés pour que les enfants du monde rural puissent être consultés à distance par les meilleurs spécialistes dans le domaine de la pédiatrie. Cela a valu un article à la 21ème Conférence IEEE/ICACT2019 à Pyeongchang en Corée du SUD. Le titre de lřarticle est intitulé: « *Proposition of Health Care System Driven by IoT and KMS for Remote Monitoring of Patients in Rural Areas: Pediatric Case* ».

Ainsi, cet article a reçu le prix du meilleur article de la conférence ICACT 2019 [92] [93].

6.4. Pistes d'amélioration du système e-santé

Pendant que nous avons travaillé à mettre en œuvre le système de e-santé qui aiderait la population à accéder aux soins médicaux dans les zones rurales, dřautres pistes de réflexion dřamélioration du système ont été abordées. Deux pistes dřamélioration ont été identifiées à savoir :

- ✓ une proposition du point de vue infrastructure de télécommunications de lřEtat Sénégalais;
- ✓ une proposition du point de vue facilitation de lřusage de tous les équipements de e-santé utilisés par les paramédicaux.

Afin que lřutilisation de tous les périphériques soit aisée, il faut deux choses :

- ✓ lřutilisation de lřIMS par lřADIE ;
- ✓ lřautomatisation de lřusage des équipements est nécessaire pour que les paramédicaux sur le terrain ne puisse être bloqués par un paramétrage compliqué donc il y a risque.

6.4.1. Proposition du point de vue infrastructure de télécommunications de l'Etat Sénégalais

Depuis 2002 à 2016, lřEtat du Sénégal à travers lřAgence de lřinformatique de lřEtat (ADIE) a bâti une infrastructure de fibre optique. LřADIE et la SENELEC ont noué un partenariat en 2016 de mutualisation de leurs réseaux de fibre optique. Ce qui permet de couvrir toutes les capitales régionales et départementales du Sénégal. Ceci constitue une bonne infrastructure

des télécommunications pour déployer tout type de réseau visant à offrir des services de bonne qualité à tous les utilisateurs.

Nous proposons la mise en place dřun réseau VoLTE de lřEtat du Sénégal. Les conditions pour redéployer un réseau VoLTE sont les suivantes :

- un réseau 4G ;
- un réseau IMS ;
- de serveurs dřapplication (*AS*) afin de développer la fonction SRVCC (*Single Radio Voice Call Continuity*). Le SRVCC est une fonction particulière du réseau IMS qui assure le maintien en cas de handover inter-système PS-CS. Il assure pour cela lřancrage des flux de la signalisation téléphonique et de la voix. La fonction SRVCC est en fait un sous-ensemble de la fonction ICS (*IMS Centralized Services*) qui définit un contrôle unique de la signalisation téléphonique basée uniquement sur les mécanismes de lřIMS. Elle sřapplique aux réseaux de mobiles quel que soit le mode PS ou CS utilisé pour mettre en place le support de la voix [8] [29].

Or, pour avoir un réseau 4G, il faut :

- un bon réseau de fibre optique (*infrastructure de télécommunications*) ;
- une disponibilité de plage de fréquence adéquate à 4G.

Depuis quelques années, le Sénégal dispose déjà dřune bonne infrastructure de fibre optique (*réseau FO ADIE*), un atout majeur pour le transport des données. Aussi, depuis juin 2015, le Sénégal est passé de la télévision analogique à la télévision numérique terrestre libérant ainsi les fréquences UHF pouvant être utilisées par les sept (7) différents opérateurs de télécommunications. Même si lřEtat décide de céder cinq (5) plages aux opérateurs privés, il en restera deux (2) quřil pourra céder une plage de fréquences à lřADIE pour quřelle puisse développer un réseau VoLTE. Les travaux de recherche déjà faits, ont créé les conditions de e-santé, les données fournies par le réseau doivent être fiables en exigeant un réseau aussi fiable. Pour aller plus loin, lřamélioration de lřIMS pourrait continuer car la fiabilité des données est de rigueur.

Une couverture presque totale du territoire en se basant sur le réseau 4G et lřIMS performant permettront dřaméliorer le système e-santé. Lřusage des moyens de communication entre les médecins spécialistes et les paramédicaux sur le terrain doit être simplifié (*utilisation de la visioconférence entre les acteurs*) tout en transitant par le Web (*WebRTC*). Tous les travaux (*expériences*) menés au niveau du laboratoire, montrent bien la faisabilité du WebRTC-IMS.

Ils peuvent être appliqués pour réaliser la visioconférence entre les acteurs afin de faciliter des échanges et de permettre aux paramédicaux des régions de recevoir des instructions des spécialistes pour un bon suivi des patients.

Une discussion a eu lieu en son temps pour le déploiement du réseau VoLTE de lřEtat dont le coût dřinvestissement est évalué dans le paragraphe ci-dessous.

6.4.1.1. Le coût de déploiement de la solution VoLTE

Il y a eu une discussion avec le deuxième opérateur téléphonique de la Corée du Sud. Les ingénieurs ont calculé le coût de déploiement de la 4G qui sřélève à 40 milliards (*le réseau fibre optique de l''Etat Sénégalais n''est pas pris en compte dans ce coût*).

Dans la poursuite de négociation des travaux, en intégrant le réseau fibre optique de lřEtat du Sénégal dans le projet, le coût de lřinvestissement pourrait être réduit autour de vingt (20) milliards. Or, ces vingt (20) milliards devraient couvrir :

- lřacquisition des équipements de télécommunications pour lřIMS ;
- lřacquisition de solutions logicielles intégrant la fonction SRVCC nécessaire pour la VoLTE.

Il est possible de faire baisser ces coûts en utilisant les logiciels libres qui ont fait leur preuve dans le domaine de la recherche tels que le Kamailio [36], le Clearwater [54].

Ce qui est essentiel, cřest de bien dimensionner les équipements qui devront hébergés le Kamailio ou le Clearwater. La fonction SRVCC peut être aussi développée localement par des ingénieurs.

Nous pouvons réduire de moitié le coût du projet avec tout ce que nous savons faire. Cet investissement est à portée de main de lřEtat du Sénégal.

6.4.2. Proposition du point de vue facilitation de l'usage de tous les équipements de e-santé utilisés par les paramédicaux

Une fois que le réseau est mis en place, les configurations et lřusage des équipements ne doivent pas constituer un frein pour sa mise en œuvre par les utilisateurs du système qui sont pour la plupart des agents du secteur de santé, nřayant pas nécessairement de connaissance en réseau ou télécommunications. Nous proposons que le système puisse intégrer la découverte

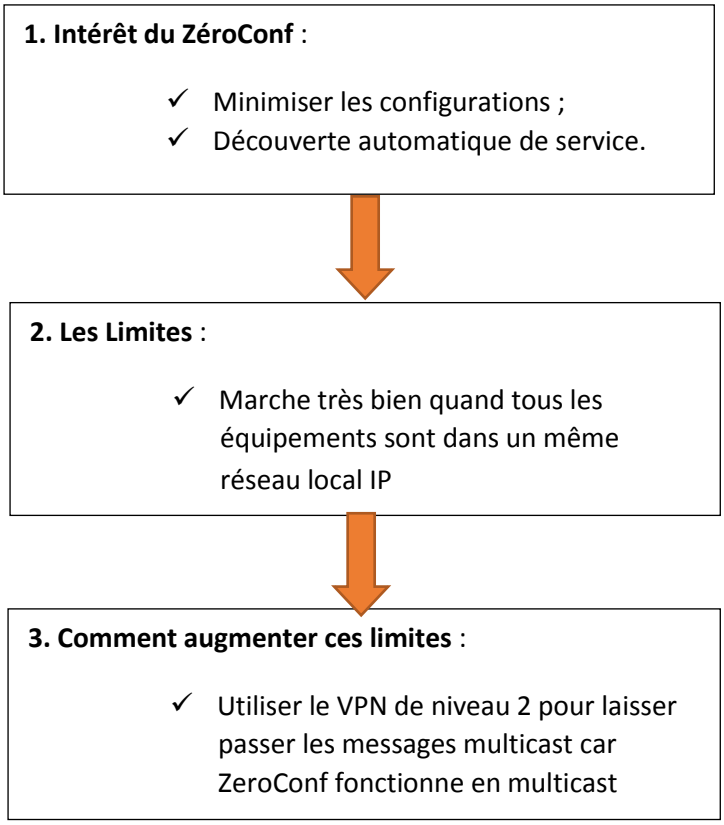
et lřautoconfiguration des terminaux. Ainsi, les difficultés liées à la configuration et à lřusage des équipements devraient être minimisées de manière à ne pas décourager les acteurs.

La découverte automatique des ressources par les terminaux des utilisateurs et lřautoconfiguration de ces derniers sont possibles grâce à lřutilisation du ZeroConf [94] [95] [96] [97]. [98] [99] [100]

En effet, ZeroConf est un ensemble de protocoles qui permet de faciliter lřusage dřun certain nombre dřéquipements. Le protocole fonctionne en mode multicast donc facile à implémenter dans un réseau local. Cependant, sa prise en charge dans un réseau étendu, nécessite un certain nombre de configuration. Des expériences faites au laboratoire, basées sur lřusage dřun VPN [101] de niveau 2 et non de niveau 3, a permis lřusage du protocole ZeroConf sur un réseau étendu où les services tels que lřaudio, la vidéo, le transfert de fichier, le partage dřécran etc… ont été découverts de manière automatique par les terminaux des utilisateurs.

Fort de ces expériences, nous proposons le regroupement de districts sanitaires en réseau logique IP que nous pourrons interconnecter par VPN de niveau 2.

Le schéma ci-dessous résume notre choix dřamélioration du système e-santé par ZéroConf et VPN :



6.5. Conclusion

Comme dans de nombreuses zones rurales du continent africain en général et en Afrique francophone en particulier, les distances entre les patients, les agents de santé et les médecins spécialistes aggravent une situation sanitaire déjà précaire, causée par un déficit de personnel médical et de structures de santé moins nombreuses.

Ce système de surveillance de l'accès universel mérite dřêtre déployé dans les zones rurales éloignées. Il réduit considérablement les dépenses et améliore la qualité de vie des patients. Il permettra à lřEtat Sénégalais de réduire considérablement le taux de mortalité. Un tel système propose de possibilités de diagnostics des patients par des spécialistes et offre par ricochet des qualités de soin au plus grand nombre, et réduit les inégalités en termes de santé entre les grands centres urbains et les zones rurales les plus isolées.

Il faut noter aussi que lřinterconnexion IMS-WebRTC permet dřétablir de discussion entre les acteurs de la santé afin de recevoir des instructions des spécialistes pour aider aux soins des malades des zones reculées. Cette proposition de solution a valu un article au journal IEEE dont le thème est : « *Proposal for a universal access solution to care in rural areas : case of Sénégal* », 20th International Conference on Advanced Communication Technology (ICACT), 11-14 Feb. 2018, Pages : 643Ŕ646. IEEE, 2018.

Pour faciliter lřaccès aux données, une découverte automatique des ressources par les terminaux des utilisateurs et lřautoconfiguration de ces derniers sont possibles grâce à lřutilisation du ZeroConf. Puis, lřusage dřun VPN de niveau 2, a permis lřusage du protocole ZeroConf sur un réseau étendu. Lřutilisation du VPN permet de sécuriser les données à partager sur les différents réseaux, un premier niveau de sécurité non négligeable.

Une autre proposition dřun système de e-santé sřappuyant sur lřIMS, le WebRTC et les objets connectés, permettra aux enfants du monde rural dřêtre consultés à distance par les meilleurs spécialistes.

Les chapitres 1, 2 et 3 établissent les généralités et font lřétat de lřart en lien avec la thématique abordée. Le chapitre 4 présente lřenvironnement et les outils utilisés dans la thèse. Les chapitres 5 et 6 font ressortir les contributions majeures durant nos travaux de recherche. Enfin, nous terminons la thèse par une conclusion générale qui suit.

Conclusion générale

Nos travaux de thèse ont commencé par la délimitation du champ de recherche en faisant la genèse de lřévolution des réseaux mobiles depuis la première étape jusquřà la sixième étape du chapitre 1. Lřétude de ces six (6) étapes démontre que lřIMS demeure le socle des architectures numériques de nouvelle génération. Lřun des avantages de lřIMS est lřutilisation du protocole IP comme standard de communication et le SIP pour la signalisation, ce qui facilite la convergence entre les réseaux mobiles, les réseaux fixes et lřInternet.

Lřétude détaillée de lřIMS permet de connaitre son architecture et son fonctionnement. Lřun de nos défis majeurs était dřimplémenter une plateforme sous Kamailio avec les logiciels libres. Ceci dans le but de nous sřintéresser à lřamélioration de la fiabilité du système IMS et de proposer des solutions dřapplications pour lřaccès aux soins de santé pour les populations en zones rurales.

Les travaux présentés dans cette thèse traitent de problématiques suivants :

- dřune part, sur la fiabilité de lřIMS concernant lřenregistrement dřun abonné sur la base de données HSS. Le HSS constitue un élément central de lřIMS ;
- dřautre part, sur lřaccès difficile aux soins de santé des populations et des plus jeunes (la pédiatrie) dans les zones rurales.

En effet, un système est dit fiable lorsque nous notons une permanente disponibilité du service pour lřabonné lors de lřétablissement dřune communication de bout en bout, aucune défaillance nřest constatée et que cette communication est de meilleure qualité pour lui.

Grâce au code ouvert des logiciels libres, nous avons proposé une architecture de tests basée sur la plateforme SIP Kamailio. Ceci nous a permis de faire des tests grandeur nature dans lřenregistrement dřun utilisateur afin de déceler un dysfonctionnement au niveau du HSS. Une proposition de solution par lřutilisation dřun broker (gestionnaire de file dřattente), va introduire un temps dřattente au niveau du HSS qui ne pourra envoyer ses données quřaprès réception du message SIP de confirmation de connexion. Ainsi, lřapport des brokers a permis de résoudre le problème de synchronisation des connexions au niveau du HSS. Ce travail a valu un article à la conférence ICACT de 2018.

Concernant lřaccès aux soins de santé, deux applications ont été proposées à savoir :

- le suivi et la surveillance des paramètres physiologiques vitaux des patients dans les zones rurales ;

- la prise en charge à distance des enfants les plus petits du monde rural.

Pour la première application, les patients sont obligés de se déplacer pour accéder aux services de santé en ville mais lřaccès est rendu difficile par les problèmes de transports et lřétat des routes. La prise en charge nřest plus évidente à cause de ces contraintes. Il faut proposer une solution dřaccès aux soins de santé de qualité au plus grand nombre en zones rurales. Pour se faire, la mise en place dřune architecture de type internet des objets va permettre le suivi et la surveillance des paramètres physiologiques vitaux des patients dans les zones rurales. Ces paramètres vitaux sont mesurés et envoyés via une carte raspberry Pi vers une base de données. Une application Web permet lřexploitation de ces résultats. Cette solution de monitoring portatif permet à lřinfirmier (e) de choisir un spécialiste si une valeur anormale est décelée des paramètres physiologiques des maladies chroniques tels que lřhypertension artérielle et le diabète. Elle permet aussi aux spécialistes de prendre les mesures appropriées instantanées, et dřanticiper sur les éventuels risques de maladies qui peuvent subvenir à lřavenir. Un tel système peut aider à réduire les coûts de déplacement aux patients, permet la prise en charge rapide et lřaccès aux soins de qualités tout en restant dans leur localité. Il permet aussi un meilleur suivi des patients.

La deuxième application contribue à la réduction du taux de mortalité infantile et juvénile dans les zones rurales. Ce taux reste élevé jusquřaujourd'hui. Pour ce faire, une plate-forme basée sur le serveur multimédia WebRTC Kurento et lřInternet des Objets, permet aux médecins de la pédiatrie, d'effectuer des consultations à distance sur les enfants accompagnés de leur mère. Ces médecins spécialistes, après avoir reçu les données biométriques du patient, prennent une décision et prescrivent un traitement approprié à distance quel que soit l'emplacement en utilisant le réseau de fibre optique du pays.

Nos propositions de solutions dans le domaine de e-santé vont aider les populations des zones rurales à se soigner le plus rapidement possible par les meilleurs spécialistes et à moindre coût. Ces solutions vont permettre de réduire considérablement les dépenses et dřaugmenter la qualité de vie des patients. Un autre bénéfice, ce que les infirmier(e)s, les généralistes et les spécialistes sřappuieront sur ce réseau pour collaborer efficacement dans lřintérêt des patients.

Ces deux applications nous ont valu deux articles : un article à la conférence ICACT de 2018 puis le deuxième article à la conférence ICACT 2019 et a obtenu le prix du meilleur article.

En définitif, il faut un très bon réseau fidèle et fiable pour lřutilisation optimum de ces applications proposées pour lřamélioration de conditions de vie de nos populations. Nous avons besoin des personnes en bon état de santé pour participer activement à lřéconomie de nos pays et au développement de lřAfrique tout entière.

Ce travail de recherche ouvre plusieurs perspectives, parmi lesquelles nous pouvons noter :

- Le modèle dřintégration du gestionnaire de file dřattente pour améliorer la fiabilité du système IMS est une évidence mais lřutilisation dřautres outils de modélisation de file dřattente pourra permettre dřobtenir des résultats probants.
- La consolidation de la table de localisation des utilisateurs de lřentité HSS est à garantir lors de lřétablissement dřune communication.
- LřIMS et le WebRTC constituent des outils de recherche à explorer dans lřoptimisation de solutions dřinteropérabilité IMS-WebRTC.
- Le renforcement davantage de la sécurité des données dans lřexploitation de ces applications doit être notre priorité.

Liste de publications

1. Ngartabé KAG-TEUBE; Yvan Paillard Kalia-Sya Dodoagnen; Samuel Ouya; Kéba Gueye, " ***Proposed solution for improving the reliability of HSS data by integrating a queue manager***.". 20th International Conference on Advanced Communication Technology (ICACT), 11-14 Feb. 2018, Page s: 685 Ŕ693. IEEE, 2018 DOI : 10.23919/ICACT.2018.8323884
2. Kéba GUEYE, Ngartabé KAG-TEUBE, Samuel OUYA, Davy Edgard MOUSSAVOU, " ***Proposal for a universal access solution to care in rural areas: case of Sénégal***. ", 20th International Conference on Advanced Communication Technology (ICACT), 11-14 Feb. 2018, Page s: 643 Ŕ646. IEEE, 2018 DOI**:** 10.23919/ICACT.2018.8323866
3. Kéba GUEYE, Bessan M. DEGBOE, Samuel OUYA, Ngartabé KAG-TEUBE " ***Proposition of Health Care System Driven by IoT and KMS for Remote Monitoring of Patients in Rural Areas: Pediatric Case.*** ", 21th International Conference on Advanced Communication Technology (ICACT), 17-20 Feb. 2019, Page s: 676 Ŕ680. IEEE, 2019 DOI**:** 10.23919/ICACT.2019.8702009

Bibliographie

[1] André Pérez ; Ř'*Architecture des réseaux de mobiles : GSM/GPRS, UMTS/HSPA, EPS, NGN, IMS*'"'*;* ISBN **978-2-7462-3279-2 ; ISSN 2102-3220** ; ©2011, Lavoisier, Paris ; www.editions.lavoisier.fr

[2] Thierry LUCIDARME ; '"'*Principes de radiocommunication de troisième génération : GSM, GPRS, UMTS…* '"'©Vuibert, Paris, 2002, **ISBN 2-7117-8693-5**

[3] BRASSAC Anne, DARRIEULAT Maya, HADJISTRATIS Emmanuel, ROUSSE David, « *Les réseaux sans fil* **»** DESS MIAGe 2001-2002 Université Paul Sabatier Université Sciences Sociales Toulouse

[4] AJGOU.R, ABDESSELAM.S, « *Evolution de réseau GSM (GPRS, EDGE)* **»**, Université El-oued et Université Med khider Biskra

[5] www.itu.int/rec/T-REC-Q.706 : Système de signalisation numéro 7 Ŕ fonctionnement attendu en signalisation du sous-système transport de messages

[6] www.efort.com/r_tutoriels/SS7_EFORT.pdf

[7] http://www.efort.com/r_tutoriels/SIGTRAN_EFORT.pdf

[8] André Pérez; Ř*La voix sur LTE: Réseau 4G et architecture IMS*'"; **ISBN 978-2-7462-4546-4; ISSN 2102-3220;** ©2013, Lavoisier, Paris; www.editions.lavoisier.fr

[9] Bouba GONI MAHAMADOU*, ,,'Voix sur LTE*'"; UCAD, ESP ; Dakar, Senegal, 2015

[10] *An Introduction to LTE: LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications*, Second Edition. Christopher Cox. © 2014 John Wiley & Sons, Ltd. Published 2014 by John Wiley & Sons, Ltd

[11] Yannick Bouguen, Eric Hardouin, François-Xavier Wolff ;řř *LTE et les réseaux 4G*'"'*;* © Groupe Eyrolles, 2012, **ISBN 978-2-212-12990-8**

[12] Huang.C, Li.J : *One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS* ; 21st International Conference on Advanced Networking and Applications (AINA'07). 2007.

[13] Harri Holma et Antti Toskala, UMTS les réseaux mobiles de 3ème generation, edition

[14] *Kühne.R, Görmer.G, Schläger.M, Carle.G :* Charging in the IP Multimedia Subsystem : A Tutorial ; IEEE Communications Magazine • July 2007

[15] Mukka Prikselka & Georg Mayer-Wiley, IMS-IP Multimedia Concepts and Services, edition Wiley

[16] Khalid Al-Begain, Chitra Balakrishna, Luis Angel Galindo, David Moro Fernandez, IMS A development and Deployment Perspective, edition Willey John et Sons
[17] Gonzalo Camarillo, Miguel A. Garcia-Martin, The 3G IP Multimedia Subsystem, edition Wiley

[18] http://www.institut-numerique.org/chapitre-ii-role-principal-de-la-signalisation-dans-un-reseau-telephonique-515d5091f296b

[19] Abdallah HANDOURA, 2009,řř*Création et sécurisation des services télécoms fixes et mobiles sur IP"*.'Thèse doctorat : Université de Bretagne Sud (France)

[20] Packet-based multimedia communications systems, H.323, http://www.itu.int/rec/T-REC-H.323/en.

[21] SIP, RFC 3261, http://www.ietf.org/rfc/rfc3261.txt.

[22] Olivier Hersent, David Gurle, Jean Pierre Petit, La Voix sur IP : Déploiement des architectures VoIP, IMS et TISPAN, protocoles SIP, 3GPP et IETF, H323, MGCP, édition Dunod

[23] Olivier Hersent, David Gurle, Jean Pierre Petit, La Voix sur IP codecs, H323, SIP, MGCP, déploiement et dimensionnement, édition Dunod

[24] Samuel OUYA, 2015, řř *Etude de la convergence des services de télécommunication et ses applications aux organisations virtuelles"*.'Thèse doctorat Télécommunications : Université Chiekh Anta Diop de Dakar (Sénégal)

[25] : site officiel du Diameter : http://www.diameter.org

[26] IETF, *"Diameter Request for comments 6733"* (RFC-6733), V. Fajardo, Ed., J. Arkko, J. Loughney, G. Zorou, Ed., DOI: 1017487/RFC6733 [Online]. Available: www.tools.ietf.org/html/rfc6733, Octobre 2012

[27] Ę*Diameter SIP Application 4740*ę (RFC- 4740) HOME Page [Online]. Available: www.tools.ietf.org/html/rfc4740

[28] IETF, *'' HTTP Authentication: Basic and Digest Access Authentication"*"(RFC2617) HOME Page [Online]. Available: www.tools.ietf.org/html/rfc2671

[29] Myleen Dosado Villaluz, Ragil Putro Wicaksono, Adrian Dan Ebora Atienza, Seiji Kunishige, Kwangrok Chang, Jennylou Banzon Caasi, *„VoLTE SRVCC Optimization as Interim Solution for LTE Networks with Coverage Discontinuity"*, MOTiV Research Co. ; Tokyo, Japan ; firstname.lastname@motiv-research.com, 978-1-4673-7116-2/15/$31.00 ©2015 IEEE, 2015

[30] **"***Cx and Dx Interfaces Based on the Diameter Protocol (Release 11)***",** 3GPP TS 29.229Ŕ 2011, 2011.

[31] Ngartabé Kag-Teube; Yvan Paillard Kalia-Sya Dodoagnen; Samuel Ouya; Kéba Gueye, « *Proposed solution for improving the reliability of HSS data by integrating a queue manager* ». 20th International Conference on Advanced Communication Technology (ICACT), 11-14 Feb. 2018, Page s: 685 Ŕ693. IEEE, 2018 DOI : 10.23919/ICACT.2018.8323884

[32] SNT/08/2016/V1/DRJ/DRG du mois dřaoût 2016 intitulé : Service dřinterconnexion catalogue 2016 de SONATEL

[33] Imène ELLOUMI, 2012,řř*Gestion de la mobilité inter réseaux d'accès et de Qualité de Service dans une approche NGN/IMS*"". Thèse doctorat : Université de Carthage (Tunisie)

[34] https://fr.wikipedia.org/wiki/Convergence_num%C3%A9rique

[35] Yvan Kalia, *„ Impact de l'IMS sur le NGN multimédia"*,"EC2LT ; Dakar, Senegal, 2012

[36] James Gaglo *„ Contributions aux environnements de développement de services de télécoms dans le contexte de réseaux mobiles full IP haut débit „*," UCAD, ESP ; Dakar, Senegal, 2015

[37] Mohamed MAACHOUI, 2015,řř*Sécurité et performance pour les réseaux de nouvelle génération (NGN)*"." Thèse doctorat : Université de Toulouse (France)

[38] MEALLING, MICHAEL ; FALTSTROM, PATRIK : The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM). In : *RFC 3761* (2004)

[39] J. Roux Ngo Bilong*, „ Etude de performances des plateformes e-learning collaboratives utilisant le WebRTC et les réseaux sociaux"*"; UCAD, ESP ; Dakar, Sénégal, 2015

[40] *Signalisation dans l"architecture WebRTC EFORT*, HOME Page [Online]. Available: http://www.efort.com, 2016

[41] I. Baz Castillo J. Millan Villegas V. Pascual, IETF (RFC 7118) *„ The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)"*", DOI: 10.17487/RFC7118, JANUARY 2014

[42] Adham Zeidan, Armin Lehmann, Ulrich Trick, Research Group for Telecommunication Networks, University of Applied Sciences Frankfurt am Main, *"WebRTC enabled multimedia conferencing and collaboration solution"*; Germany; zeidan@e-technik.org

[43] 3rd Generation Partnership Project*;" Technical Specification Group Services and System Aspects"*; Study on Web Real Time Communication (WebRTC) access to IP Multimedia Subsystem (IMS); Stage 2 (Release 12**),** Décembre 2013

[44] Jim Van Meggelen, Leif Madsen & Jared Smith Asterisk The Future of Telephony 2nd Edition, Edition ŘO'REILLYř, année 2007

[45] Sébastien Déon VoIP et ToIP Asterisk: La téléphonie sur IP, Edition ŘENř, année 2007

[46] Priyanka Gupta, Neha Agrawal, Mohammed Abdul Qadeer, « *GSM and PSTN Gateway for Asterisk EPBX* ». 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), 26-28 July 2013, IEEE 2013

[47] Imran, Ale, Mohammed A. Qadeer, and M. Khan. ţ*Asterisk VoIP private branch exchange*.ţ In Multimedia, Signal Processing and Communication Technologies, 2009. IMPACTř09. International, pp. 217-220. IEEE, 2009.

[48] Qadeer, Mohammed Abdul. ţ*Dynamic Call Transfer through Wi-Fi Networks Using Asterisk*.ţ In Proceedings of the International Conference on Soft Computing for Problem Solving (SocProS 2011) December 20-22, 2011, pp. 51-61. Springer India, 2012.

[49] Mohammed Abdul Qadeer; Kanika Shah ; Utkarsh Goel, « *Voice - Video Communication on Mobile Phones and PCs' Using Asterisk EPBX* ». 2012 International Conference on Communication Systems and Network Technologies, Page s: 534 Ŕ538, IEEE 2012

[50] Sarwar Khan ; Nouman Sadiq. « *Design and configuration of VoIP based PBX using asterisk server and OPNET platform* ». International Electrical Engineering Congress (iEECON)**,** 8-10 March 2017, Page s: 1 Ŕ4, IEEE, 2017 DOI: 10.1109/IEECON.2017.8075808

[51] Abdullah Mohammad Ansari ; Md. Faisal Nehal ; Mohammed Abdul Qadeer, « *SIP-based Interactive Voice Response System using FreeSwitch EPBX* », Tenth International Conference on Wireless and Optical Communications Networks (WOCN) 26-28 July 2013, Page s: 1 Ŕ5, IEEE, 2013 **DOI:** 10.1109/WOCN.2013.6616224

[52] *„ŻAMQP: Advanced Message Queuing Protocol Protocol´´*, Specification Version 0-9-1, General-Purpose Messaging Standard, 13 November 2008

[53] Victor González Chamorro; Carlos Nuñez Castillo; Fabio Lopez-Pires, « *An Elastic VoIP Solution Based on OpenStack* ». International Conference on Information Systems Engineering (ICISE), 20-22 April 2016, Page s: 43 Ŕ 47, IEEE 2016. DOI : 10.1109/ICISE.2016.8

[54] *„Ţ Project Clearwater Release 1.0´´*, Metaswitch Networks, July 25, 2016

[55] Raja Anwaar Ali; Anooshah Nooshad Khan; Saba Arshad; Usman Younis, « *Towards the development of LTE networks: Implementation of OpenIMSCore in asterisk/OpenBTS GSM network* ». International Conference on Open Source Systems and Technologies, 16-18 Dec. 2013, Page s: 103 Ŕ106, IEEE, 2013. DOI : 10.1109/ICOSST.2013.6720614

[56] Afaq Hasan Khan; Mohammed Abdul Qadeer, « *Implementation of an IMS Testbed for Wired and Wireless Clients* ». International Conference on Data Storage and Data Engineering, 9-10 Feb. 2010, Page s : 106 Ŕ110, IEEE, 2010

[57] Eueung Mulyana; Tutun Juhana; Dwianto Dana Satriya; Dian Fatra Anggita, « *IP Multimedia Subsystem: A lab-scale test-bed: Implementation and case study for Click-to-Dial and VoD services* ». 6th International Conference on Telecommunication Systems, Services,

and Applications (TSSA), 20-21 Oct. 2011, Page s : 181 Ŕ 185, IEEE, 2011. DOI : 10.1109/TSSA.2011.6095430

[58] Luis López Fernández, Miguel París Díaz, Raúl Benítez Mejías, Francisco Javier López, José Antonio Santos Naevatec;*" Kurento: a media server technology for convergent WWW/mobile real-timemultimedia communications supporting WebRTC"*¸" Grupo de Sistemas y Comunicaciones (GSyC) Universidad Rey Juan Carlos (URJC), (Madrid), Spain; Las Rozas (Madrid), Spain; DOI: 978-1-4673-5828-6 ©2013 IEEE

[59] Luis López-Fernández; Micael Gallego; Boni García; David Fernández-López; Francisco Javier López, « *Authentication, Authorization, and Accounting in WebRTC PaaS Infrastructures: The Case of Kurento* ». 15 August 2014, Page s: 34 Ŕ 40, IEEE Internet Computing, 2014, Volume: 18, Issue: 6. DOI: 10.1109/MIC.2014.102

[60] Luis López Fernández; Miguel París Díaz; Raúl Benítez Mejías; Francisco Javier López; José Antonio Santos, « *Kurento: a media server technology for convergent WWW/mobile real-time multimedia communications supporting WebRTC* ». IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 4-7 June 2013, Page s : 1 Ŕ 6, IEEE, 2013. DOI : 10.1109/WoWMoM.2013.6583507

[61] Boni Garcia; Luis Lopez-Fernandez; Micael Gallego; Francisco Gortazar, « *Kurento: The Swiss Army Knife of WebRTC Media Servers* ». IEEE Communications Standards Magazine, 26 July 2017, Page s: 44 Ŕ 51, IEEE, 2017, Volume: 1, Issue: 2. DOI:10.1109/MCOMSTD.2017.1700006

[62] Kay Haensge; Michael Maruschke, « *QoS-based WebRTC access to an EPS network infrastructure* ». 18th International Conference on Intelligence in Next Generation Networks, Page s: 9 Ŕ 15, IEEE, 2015

[63] Boni Garcia; Luis Lopez-Fernandez; Francisco Gortazar; Micael Gallego, « *Analysis of Video Quality and End-to-End Latency in WebRTC* ». IEEE Globecom Workshops (GC Wkshps), 4-8 Dec. 2016, Page s : 1 Ŕ 6, IEEE, 2016. DOI : 10.1109/GLOCOMW.2016.7848838

[64] Cristian Constantin Spoiala; Alin Calinciuc; Corneliu Octavian Turcu; Constantin Filote, « *Performance comparison of a WebRTC server on Docker versus virtual machine* ». International Conference on Development and Application Systems (DAS), 19-21 May 2016, Page s: 295 Ŕ 298, IEEE, 2016. DOI : 10.1109/DAAS.2016.7492590

[65] 3rd Generation Partnership Project*;" Technical Specification Group Services and System Aspects"*; Study on Web Real Time Communication (WebRTC) access to IP Multimedia Subsystem (IMS); Stage 2 (Release 12**),** Décembre 2013

[66] Pavel Segeč, Peter Palúch, Jozef Papán, Milan Kubina, *„ťhe integration of WebRTC and SIP: way of enhancing real-time, interactive multimedia communication"*¨DOI: 978-1-4799-7740-6/, ©2014 IEEE, December 4-5, 2014

[67] Samuel OUYA, Gervais MENDY, Cheikhane SEYED, Ahmath Bamba MBACKE, *„ WebRTC platform proposition as a support to the educational system of universities in a limited Internet connection context"*, DOI: 978-1-4673-8712-5, ©2015 IEEE

[68] Tobia Castaldi, Lorenzo Miniero, and Simon Pietro Romano, University of Napoli Federico II; *"On the Seamless Interaction between WebRTC Browsers and SIP-Based Conferencing Systems"*, DOI: 0163-6804, © 2013, IEEE IEEE Communications Magazine, April 2013

[69] Marius Corici; Mihai Constantin; Dana Satriya; Dragos Vingarzan; Valentin Vlad; Lukas Wöllner, *« Integrating off-the-shelf 3GPP access networks in the OpenEPC software toolkit: Realizing cost-efficient and complete small-scale operator testbeds* ». IEEE Globecom Workshops, 3-7 Dec. 2012, Page s : 1724 Ŕ 1729, IEEE, 2012. DOI : 10.1109/GLOCOMW.2012.6477845

[70] Mohammad Abu-Lebdeh; Fatna Belqasmi; Roch Glitho, « *A 3GPP 4G Evolved Packet Core-based system architecture for QoS-enabled mobile video surveillance applications* ». Third International Conference on The Network of the Future (NOF), 21-23 Nov. 2012, Page s : 1 Ŕ 6, IEEE 2012. DOI : 10.1109/NOF.2012.6464000

[71] Mohammad Abu-Lebdeh; Fatna Belqasmi; Roch Glitho, « *An Architecture for QoS-Enabled Mobile Video Surveillance Applications in a 4G EPC and M2M Environment* ». IEEE Access, 21 July 2016. Page s: 4082 Ŕ 4093, IEEE 2016, Volume: 4. DOI: 10.1109/ACCESS.2016.2592919

[72] Valeriu Manuel Ionescu, « *The analysis of the performance of RabbitMQ and ActiveMQ* ». 14th RoEduNet International Conference - Networking in Education and Research (RoEduNet NER), 24-26 Sept. 2015, Page s : 132 Ŕ 137, IEEE 2015. DOI : 10.1109/RoEduNet.2015.7311982

[73] Xian Jun Hong; Hyun Sik Yan; Young Han Kim, « *Performance Analysis of RESTful API and RabbitMQ for Microservice Web Application* ». International Conference on Information and Communication Technology Convergence (ICTC), 17-19 Oct. 2018, Page s : 257 Ŕ 259, IEEE 2018. DOI : 10.1109/ICTC.2018.8539409

[74] Konstantinos Vandikas; Vlasios Tsiatsis, « *Performance Evaluation of an IoT Platform* ». Eighth International Conference on Next Generation Mobile Apps, Services and Technologies, 10-12 Sept. 2014, Page s : 141 Ŕ 146, IEEE 2014. DOI : 10.1109/NGMAST.2014.66

[75] Maciej Rostanski; Krzysztof Grochla; Aleksander Seman, « *Evaluation of highly available and fault-tolerant middleware clustered architectures using RabbitMQ* ». Federated Conference on Computer Science and Information Systems, 7-10 Sept. 2014, Page s : 879 Ŕ 884, IEEE 2014. DOI : 10.15439/2014F48

[76] M. Dinker, P. Breult et G.Sevestre. Aspects Modernes de Fiabilité. Les presses de lřUniversité de Montreal édition, 1974.

[77] A. Archip, N. Botezatu, E. Şerban, P. C. Herghelegiu and A. Zală, "*An IoT based system for remote patient monitoring*," 2016 17th International Carpathian Control Conference (ICCC), Tatranska Lomnica, 2016, pp. 1-6

[78] S. H. Almotiri, M. A. Khan and M. A. Alghamdi, "*Mobile Health (m-Health) System in the Context of IoT*," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, 2016, pp. 39-42

[79] M. A. Al-Taee, W. Al-Nuaimy, A. Al-Ataby, Z. J. Muhsin and S. N. Abood, "*Mobile health platform for diabetes management based on the Internet-of-Things,*" 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), Amman, 2015, pp. 1-5.

[80] ADIE, [online] Available : https://www.adie.sn/fr/notre-histoire

[81] L'hypertension, [online]
Available http://aps.sn/actualites/societe/sante/article/hypertension-un-specialiste-evoque-un-taux-de-prevalence-de-24

[82] Gerard J. Tortora, Bryan H. Derrickson, Ř*Principales of Anatomy and Physiology*ř, Wiley, 2014

[83] M. U. H. A. Rasyid, A. A. Pranata, B. H. Lee, F. A. Saputra and A. Sudarsono, "*Portable electrocardiogram sensor monitoring system based on Body Area Network*," 2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Nantou, 2016, pp.1-2.

[84] Yun-Hong Noh ; Jiunn Huei Yap ; and Do-Un Jeong, Implementation of the Abnormal ECG Monitoring System Using Heartbeat Check Map Technique. In the proceedings of International Conference on IT Convergence and Security, December 16-18, 2013.

[85] N. M. Zainee, and K. Chellappan, Ę*Emergency Clinic MultiSensor Continuous Monitoring Prototype Using e-Health Platform*,ę IEEE Conference on Biomedical Engineering and Sciences (IECBES),2014

[86] Kéba GUEYE, Ngartabé KAG-TEUBE, Samuel OUYA, Davy Edgard MOUSSAVOU, « *Proposal for a universal access solution to care in rural areas: case of Sénégal* », 20th International Conference on Advanced Communication Technology (ICACT), 11-14 Feb. 2018, Page s: 643 Ŕ646. IEEE, 2018 **DOI :** 10.23919/ICACT.2018.8323866

[87] COOKING HACKS : *e-Health Sensor Platform V2.0 for Arduino and Raspberry Pi [Biometric / Medical Applications]*, [online], 2015, Available : https://www.cooking-hacks.com/documentation/tutorials/ehealth-biometric-sensor-platform-arduino-raspberry-pi-medical

[88] Eben Upton, Gareth Halfacree, Ř*Raspberry Pi User Guide*ř, Wiley, 2014

[89] Sayed Mohsin Reza, Md. Mahfujur Rahman, Md. Hasnat Parvez, Shamim Al Mamun, M. Shamim Kaiser, Innovative Approach in Web Application Effort & Cost Estimation using

Functional Measurement Type. International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), May 2015.

[90] F. Abtahi, B. Aslamy, I. Boujabir1, F. Seoane, and K. Lindecrantz, An Affordable ECG and Respiration Monitoring System Based on Raspberry PI and ADAS1000 : First Step towards Homecare Applications. 16th Nordic-Baltic Conference on Biomedical Engineering, IFMBE Proceedings 48, DOI : 10.1007/978-3-319-12967-9 2.

[91] K. Siau, Health Care Informatics. IEEE Transactions on Information Technology in Biomedicine, vol. 7, March, 2003.

[92] Kéba GUEYE, Bessan M. DEGBOE, Samuel OUYA, Ngartabé KAG-TEUBE, « *Proposition of Health Care System Driven by IoT and KMS for Remote Monitoring of Patients in Rural Areas : Pediatric Case* », 21th International Conference on Advanced Communication Technology (ICACT), 17-20 Feb. 2019, Page s: 676 Ŕ 680. IEEE, 2019 DOI : 10.23919/ICACT.2019.8702009

[93] *le prix du meilleur de l¨article*, [Online]. Available : http://www.esp.sn, 2019

[94] Farhan Siddiqui, Sherali Zeadally, Thabet Kacem and Scott Fowler, Zero Configuration Networking: Implementation, performance, and security, 2012, Computers & electrical engineering, (38), 5, 1129-1145.

[95] Aidan Williams, Ŗ*Requirements for Automatic Configuration of IP Hosts*ŗ, Internet Draft, September 2002 available at http://files.zeroconf.org/draft-ietf-zeroconf-reqts-12.txt

[96] Ping Dong, Hongke Zhang, Hongbin Luo, Ting-Yun Chi, Sy-Yen Kuo, ŖA network-based mobility management scheme for future Internetŗ, Computers & Electrical Engineering, Volume 36, Issue 2, March 2010, Pages 291-302.

[97] Dittrich, A. ; Salfner, F., Ŗ*Experimental responsiveness evaluation of decentralized service discovery*ŗ, IEEE International Symposium on Parallel and Distributed Processing, 2010, Pages 1 Ŕ 7.

[98] E. Guttman, Ŗ*Autoconfiguration for IP Networking*,ŗ June 2001, available at http://www.Zeroconf.org/w3onwire-Zeroconf.pdf

[99] Stuart Cheshire, "*Dynamic Configuration of IPv4 link-local addresses*", draft-ietf-zeroconf-ipv4-linklocal-
00.txt, 2005.

[100] Mono.Zeroconf Home Page available at http://www.mono-project.com/Mono.Zeroconf

[101] J.P ARCHIER, « Les VPN, fonctionnement et mise en oeuvre », éditions eni, 2011

[102] The Internet Society, ŖSIP : Protocole dřinitialisation de sessionŗ,abcdrfc.free.fr/rfc-vf/pdf/rfc3261.pdf, 2006, consulté septembre 2018

Annexes

A.1. Normes et standards de l'IMS

Référence	Objet
3GPP TS 22.173	IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services; Stage 1
3GPP TS 22.340	IP Multimedia System (IMS) messaging; Stage 1
3GPP TS 23.002	Network architecture
3GPP TS 23.008	Organization of subscriber data
3GPP TS 23.060	General Packet Radio Service (GPRS) ; Service description
3GPP TS 23.141	Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 2
3GPP TS 23.228	IP multimedia subsystem
3GPP TS 24.141	Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3
3GPP TS 24.228	Signalling flows for the IP multimedia call control based on SIP and SDP - -
3GPP TS 24.229	IP Multimedia Call Control Protocol based on SIP and SDP
3GPP TS 24.238	Session Initiation Protocol (SIP) based user configuration - -
3GPP TS 24.247	Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem ; Stage 3
3GPP TS 24.604	Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem ; Protocol specification
3GPP TS 24.607	Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem
3GPP TS 24.608	Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem
3GPP TS 24.610	Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem ; Protocol specification
3GPP TS 24.623	Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services - -
3GPP TS 24.628	Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem ; Protocol specification
3GPP TS 29.162	Interworking between the IM CN subsystem and IP networks
3GPP TS 32.240	Charging management ; Charging architecture and principles
3GPP TS 32.260	Charging management ; IP Multimedia Subsystem (IMS) charging
IETF RFC 3261	SIP : Session Initiation Protocol
IETF RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
IETF RFC 3265	Session Initiation Protocol (SIP) ŔSpecific Event Notification
IETF RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method
IETF RFC 3312	Integration of resources management and SIP
IETF RFC 3313	Private SIP Extensions for Media Authorization
IETF RFC 3319	DHCPv6 Options for SIP Servers
IETF RFC 3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)
IETF RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks
IETF RFC 3428	Session Initiation Protocol (SIP) Extension for Instant Messaging

IETF RFC 3455	Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
IETF RFC 3680	A Session Initiation Protocol (SIP) Event Package for Registrations
IETF RFC 3863	Presence Information Data Format (PIDF)
IETF RFC 4566	SDP : Session Description Protocol
IETF RFC 4916	Connected Identity in the Session Initiation Protocol (SIP)
IETF RFC 5365	Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP)

Tableau 1 - Normes et standards de l'IMS [3GPP, 2011]

A.2. Codes d'état et motifs du protocole SIP

Réponses informatives (Codes 1xx)

Code d'état	Motif	Explication
100	Trying	Tentative en cours
180	Ringing	Sonnerie
181	Call Is Being Forwarded Ŕ	Transfert d‟appel
182	Queued	File d‟attente
183	Session Progress Ŕ	Progrès de session

Tableau 2 – SIP, Codes 1xx - Réponses informatives [101]

Réponses réussies (Codes 2xx)

Code d'état	Motif	Explication
200	OK	
202	Accepted : Used for referrals	Accepté : utilisé pour orientation

Tableau 3 – SIP, Codes 2xx - Réponses réussies [101]

Réponses de redirection (Codes 3xx)

Code d'état	Motif	Explication
300	Multiple Choices	Choix multiples
301	Moved Permanently	Déplacé
302	Moved Temporarily	Temporairement déplacé
305	Use Proxy	Utilisation par proxy
380	Alternative Service	Service alternatif

Tableau 4 – SIP, Codes 3xx - Réponses de redirection [101]

Erreurs du client (Codes 4xx)

Code d'état	Motif	Explication
400	Bad Request	Requête erronée
401	Unauthorized	Refusé : seulement utilisé par les registrars. Les proxies doivent employer l‟autorisation par proxy
402	Payment Required (Reserved for future use)	Paiement nécessaire (Réservé pour utilisation ultérieure)
403	Forbidden	Interdit
404	Not Found	Introuvable : utilisateur non localisé
405	Method Not Allowed	Méthode non autorisée
406	Not Acceptable	Requête non acceptable
407	Proxy Authentication Required	Authentification proxy nécessaire
408	Request Timeout	Délai de demande écoulé : utilisateur non trouvé dans le temps accordé
410	Gone	Désinscrit : lřutilisateur a existé mais n‟est désormais plus disponible
413	Request Entity Too Large	Requête trop large
414	Request-URI Too Long	Requête URI trop longue
415	Unsupported Media Type	Type de media non compatible
416	Unsupported URI Scheme	Schéma URI non compatible
420	Bad Extension	Extension erronée : lřextension nřexiste pas, le serveur ne comprend pas la requête
421	Extension Required	Extension nécessaire
423	Interval Too Brief	Intervalle trop court
480	Temporarily Unavailable	Momentanément non disponible
481	Call/Transaction Does Not Exist	Appel/transaction nřexiste pas
482	Loop Detected	Boucle détectée
483	Too Many Hops	Trop de bonds
484	Address Incomplete	Adresse incomplète
485	Ambiguous	Ambiguë
486	Busy Here	Occupé
487	Request Terminated	Requête avortée
488	Not Acceptable Here	Nřest pas acceptable ici
491	Request Pending	Requête en attente
493	Undecipherable	Indéchiffrable : ne peut pas décrypter le corps S/MIME

Tableau 5 – SIP, Codes 4xx - Erreurs du client [101]

Erreurs du serveur (Codes 5xx)

Code d'état	Motif	Explication
500	Server Internal Error	Erreur interne de serveur
501	Not Implemented	La méthode de requête SIP nřest pas implémentée ici
502	Bad Gateway	Mauvaise passerelle
503	Service Unavailable	Service non disponible
504	Server Time-out	Délai dřattente de serveur
505	Version Not Supported	Le serveur nřest pas compatible avec la version du protocole SIP
513	Message Too Large	Message trop large

Tableau 6 – SIP, Codes 5xx - Erreurs du serveur [101]

Erreurs générales (Codes 6xx)

Code d'état	Motif	Explication
600	Busy Everywhere	Occupé
603	Decline	Refusé
604	Does Not Exist Anywhere	N‟existe pas
606	Not Acceptable	Non acceptable

Tableau 7 - SIP, Codes 6xx - Erreurs générales [101]