TABLE DE MATIERES

NOTATIONS

3G	3ème Génération
3GPP	Third Generation Partnership Project
3GPP2	Second Generation Partnership Project
ADSL	Asymetric Digital Subscriber Line
API	Application Programming Interface
ARIB/TTC	Association for Radio Industries and Business/Telecommunication Technology Comittee
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
ARPANET	ARPA Network
AS	Application Server
ATM	Asynchronous Transfer Mode
AuC	Authentification Center
BRAN	Broadband Radio Access Network
CAMEL	Customized Application for Mobile Network Enhanced Logic
CC	Call Control
CDMA	Code Division Multiple Access
CDR	Call Detailed Records
COPS	Common Open Policy Service Protocol
CRNC	Controlling RNC
CS	Circuit Switched
CSCF	Call State Control Function
CWTS	China Wireless Telecommunication Standard Group
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DRNC	Drift RNC
DSL	Digital Subscriber Line
EDGE	Enhanced Data rate for GSM Evolution
EGP	Exterior Gateway Protocol

EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile service Switching Center
GPRS	Global Packet Radio System
GPS	Global Positioning System
GSM	Global System for Mobile communications
GUI	Graphic User Interface
HDLC	High level Data Link Protocol
HLEN	IP Header Length
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
HSS	Home Subscriber Server
HTTP	Hypertext Transfert Protocol
IANA	Internet Assigned Number Authority
I-CSCF	Interrogating CSCF
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IMEI	Internal Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	Intenational Mobile subscriber Identity
IMS-MGW	IMS Media Gateway
IM-SSF	IP Multimedia Service Switching Function
IMT	International Mobile Telecommunications
INAP	Intelligent Network Application Part
IP	Internet Protocol
IP MS	IP Media Server
ISC	IMS Service Control
ISDN	Integrated Switched Digital Network

ISO	International Organization Standardization
ISUP	ISDN User Part
JDBC	Java DataBase Connectivity
JSP	Java Server Page
LA	Location Area
LET	Longueur de l'En-Tête
MAC	Media Access Control
ME	Mobile Equipment
MEGACO	Media Gateway Control
MGC	Media Gateway Controller
MGCF	MGC Function
MGW	Media Gateway
MMS	Multimedia Message Service
MPLS	MultiProtocol Label Switching
MRF	Multimedia Resource Function
MRFC	MRF Controller
MRFP	MRF Processor
MSC	Mobile service Switching Center
MSISDN	Mobile Station ISDN Number
MT	Mobile Termination
NCP	Network Control Protocol
NFS	Network File System
NGN	Next Generation Network
OSA	Open Service Architecture
OSA SCS	OSA Service Capability Server
OSI	Open System Interconection
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
P-CSCF	Proxy CSCF
PDF	Police Decision Functions
PDU	Protocol Data Unit

PoC	Push to talk over Cellular
PS	Packet Switched
P-TMSI	Packet TMSI
PTT	Push To Talk
QoS	Quality of Service
RA	Routing Area
RARP	Reverse Address Resolution Protocol
RFC	Request For Comments
RIP	Routing Information Protocol
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
RRCF	RRC Function
RSVP	Reservation Protocol
RTC	Réseau Téléphonique Commuté
RTCP	Real time Transport Control Protocol
RTCP/RNIS	Réseau Téléphonique Commuté Public/Réseau Numérique à Intégration de Services
RTP	Real time Transport Protocol
S-CSCF	Serving CSCF
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SGBD	Système de Gestion de Base de Données
SGSN	Serving GPRS Support Node
SIGTRAN	Signalling Transport
SIM	Subscribe Identification Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRAN	Satellite Radio Access Network

SRF	Specialized Resource Function
SRNC	Serving RNC
SS7	Signaling System number 7
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TE	Terminal Equipment
TISPAN	Telephony and Internet converged Services and Protocols for Advanced Networking
TMSI	Temporary MS Identity
T-PDU	Transport PDU
T-SGW	Trunking Signaling Gateway
TTA	Telecommunications Technology Association
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment
UICC	UMTS Integrated Circuit Card
UIT-T	Union Internationale des Télécommunications - Télécommunications
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
WCDMA	Wideband Code Division Multiple Access
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WWW	World Wide Web
xDSL	x Digital Subscriber Line

INTRODUCTION GENERALE

Dans cette nouvelle ère de technologie de plus en plus sophistiquée et la course vers la miniaturisation, la télécommunication se situe au cœur même de ces évolutions. Cette évolution des télécommunications est de plus en plus liée à l'informatique.

Actuellement les réseaux innervent complètement la planète et grâce aux évolutions d'équipements de communication, il est permis d'atteindre de hauts débits. Parmi ces réseaux figurent les réseaux cellulaires tels le GSM qui est une grande évolution dans le domaine de la télécommunication ces dernières années, l'UMTS qui est une évolution du réseau de deuxième génération qu'est le GSM, et depuis quelques temps le réseau de nouvelle génération ou NGN (Next Generation Network) qui a permis de définir l'IMS (IP Multimedia Subsystem) et de l'intégrer dans le réseau UMTS afin de faciliter la convergence de ce réseau vers un réseau « Tout IP ».

Ces évolutions résultent surtout des demandes accrues de services venant des utilisateurs et des entreprises qui nécessitent un système beaucoup plus performant en termes de débit et de bande passante d'une part, et les problèmes liés à l'incapacité des systèmes précédents de satisfaire ces demandes d'autre part. Les services demandés par les utilisateurs convergent surtout vers des services nécessitant des débits élevés notamment le multimédia, etc.

Le monde de la télécommunication doit alors lever de nouveaux défis : l'infrastructure et les technologies conçues pour porter exclusivement la téléphonie doivent s'orienter surtout sur les services et le multimédia.

L'Internet qui est le réseau opérant sous IP (Internet Protocol), reste le modèle le plus intéressant et possédant encore un domaine très large pour des recherches pouvant satisfaire les demandes, de plus en plus exigeantes des clients, qui vont de paire avec la concurrence au sein des opérateurs de télécommunications.

Ce présent mémoire présente, d'un point de vue système, l'architecture, les techniques mises en œuvre et les services proposés par le réseau cellulaire UMTS intégrant un sous système multimédia ou IMS pour permettre une évolution vers le « Tout IP » ainsi que la mise en œuvre de nouveaux services plus attractifs et facilitant la vie de l'homme et des entreprises.

Dans ce travail, nous allons voir en premier lieu une présentation du protocole IP (Internet Protocol) qui est le protocole largement utilisé dans les réseaux « Tout IP ». Nous allons y résumer son historique et sa description. Par la suite, nous allons développer le réseau de troisième

génération, en l'occurrence l'UMTS pour avoir une vue globale sur les techniques et architectures qu'il utilise et les services qu'il propose. Ultérieurement, nous allons présenter en profondeur ce que l'on entend par IMS en développant ses principes, son architecture et les protocoles qu'il utilise. Et enfin, on présentera la simulation d'une application se basant sur les principes de l'IMS.

CHAPITRE 1. LE PROTOCOLE INTERNET (IP)

1.1. Historique : [1] [2] [3] [4]

Les travaux de l'ARPA (Advanced Research Project Agency) débutèrent au milieu des années 70 dans le but de développer un réseau à commutation de paquet afin d'échanger plus facilement courriers et données entre les différents centres. Le but étant de construire un réseau résistant à d'éventuelles attaques militaires ou à des catastrophes naturelles ; il ne fallait pas de points dont la neutralisation pouvait entraîner l'arrêt complet du réseau.

C'est ainsi que le réseau ARPANET fut conçu sans nœud particulier le contrôlant de telle sorte que si une voie de communication venait à être détruite, le réseau est capable de déterminer un nouveau chemin d'acheminement des données.

En 1974, TCP est créé afin d'améliorer et de standardiser le mode de connexion entre machines hétérogènes.

En 1978, TCP est fragmenté en TCP/IP, et c'est vers 1980 que le réseau Internet est apparu. A ce moment là, l'ARPA commença à faire évoluer les ordinateurs en utilisant des protocoles de communication plus élaborés tels que TCP/IP.

Vers 1989 est créé par Tim Bernes-Lee le WWW (World Wide Web), mais c'est seulement vers le milieu des années 90 qu'il est exploité pour le commerce électronique.

IP est l'acronyme de « Internet Protocol », il est standardisé dans la RFC 791 et a été conçu en 1981 pour remplacer NCP (Network Control Protocol), le protocole de l'ARPANET.

Plus de vingt ans après sa première implémentation, ses limitations se font de plus en plus pénalisantes pour les nouveaux usagers sur les réseaux. Avant de le jeter aux sorties, posons-nous la question de qui pouvait prévoir à cette époque où moins de mille ordinateurs étaient reliés ensembles, que deux décennies plus tard des dizaines de millions d'hôtes l'utiliseraient comme principal protocole de communication ?

Sa longévité est donc remarquable et il convient de l'analyser de près avant de pouvoir le critiquer de manière constructive.

1.2. Description du protocole IP : [1] [2] [3] [4] [6] [7]

Comme son nom l'indique (Internet Protocol), le protocole IP a pour rôle de router le trafic à travers un ensemble de réseaux interconnectés. Ceci est réalisé en transférant les datagrammes d'un module Internet à l'autre jusqu'à atteindre la destination. Il a été conçu pour réaliser l'interconnexion de réseaux informatiques et permettre ainsi les communications entre systèmes.

Le protocole IP multiplexe les protocoles de la couche transport et a la faculté de détruire les paquets ayant transités trop longtemps sur le réseau. Il permet également de fragmenter et de rassembler de nouveau les fragments de données. Cependant, il n'effectue ni contrôle d'erreur, ni contrôle de flux.

Un des plus importants mécanismes du protocole Internet est la gestion de cette adresse Internet.

Lors de l'acheminement d'un datagramme d'un module Internet vers un autre, les datagrammes peuvent avoir éventuellement à traverser une section de réseau qui admet une taille maximale de paquet inférieure à celle du datagramme. Pour surmonter ce problème, un mécanisme de fragmentation est géré par le protocole Internet.

Remarque : Dans le modèle OSI, nous parlons plutôt de paquets au niveau de la couche réseau. En revanche, dans le modèle TCP/IP, l'unité transférée est le datagramme. Toutefois, dans la suite de l'ouvrage, nous les mentionnerons indifféremment.

1.3. Principe de l'adressage des machines : [1] [2] [3] [4] [6] [7] [8]

Une distinction doit être faite entre nom, adresse, et chemin. Un nom indique ce que nous cherchons. Une adresse indique où cela se trouve. Un chemin indique comment y aboutir. Le protocole Internet s'occupe essentiellement des adresses. C'est à des protocoles de niveau plus élevé (exemple : hôte-vers-hôte ou application) que revient la tâche de lier des noms à des adresses. Le module Internet déduit de l'adresse Internet une adresse réseau local. La tâche qui consiste à transcrire l'adresse de réseau local en termes de chemin (exemple : sur un réseau local ou dans un routeur) revient au protocole de bas niveau.

1.3.1. Structure d'adresses IP :

Chaque machine d'Internet possède une adresse IPv4 représenter sur un entier de 4 octets (32 bits) notés de façon décimale de 0 à 255, ce qui lui permet d'être identifiée de manière unique dans le réseau. Une adresse est constituée de deux parties : un identificateur de réseau (netid) et un identificateur de machine pour ce réseau (hostid), {netid, hostid}. Elle commence toujours par le numéro ou l'identificateur de réseau, suivi de l'identificateur de machine. Pour assurer l'unicité des numéros de réseau, les adresses Internet sont attribuées par un organisme central, l'InterNIC.

Lorsque l'on veut établir une communication, il est intuitivement indispensable de posséder trois informations :

- Le nom de la machine distante,
- Son adresse,

- La route à suivre pour y parvenir.

Le nom dit « qui » est l'hôte distant, l'adresse nous dit « où » il se trouve et la route « comment » on y parvient.

En règle générale les utilisateurs préfèrent des noms symboliques pour identifier les machines tandis que les processeurs des machines sont plus à l'aise avec les nombres.

Cet adressage n'est pas hiérarchisé dans le sens que 193.50.126.0 pourrait être un réseau japonais, alors que 193.50.125.0 serait un réseau français. C'est la très grosse faiblesse de cet adressage. Le successeur (IPv6) prévoit des hiérarchies d'adresses à la manière du téléphone.

Etant donné que la saturation d'adressage ne semble pas encore être un problème majeur, IPv4 reste largement le plus utilisé malgré l'existence de la nouvelle génération du protocole IP : IPv6.

IPv6 utilise un adressage utilisant huit groupes de quatre lettres hexadécimales séparés par « : ».

Les enjeux majeurs de l'IPv6, outre l'extension de l'espace d'adressage sont : un traitement plus rapide grâce à un en-tête plus simplifié, la sécurité, la notion de flux (qualité de service, etc).

1.3.2. Les classes d'adresses IP :

L'adresse réseau est placée sur les bits de poids forts, alors que l'adresse machine est calculée sur les bits de poids faibles. Pour des raisons administratives et de routage, on regroupe ces adresses sous forme de classes. On pourra ensuite utiliser ces adresses à sa guise pour gérer son réseau. Il existe plusieurs classes d'adresses. On parle des classes A, B, C, D et E. Elles sont différenciées par les bits de poids forts qui les composent.

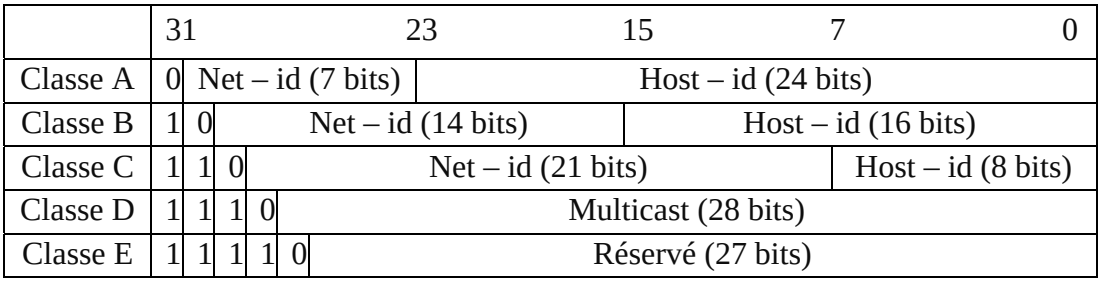

Figure 1.01 : Classes d'adresses IP

D'après cette figure, nous pourrons tirer les nombres de réseau et de nœuds (machines) possibles. Les tableaux suivants résument ces nombres de réseau et de nœuds :

Classe d'adresse IP	Nombre de réseaux	Nombre de nœuds (machines)
A	127	16.777.214
B	16.383	65.534
C	2.097.151	254

Tableau1.01 : Nombre de réseaux et nombres de nœuds pour les classes A, B et C

Classe d’adresse IP	Minimum	Maximum
A	0	126
B	128	191
C	192	223
D	224	239
E	240	247

Tableau 1.02 : Les numéros d’adressage de réseau possibles pour chaque classe d'adresse

Une adresse IP est toujours de la forme X1.X2.X3.X4 (les Xi sont des blocs de 8 bits). La spécification du netid dépend de la classe. Dans le cas d’une classe A, la valeur de X1 permet de reconnaître le réseau ; les X2, X3, X4 permettent de constituer des adresses individuelles. On pourra donc adresser théoriquement 16 777 214 machines. Dans le cas d’une classe B, il est spécifié par X1 et X2. On pourra alors adresser 65 534 machines. Une classe C fixe les valeurs de X1, X2, X3 pour le netid. On pourra donc adresser 254 machines. La classe D est une classe quelque peu différente, puisqu’elle est réservée à une utilisation particulière : le multicast. La classe E est quant à elle une classe non utilisée à ce jour.

Le multicast ou multi diffusion est une technique utilisée par les protocoles spéciaux pour transmettre simultanément des messages à un groupe donné de nœuds différents.

Remarque : Il y a des adresses spéciales que le public ne peut pas utiliser comme adresse d’identification :

- Adresse machine locale, {0, hostid} : adresse IP dont le champ réseau (netid) ne contient que des zéros ;
- Adresse réseau, {netid, 0} : adresse IP dont la partie identificateur de machine (hostid) ne comprend que des zéros. La valeur zéro ne peut être attribuée à une machine réelle.
- Adresse de bouclage, {127, <quelconque>} : adresse IP dont le numéro du champ réseau (netid) est 127. Tout paquet envoyé par une application TCP/IP à une adresse de bouclage sera renvoyé à l’application sans que le paquet n’atteigne le support réseau.

L’I.A.N.A a réservé les trois blocs d’adresses IP suivants pour l’adressage des réseaux privés :

- 1 adresse de classe A : 10.0.0.0 – 10.255.255.255
- 16 adresses de classe B : 172.16.0.0 – 172.31.255.255
- 255 adresses de classe C : 192.168.0.0 – 192.168.255.255

1.4. Datagrammes IP : [1] [2] [4] [6] [7] [8]

1.4.1. Format des datagrammes IP :

Les données qui franchissent la couche IP, alias couche Internet, sont appelées « datagrammes IP », datagrammes Internet ou datagramme tout court.

<table>
<tr><td colspan="8">31 24 19 16 8 4 0</td></tr>
<tr><td colspan="2">Version</td><td>HLEN</td><td colspan="2">Type de Service</td><td colspan="3">Longueur totale</td></tr>
<tr><td colspan="5">Identification</td><td>Indicateurs</td><td colspan="2">Décalage de fragment</td></tr>
<tr><td colspan="3">Durée de vie</td><td colspan="2">Protocole</td><td colspan="3">Somme de contrôle d’en-tête</td></tr>
<tr><td colspan="8">Adresse IP source</td></tr>
<tr><td colspan="8">Adresse IP destination</td></tr>
<tr><td colspan="6">Option IP (s’il y a lieu)</td><td colspan="2">Remplissage</td></tr>
<tr><td colspan="8">Données</td></tr>
</table>

Figure 1.02 : Format des datagrammes IP

Version : 4 bits

Le champ Version indique la version de protocole utilisée.

HLEN (IP header length ou LET-Longueur de l’en-tête IP) : 4 bits

Le champ longueur de l’en-tête (LET) indique la longueur de l’en-tête du datagramme en mots de 32 bits. Il faut noter que ce champ ne peut prendre une valeur en dessous de 5 pour être valide.

Type de Service : 8 bits

Le champ Type de Service indique l’importance qui lui a été accordée par un protocole de couche supérieure donné. Il indique au dispositif chargé de l’acheminement des datagrammes, le routeur, l’attitude à avoir vis-à-vis des datagrammes. Les bits de ce champ sont répartis comme suit :

Bits 0-2 : Priorité.

Bit 3 : 0 = Retard standard,

1 = Retard faible.

Bits 4 :0 = Débit standard,

1 = Haut débit.

Bits 5 :0 = Taux d'erreur standard

1 = Taux d'erreur faible.

Bit 6-7 : Réservé.

<table>
<tr><td colspan="3">Priorité</td><td>R</td><td>D</td><td>T</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td></td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
</table>

Figure 1.03 : Le champ Type de Service IP

Longueur Totale : 16 bits

Le champ Longueur Totale précise la longueur du datagramme IP en entier y compris en-tête et données, mesurée en octets. Ce champ ne permet de coder qu'une longueur de datagramme d'au plus 65.535 octets étant donné qu'il est codé sur 16 bits.

Identification : 16 bits

Le champ Identification contient un nombre entier qui identifie le datagramme actuel. Il contient une valeur entière utilisée pour identifier les fragments d'un datagramme. Ce champ doit être unique pour chaque nouveau datagramme.

Indicateurs : 3 bits

Un champ de 3 bits dont les 2 bits inférieurs contrôlent la fragmentation : 1 bit précise si le paquet peut être fragmenté et le second indique si le paquet est le dernier fragment d'une série de paquets fragmentés.

Bit 0 : réservé, doit être laissé à zéro

Bit 1: (AF) 0 = Fragmentation possible,

1 = Non fractionnable.

Bit 2: (DF) 0 = Dernier fragment,

1 = Fragment intermédiaire.

0	AF	DF
0	1	2

Figure 1.04 : Champ indicateur

Décalage de Fragment : 13 bits

Ce champ sert à rassembler les fragments du datagramme. Il indique le décalage du premier octet par rapport au datagramme complet. Cette position relative est mesurée en blocs de 8 octets (64 bits). Le décalage du premier fragment vaut zéro.

Durée de vie : 8 bits

C'est un compteur qui décroit graduellement, par décrément, jusqu'à zéro. A ce moment, le datagramme est supprimé, ce qui empêche les paquets d'être continuellement en boucle.

Protocole : 8 bits

Ce champ précise le protocole de niveau supérieur qui recevra les paquets entrants après la fin du traitement IP. Les différentes valeurs admises pour divers protocoles sont listées dans la RFC 1060. Exemples : 17 pour UDP, 6 pour TCP, etc.

Somme de contrôle d'en-tête (Checksum): 16 bits

Ce champ assure l'intégrité de l'en-tête IP. Le Checksum doit être recalculé et vérifié en chaque point du réseau où l'en-tête est réinterprété puisque certains champs de l'en-tête sont modifiés (exemple : durée de vie) pendant leur transit à travers le réseau.

Adresse IP source, 32 bits, indique le nœud émetteur.

Adresse IP destination, 32 bits, indique le nœud récepteur.

Options : variable

Ce champ permet au protocole IP de supporter différentes options, telle la sécurité.

1.4.2. Routage des datagrammes :

Le routage est primordial pour l'interconnexion des réseaux. Le réseau Internet est en fait composé d'une multitude de petits réseaux interconnectés entre eux. Chaque réseau envoie et reçoit des informations par le biais de passerelles.

Chaque réseau connecté comprend au minimum une passerelle. Chaque passerelle est obligatoirement connectée à une autre passerelle, appartenant à un autre réseau. Les passerelles sont généralement des routeurs, appareils dédiés au routage de paquets.

Un routeur est donc nécessaire pour relier deux réseaux entre eux, car il n'est pas concevable de relier tous les réseaux par la liaison Ethernet (ou tout autre technologie adaptée aux réseaux locaux). En effet, si on prend le cas d'un établissement universitaire, il est totalement inconcevable de le relier à un autre site distant de plusieurs kilomètres par une liaison Ethernet. Les limites de transmission physique par liaison Ethernet seraient largement dépassées (distance, données et contraintes techniques, électriques et électroniques), mais aussi à cause du coût que cela engendrerait.

On fait donc appel aux liaisons louées, qui sont fournies par les opérateurs télécoms. Chaque ligne dispose donc de son propre protocole et de son propre débit (exemple : E1 = 2Mbit/s, E3 = 34Mbit/s, etc).

Les routeurs ne décodent pas les trames au-delà de la couche 3 du modèle OSI. Par contre, comme les routeurs retranscrivent les trames d'un protocole dans un autre, il faut que le logiciel intégré dans le routeur soit capable de router ce protocole.

Si on utilise un protocole non routable (ARP par exemple), le routeur ne fait que transporter le paquet d'un point à un autre, et on parle alors de pontage (ou de proxy). Ainsi, un pont ne fait que transcrire bêtement des trames entre deux réseaux reliés par une interface autre que celle du réseau

local, alors qu'un routeur sera capable d'orienter les paquets selon leur destination. Un pont n'est pas capable d'appréhender un protocole au-delà du niveau 2 du modèle OSI.

Il existe différents niveaux de routeurs, ceux-ci fonctionnent donc avec des protocoles différents :

- Les routeurs noyaux sont les routeurs principaux car ce sont eux qui relient les différents réseaux.
- Les routeurs externes permettent une liaison des réseaux autonomes entre eux. Ils fonctionnent avec un protocole appelé EGP (Exterior Gateway Protocol) qui évolue petit à petit en gardant la même appellation.
- Les routeurs internes permettent le routage des informations à l'intérieur d'un réseau autonome. Ils s'échangent des informations grâce à des protocoles appelés IGP (Interior Gaterway Protocol).

Les routeurs possèdent des tables de routage leur permettant de choisir l'interface de sortie d'un datagramme à partir des informations stockées dans cette dernière. Les routeurs prennent également des décisions en fonction de la densité du trafic et du débit des liaisons (bande passante). La sélection du chemin permet à un routeur d'évaluer les chemins disponibles vers une destination donnée et de définir le meilleur chemin pour traiter un datagramme.

Adresse de destination	Adresse du prochain routeur directement accessible	Interface
194.56.32.124	131.124.51.108	2
53.114.24.239	194.8.212.6	3
187.218.176.54	129.15.64.87	1

Tableau 1.03 : Exemple de table de routage

Il existe plusieurs protocoles de routage comme le RIP (Routing Information Protocol), l'OSPF (Open Shortest Path First), etc. Nous allons voir ces deux protocoles (c'est à dire le RIP et l'OSPF) et comprendre leurs fonctionnements.

1.4.2.1. Le protocole RIP :

Le protocole RIP est apparu avec la version BSD d'Unix, il est documenté dans la RFC 1058 (1988 - Version 1 du protocole) et la RFC 1388 (1993 - Version 2 du protocole). Ce protocole est basé sur des travaux plus anciens menés par la firme Xerox.

Le protocole RIP utilise le concept de « vecteur de distance », qui s'appuie sur un algorithme de calcul du chemin le plus court dans un graphe. Le graphe est celui des routeurs, la longueur du chemin est établie en nombre de sauts (hop), ou métrique, entre la source et la destination, c'est à

dire en comptant toutes les liaisons. Cette distance est exprimée comme un nombre entier variant entre 1 et 15 ; la valeur 16 est considérée comme l'infini et indique une mise à l'écart de la route.
La méthode de routage à vecteur de distance détermine la direction (vecteur) et la distance vers n'importe quel lien de l'inter-réseau. Les algorithmes de routage à vecteur de distance transmettent des copies périodiques d'une table de routage d'un routeur à un autre. Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications topologiques.
Chaque routeur émet dans un datagramme portant une adresse IP de broadcast, à fréquence fixe (environ 30 secondes), le contenu de sa table de routage et écoute celle des autres routeurs pour compléter sa propre table. Ainsi se propagent les tables de routes d'un bout à l'autre du réseau. Pour éviter une « tempête de mises à jour », le délai de 30 secondes est augmenté d'une valeur aléatoire comprise entre 1 et 5 secondes.
Si une route n'est pas annoncée au moins une fois en trois minutes, la distance devient « infinie », et la route sera retirée un peu plus tard de la table (elle est propagée avec cette métrique).
RIP est le protocole le plus fréquemment utilisé pour transférer des informations de routage entre des routeurs situés sur un même réseau.
Le protocole RIP pose un problème lorsque la destination choisie ne peut pas être atteinte parce qu'elle est trop éloignée. Avec le protocole RIP, les données peuvent exécuter 15 sauts au maximum. Par conséquent, il n'est pas possible d'atteindre un réseau de destination à une distance de plus de 15 routeurs.

1.4.2.2. Le protocole OSPF :

Le protocole OSPF a été conçu au sein de l'IETF (Internet Engineering Task Force) à la fin des années 80. Il utilise plusieurs critères pour sélectionner le meilleur chemin vers une destination. Ces critères incluent des métriques de coût qui tiennent compte notamment de la vitesse d'acheminement, du trafic, de la fiabilité et de la sécurité.
Contrairement à RIP, OSPF n'utilise pas de vecteur de distance mais base ses décisions de routage sur le concept d'état des liaisons. Celui-ci permet un usage beaucoup plus fin des performances réelles des réseaux traversés, puisque cette métrique est changeante au cours du temps. Si on ajoute à cela une méthode de propagation très rapide des routes par inondation, sans boucle et la possibilité de chemins multiples, OSPF, bien que beaucoup plus complexe que RIP, ses performances et sa stabilité sont supérieures. Il a toutes les qualités pour remplacer le RIP, même sur les tous petits réseaux. Le protocole OSPF utilise une base de données distribuée qui permet de

garder en mémoire l'état des liaisons. Ces informations forment une description de la topologie du réseau et de l'état de l'infrastructure.

Son avantage majeur réside dans le fait qu'il y a moins d'informations à faire circuler entre les routeurs, le protocole OSPF, n'envoyant pas à ses voisins le nombre de sauts qui les sépare mais l'état de la liaison qui les sépare, ce qui permet d'avoir une meilleure bande passante disponible. Cependant, il est important de noter que des problèmes de performances persistent. L'algorithme utilisé par OSPF pour ses calculs de routes est extrêmement gourmand en ressources processeurs. En effet, plus une zone est importante, plus le nombre de calculs exécutés est conséquent.

Pour éviter ces problèmes de performances, il est conseillé de limiter le nombre de routeurs par zone à 50.

OSPF doit son nom à l'algorithme d'Edsger W. Dijkstra de recherche du chemin le plus court d'abord lors du parcours d'un graphe. Le « Open » vient du fait qu'il s'agit d'un protocole ouvert de l'IETF, c'est à dire qu'il n'a pas de copyright, dans la RFC 2328.

1.5. Résolution d'adresses logiques : [3] [4] [6] [7] [8]

Toute interface du réseau est modélisée par une adresse logique IP. Or, pour la transmission sur l'interface physique, cette information n'est pas accessible à cause de l'encapsulation dans la trame qui contient des adresses matérielles, adresses MAC, qui sont généralement attribuées par les fabricants de la carte réseau et codées en dur sur la carte. Nous devons mettre en place des techniques de correspondance d'adresses vue que nous ne connaissons que l'adresse IP du destinataire. Ces techniques sont modélisées par les protocoles ARP et RARP.

1.5.1. Le protocole ARP :

1.5.1.1. Introduction :

Les adresses IP sont attribuées indépendamment des adresses matérielles des machines. Pour envoyer un datagramme dans l'internet, le logiciel réseau doit convertir l'adresse IP en une adresse physique qui est utilisée pour transmettre la trame. Si l'adresse physique est un entier court, elle peut être facilement modifiée pour lui faire correspondre l'adresse machine IP. Sinon, la traduction doit être effectuée dynamiquement.

C'est le protocole ARP qui effectue cette traduction en s'appuyant sur le réseau physique. ARP permet aux machines de résoudre les adresses sans utiliser de table statique. Une machine utilise ARP pour déterminer l'adresse physique destinataire en diffusant (broadcast), sur le sous réseau, une requête ARP qui contient l'adresse IP à traduire et une adresse matérielle de diffusion, ou

adresse MAC de diffusion, ayant le format FF-FF-FF-FF-FF-FF. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique. Pour rendre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues et réduit ainsi le nombre d'émissions en mode broadcast.

1.5.1.2. Fonctionnement :

Lorsqu'une source détermine l'adresse IP d'une destination, elle consulte sa table ARP pour trouver l'adresse MAC de destination. Si la source trouve une entrée dans sa table (adresse IP de destination correspondant à l'adresse MAC de destination), elle relie l'adresse IP à l'adresse MAC de destination grâce à une requête ARP.

Un hôte souhaitant envoyer des données à un autre hôte, ne connaissant pas l'adresse MAC de destination, lance un requête ARP. Cette requête lui permet de détecter l'adresse MAC de destination.

Comme les paquets des requêtes ARP circulent en mode broadcast, tous les équipements du réseau local reçoivent les paquets et les transmettent à la couche réseau pour qu'ils soient examinés. Seul l'équipement qui a la même adresse IP que dans la requête ARP répond (en mode « unicast ») en envoyant son adresse MAC à l'équipement source.

Lorsque l'équipement source reçoit la réponse ARP, il extrait l'adresse MAC et met à jour sa table ARP. L'équipement source peut ensuite adresser correctement ses données.

1.5.2. Le protocole RARP :

Le protocole RARP (Reverse Address Resolution Protocol) est beaucoup moins utilisé, il signifie Protocole ARP inversé, il s'agit donc d'une sorte d'annuaire inversé des adresses logiques et physiques.

Le protocole RARP permet à une station de connaître son adresse IP à partir d'une table de correspondance entre adresse MAC (adresse physique) et adresses IP hébergées par une passerelle située sur le même réseau local.

Pour communiquer en TCP/IP, une machine a besoin d'au moins une adresse IP, l'idée de ce protocole est de la demander au réseau.

Le protocole RARP est adapté d'ARP : l'émetteur envoie une requête RARP spécifiant son adresse physique dans un datagramme de même format que celui d'ARP et avec une adresse de « broadcast » physique.

Toutes les stations en activité reçoivent la requête, celles qui sont habilitées à répondre (serveurs RARP) complètent le datagramme et le renvoient directement (unicast) à l'émetteur de la requête puisqu'elle connait son adresse physique.
Le protocole RARP est défini dans la RFC 903.

CHAPITRE 2. L'UMTS (Universal Mobile Telecommunication System)

2.1. Présentation de l'UMTS : [9] [10] [11] [12] [15] [18]

Suite à la première génération de téléphonie mobile, utilisant la modulation analogique et la seconde, caractérisée par une modulation numérique et une normalisation internationale mais régionale, les normalisations se sont tournées vers un système unique de troisième génération.

Cette troisième génération, l'UMTS ou Universal Mobile Telecommunication System, est une norme pour la transmission vocale, texte, vidéo ou multimédia numérisée. C'est une évolution décisive par rapport au GSM, mais contrairement à ce dernier, elle est une norme internationale unifiée, basée sur une combinaison de services fixes et mobiles. La téléphonie standard, l'accès à l'internet, la téléphonie vidéo et des services spécialement adaptés tels que les actualités et les informations sur la bourse sont mises à la disposition des utilisateurs sans interruption, où qu'ils soient et lorsqu'ils sont en déplacement.

2.1.1. Définition de l'UMTS (Universal Mobile Telecommunication System) :

2.1.1.1. Définition :

C'est une norme cellulaire numérique pour les systèmes de télécommunications mobiles 3G. Cette norme a été normalisée par le 3GPP (Third Generation Partnership Project).

Cette technologie fait partie de la famille des IMT, appartenant à la norme des technologies dite de 3ème génération. Il est prévu que cette technologie remplace au fur et à mesure le réseau GSM.

La création de nouvelle fréquence est nécessaire à son utilisation. Il permet l'utilisation d'une bande passante beaucoup plus importante de l'ordre de (2Mbit/s théorique, de 300 kbit/s dans la pratique).

De nos jours, le GSM arrive rapidement à saturation et cela pose un problème sur le nombre de clients raccordés sur ce réseau.

La création de bande de fréquences supplémentaires permettrait de rajouter des fréquences favorables à une expansion du réseau, favorable aux opérateurs téléphoniques.

2.1.1.2. Avantages :

Cette technologie possède de nombreux avantages :

- La possibilité d'accroître l'accès à Internet à partir d'un téléphone portable, et d'augmenter la vitesse de transfert.
- La qualité audio est nettement améliorée, et se rapproche de celle du téléphone fixe.
- De nombreuses applications plus performantes voient le jour grâce à cette technologie, laissant passer trois fois plus d informations qu'à la normale.

- Une uniformisation des normes téléphoniques à travers le monde est enfin possible. De nombreux réseaux ne supportant la norme GSM pourront utiliser l'UMTS.
- Le nombre de personnes pouvant être raccordées au réseau se retrouvera accru.
- Le débit offert par l'UMTS est nettement supérieur à ceux du GSM et du GPRS. Ce débit peut atteindre jusqu'à 2Mbit/s en lieu fixe et dans les meilleures conditions, mais pour un terminal en mouvement, on n'a que 384 kbit/s.

2.1.2. Objectifs :

Comme nous l'avons dit plus haut, le premier objectif de l'UMTS est l'unification de l'ensemble des systèmes existants en matière de téléphonie mobile, le problème avec la seconde génération réside dans le fait que dès que l'on change de zone, il y a changement de norme. A cet effet la 3GPP, ou 3rd Generation Partnership Project, qui regroupe l'ETSI (Europe), l'ANSI T-1 (Etats-Unis), l'ARIB/TTC (Japon), la TTA (Corée du Sud) et CWTS (Chine), a standardisé l'UMTS.

Un second objectif serait d'assurer la compatibilité avec les systèmes de seconde génération de part les services offerts à l'usager et aussi la transparence du réseau par ce dernier c'est à dire qu'il ne doit pas se rendre compte qu'il passe d'un réseau à un autre.

Ensuite, ce système de téléphonie mobile a la possibilité de supporter les multimédias. Les terminaux ont la capacité d'accepter simultanément des services de natures différentes : voix, visiophonie, navigation web et transfert de fichiers. Pour ce faire, il est nécessaire d'augmenter les débits supportés par le réseau.

Enfin, l'UMTS propose quatre classes de services en tenant compte de trois contraintes : le délai de transfert, la variation de ce délai et la tolérance aux erreurs de transmission. Nous avons ainsi les classes A (conversational) et B (streaming) pour les applications à contrainte temps réel, puis les classes C (interactive) et D (background) pour les applications de données sensibles aux erreurs de transmission.

- Classe A : représente la téléphonie, la visiophonie et les jeux interactifs. Elle regroupe tous les services bidirectionnels impliquant deux interlocuteurs ou plus.
- Classe B : représente les services vidéo à la demande, la diffusion radiophonique et les applications de transfert d'images. Cette classe implique un utilisateur et un serveur de données. Ces données sont majoritairement distribuées dans le sens serveur utilisateur.
- Classe C : représente la navigation sur internet, le transfert de fichiers par FTP, le transfert de messages électroniques et toutes les applications de commerce électronique. Ces applications ne requièrent aucune performance temps réel particulière.

- Classe D : représente le transfert de fax, la notification de message électronique et la messagerie de type SMS. La différence avec la classe C est que les informations transmises sont de priorités inférieures à celles de la classe C.

2.1.3. Caractéristiques :

Les principales caractéristiques de l'UMTS sont :

- L'assurance en mobilité d'un débit de 144 kbit/s, de préférence 384 kbit/s partout où le service est assuré ;
- L'assurance dans certaines zones d'un débit de 2 Mbit/s ;
- Une haute efficacité spectrale par rapport au système de seconde génération ;
- Une haute flexibilité pour permettre aisément l'introduction de nouveaux services.

Les deux premières caractéristiques sont les conséquences des diverses techniques utilisées par l'UMTS.

En ce qui concerne la haute efficacité spectrale, elle s'obtient par l'utilisation de l'accès multiples, par répartition des codes ou CDMA. C'est une technique qui consiste à redistribuer et étaler le signal sur toute la bande de fréquence et rendre « invisible » idéalement, pour les autres utilisateurs, l'utilisation de la même bande de fréquence. Cela est possible grâce à l'utilisation des codes différents pour chaque utilisateur. Ces codes présentent les propriétés d'auto-corrélation maximale et d'inter-corrélation nulle.

La flexibilité permettant l'introduction de nouveaux services est obtenue par l'intégration d'un système d'exploitation et des applications dans les terminaux UMTS.

En plus de ces quatre caractéristiques citées ci-dessus, il y en a encore d'autres dont voici quelques unes :

- Utilisation de la commutation de paquets à l'intérieur du réseau cœur ;
- Attribution d'adressage IP pour les terminaux (pour la transmission de données) ;
- IPv6 est obligatoire dans la norme UMTS ;
- Les fréquences utilisées par le réseau sont : 1885-1920 MHz pour la voie montante et 2010-2025 MHz pour la voie descendante pour la technologie d'accès UTRA/TDD, 1920-1980 MHz pour la voie montante et 2110-2170 MHz pour la voie descendante pour la technologie d'accès UTRA/FDD ;
- Une carte à puce assure la sécurité du terminal et la confidentialité des communications (utilisation d'un algorithme de cryptage à clé publique).

2.2. Architecture du réseau UMTS : [9] [10] [11] [12] [13] [14] [15] [16] [18]

Un travail considérable de modélisation a permis de définir clairement le système UMTS. Fortement inspiré du GSM, il propose cependant une architecture et un découpage fonctionnel plus ouvert en séparant les fonctions liées à la technologie d'accès de celles qui ne dépendent pas du mode d'accès. Ce concept de séparation de la couche d'accès du reste du réseau accroît l'évolutivité de la norme UMTS. Cela permettra de faire évoluer l'interface radio en minimisant les impacts sur les équipements du réseau.

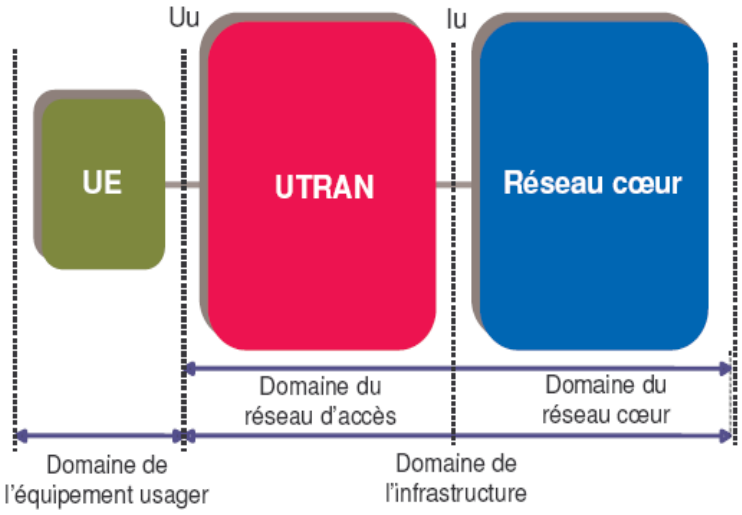

Figure 2.01 : Architecture générale de l'UMTS

2.2.1. Domaine de l'équipement usager :

Le domaine de l'équipement usager UE (User Equipment) comprend l'ensemble des équipements terminaux. Il est constitué d'un ME (Mobile Equipment) et d'un USIM (Universal Subscriber Identity Module).

Le ME (Mobile Equipment) est un terminal radio employé pour la communication radio sur l'interface Uu. Le ME est une partie fonctionnelle de l'UE composée de l'équipement terminal (TE) et de la terminaison mobile (MT).

La MT (Mobile Termination) est une partie de l'UE qui effectue des fonctions spécifiques à la transmission et à la réception sur l'interface radio.

Le TE (Terminal Equipment) est une partie de l'UE où les données de l'application sont générées en émission ou traitées en réception.

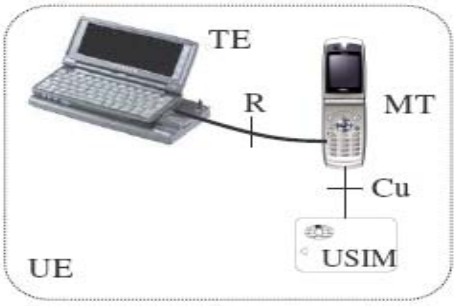

Figure 2.02 : Configuration possible de l'UE

L'USIM est une application contenue dans l'UICC (UMTS Integrated Circuit Card) qui gère les procédures d'authentification et de chiffrement ainsi que les services auxquels l'abonné a souscrit et permet l'accès à ces services par le réseau mobile. Elle peut être utilisée sur un terminal UMTS indépendamment du fabricant, en général de l'opérateur du réseau : la carte associe un abonné à un ou plusieurs fournisseurs de services et pas nécessairement à l'opérateur du réseau courant. L'USIM contient :

- La liste des réseaux interdits
- Les clés de chiffrement et d'intégrité
- IMSI (International Mobile Subscriber Identity)
- MSISDN (Mobile Station International ISDN Number)
- Les identités temporaires de l'usager (TMSI et P-TMSI)
- Les identités des zones de localisation courantes de l'UE, etc.

L'UICC est une carte à puce dotée de caractéristiques électromécaniques standardisées et qui contient une USIM et SIM, ce qui va permettre son utilisation aussi bien dans un réseau UMTS que GSM.

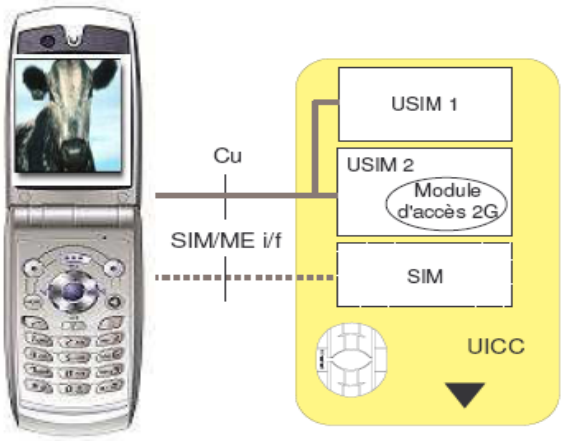

Figure 2.03 : Carte UICC

Comme dans la majorité des systèmes de radiocommunication mobile (en particulier le GSM), un numéro IMSI (International Mobile Subscriber Identity) permet au réseau d'identifier l'abonné de manière unique. Ce numéro n'est pas connu de l'utilisateur. Pour être appelé, celui-ci se voit attribuer un ou plusieurs numéros MSISDN (Mobile Station ISDN Number). Pour préserver la compatibilité avec le réseau GSM, le terminal UMTS doit communiquer l'IMEI (Internal Mobile Equipement Identity) au réseau. Ce paramètre identifie le terminal et peut en cas de fraude être bloqué.

2.2.2. Domaine du réseau cœur et du réseau d'accès :

Le réseau UMTS est composé d'un réseau cœur et d'un réseau d'accès. L'interface entre ces deux réseaux est appelée « Iu ». Cette interface a été définie d'une manière aussi générique que possible afin d'être capable de connecter, en plus de l'UTRAN, des réseaux d'accès de technologies différentes au réseau cœur de l'UMTS. Ainsi pourra se connecter par exemple le SRAN (Satellite Radio Access Network) ou le BRAN (Broadband Radio Access Network), qui est un réseau d'accès large bande utilisant une technologie d'accès de type WLAN (Wireless Local Area Network).

2.2.2.1. Le réseau cœur :

Le réseau cœur de l'UMTS est scindé en 2 domaines de service :

- le CS (*Circuit Switched*) domain,
- le PS (Packet Switched) domain.

Le domaine CS est utilisé pour la téléphonie tandis que le domaine PS permet la commutation de paquets (utilisé pour les données, Internet, etc). Ainsi les téléphones de 3ème génération peuvent gérer simultanément une communication paquet et circuit. Cette notion de domaine permet de modéliser la notion de service dans le réseau cœur et donne la possibilité de créer ultérieurement d'autres domaines de service.

Les éléments du réseau cœur sont répartis en 3 groupes, comme l'illustre la figure ci-dessous. Le domaine CS comprend le MSC, le GMSC et le VLR. Le domaine PS comprend le SGSN et le GGSN. Le dernier groupe comprend les éléments communs aux domaines PS et CS, le HLR, l'EIR, et l'AuC.

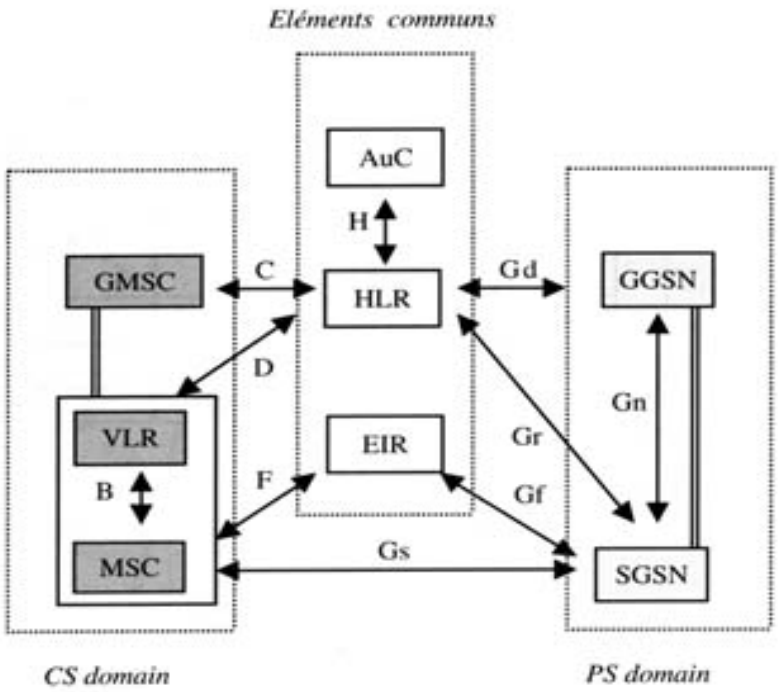

Figure 2.04 : Le réseau cœur de l'UMTS

2.2.2.1.1. Le groupe des éléments communs :

Le **HLR (**Home Location Register**)** est la base de données contenant les informations relatives à l'abonné gérée par l'opérateur. Pour chaque abonné, le HLR mémorise les informations suivantes :

- les informations de souscription (abonnement, souscription à tel service, débit maximal autorisé, etc)
- l'identité du mobile, ou IMSI (International Mobile Sation Identity)
- le numéro d'appel de l'abonné.

L'**AuC (**Authentification Center**)** est un élément permettant au réseau d'assurer certaines fonctions de sécurité, à savoir : l'authentification de l'abonné, le chiffrement de la communication. Ces deux fonctions de sécurité sont activées au début de l'établissement de l'appel avec l'abonné. En cas d'échec d'une d'entre elles, l'appel est rejeté. L'AuC est couplé au HLR et contient pour chaque abonné une clé d'identification lui permettant d'assurer les fonctions d'authentification et de chiffrement.

L'**EIR (**Equipment Identity Register**)** est un équipement optionnel destiné à lutter contre le vol des terminaux mobiles. L'EIR est en fait une base de données contenant la liste des mobiles interdits (black list). L'identification du mobile se fait grâce à son IMEI (International Mobile Station Equipement Identity).

2.2.2.1.2. Le domaine CS :

Le domaine circuit permettra de gérer les services temps réel dédiés aux conversations téléphoniques (vidéo-téléphonie, jeux vidéo, streaming, application multimédia). Ces applications nécessitent un temps de transfert rapide. Lors de l'introduction de l'UMTS, le débit du mode domaine circuit sera de 384kbit/s. L'infrastructure s'appuiera alors sur les principaux éléments du réseau GSM : MSC/VLR (bases de données existantes) et le GMSC afin d'avoir une connexion directe vers le réseau externe.

Le **MSC (**Mobile-services Switching Center**)** est un commutateur de données et de signalisation. Il est chargé de gérer l'établissement de la communication avec le mobile.

Le **GMSC (**Gateway MSC**)** est un MSC un peu particulier servant de passerelle entre le réseau UMTS et le RTCP (Réseau Téléphonique Commuté Public). Lorsqu'on cherche à joindre un mobile depuis un réseau extérieur à l'UMTS, l'appel passe par le GMSC, qui effectue une interrogation du HLR avant de router l'appel vers le MSC dont dépend l'abonné.

Le **VLR (**Visitor Location Register**)** est une base de données attachée à un ou plusieurs MSC. Le VLR est utilisé pour enregistrer les abonnés dans une zone géographique appelée LA (Location Area). Le VLR contient des données assez similaires à celles du HLR. Le VLR mémorise pour chaque abonné plusieurs informations telles que l'identité temporaire du mobile (pour limiter la fraude liée à l'interception et à l'utilisation frauduleuse de l'IMSI) ou la zone de localisation (LA) courante de l'abonné.

2.2.2.1.3. Le domaine PS :

Le domaine paquet permettra de gérer les services non temps réel. Il s'agit principalement de la navigation sur Internet, de la gestion de jeux en réseaux et de l'accès/utilisation des e-mails. Ces applications sont moins sensibles au temps de transfert, c'est la raison pour laquelle les données transiteront en mode paquet. Le débit du domaine paquet sera sept fois plus rapide que le mode circuit, environ 2Mbits/s. L'infrastructure s'appuiera alors sur les principaux éléments du réseau GPRS : SGSN (bases de données existantes en mode paquet GPRS, équivalent des MSC/VLR en réseau GSM) et le GGSN (équivalent du GMSC en réseau GSM) qui jouera le rôle de commutateur vers le réseau Internet et les autres réseaux publics ou privés de transmission de données.

Le **SGSN (**Serving GPRS Support Node**)** joue le même rôle que le VLR, c'est à dire la localisation de l'abonné mais cette fois sur une RA (Routing Area).

Le **GGSN (**Gateway GPRS Support Node**)** a une fonction identique au GMSC pour la partie paquet du réseau, en jouant le rôle de passerelle vers les réseaux à commutation de paquets extérieurs (Internet public, un intranet privé, etc).

2.2.2.2. Le réseau d'accès UTRAN :

Le réseau terrestre d'accès radio de l'UMTS (UTRAN) assure le transport des flux entre le terminal mobile et le réseau cœur. Il est composé d'un ensemble de sous-systèmes du réseau nommé RNS (Radio Network Subsystem). La figure suivante illustre les éléments du réseau d'accès :

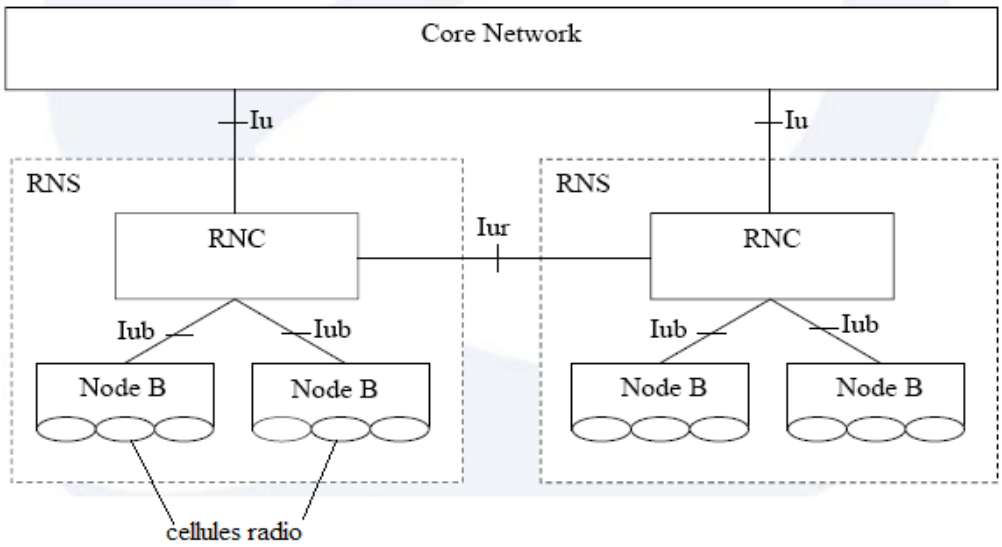

Figure 2.05 : Réseau d'accès UTRAN

2.2.2.2.1. Le NodeB :

Le principal rôle qui lui incombe est d'assurer les fonctions de réception et de transmission radio pour une ou plusieurs cellules de l'UTRAN. Il convertit le flot de données entre l'interface radio (Uu) et l'interface Iub assure les traitements radio au niveau couche physique (contrôle de puissance, etc).

2.2.2.2.2. Le RNC (Radio Network Controller) :

Son rôle capital est le routage des communications entre le NodeB et le réseau cœur. Lorsqu'un mobile est en communication, une connexion RRC (Radio Resource Control) est établie entre le mobile et un RNC de l'UTRAN. Le RNC en charge de cette connexion est appelé serving RNC (SRNC). Lorsque l'usager se déplace dans le réseau, il peut être conduit à changer de cellule en cours de communication, et peut même se retrouver dans une cellule faisant partie d'un NodeB ne dépendant plus de son SRNC. On appelle controlling RNC (CRNC) le RNC en charge des cellules

distantes. D'un point de vue RRC, le RNC distant est appelé drift RNC (DRNC). Les données échangées entre le SRNC et le mobile transitent par les interfaces Iur et Iub. Le DRNC joue donc le rôle de simple routeur vis-à-vis de ces données.

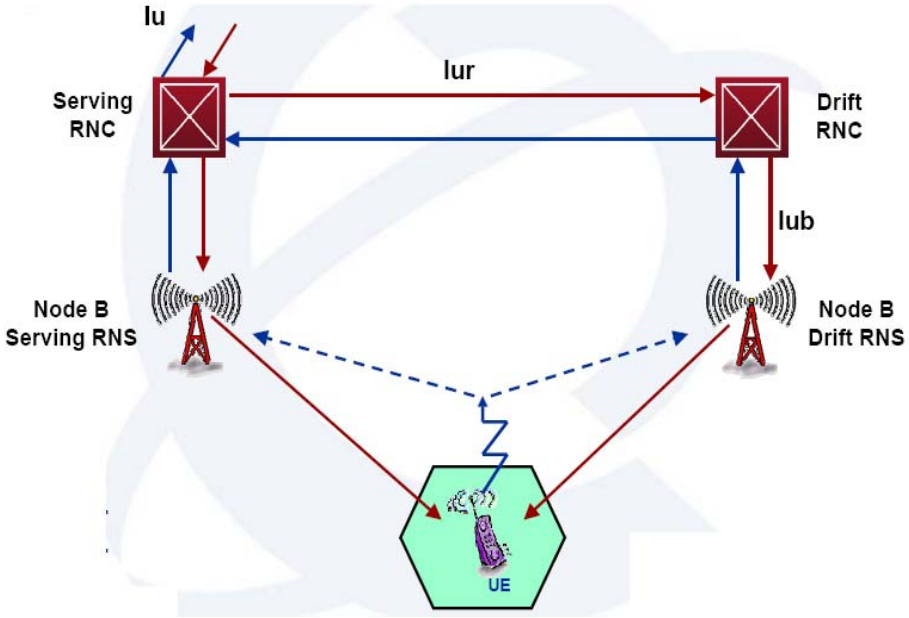

Figure 2.06 : Soft-handover impliquant deux cellules différentes

Le tableau suivant représente les interfaces de l'UTRAN.

Interface	Localisation	Description en bref
Uu	UE-UTRAN	Interface radio qui permet au mobile de communiquer avec l'UTRAN. La technologie UTRA est utilisée dans cette interface.
Iu	UTRAN-réseau cœur	Interface Iu-CS. Elle permet au RNC de communiquer avec le MSC/VLR (services en mode circuit).
		Interface Iu-PS. Elle permet au RNC de communiquer avec le SGSN (services en mode paquet)
Iur	RNC-RNC	Elle permet à deux RNC de communiquer. Nécessaire en CDMA pour effectuer, entre autres, la procédure de macrodiversité.
Iub	NodeB-RNC	C'est par cette interface que communiquent le NodeB et le RNC

Tableau 2.01 : Les interfaces de l'UTRAN

Le réseau UMTS repose donc sur un réseau cœur et un réseau d'accès.

2.3. Les services proposés par l'UMTS : [10] [12] [14] [15] [16] [18]

2.3.1. De la voix toujours avec plus d'appels :

A la différence du système actuel où les communications vocales passent par le réseau GSM et les données par le GPRS, en 3G voix et données, dans une zone couverte, transitent par le même canal.

La base de ces services reste évidemment l'acheminement des appels vocaux. Pourtant, les réseaux UMTS sont capables de supporter des montées en charge bien plus importantes que les réseaux GSM. Les apports de cette technologie se manifestent par une moindre saturation et une meilleure qualité audio.

2.3.2. Les nouveautés :

2.3.2.1. La visiophonie :

Un terminal compatible 3G intégrant une caméra suffit pour communiquer par la voix et l'image avec des correspondants également équipés. Ces téléphones sont dotés d'un bouton spécifique pour les appels en visiophonie, le numéro reste le même que pour une communication classique.

L'écran du mobile diffuse l'image du correspondant, tandis que l'on peut aussi visualiser en incrustant sa propre image.

Il sera également possible de laisser un message vidéo à la personne appelée, en l'enregistrant auprès d'un service dédié, similaire en tout point à la messagerie vocale, ou en envoyant un MMS vidéo.

2.3.2.2. La transmission vidéo en temps réel :

Un débit de transmission de 150 à 300 kbit/s autorise l'usage du streaming, cette technologie de transmission de données en flux continu, sans téléchargement, est déjà couramment utilisée sur Internet pour visionner des vidéos et écouter la radio par exemple. Les opérateurs proposent du contenu vidéo voire l'accès à des chaînes de télévision. A cette exception près, les vidéos sont proposées en exclusivité sous la forme d'émissions quotidiennes de format court (deux à trois minutes maximum).

Elles sont accessibles par le biais du portail multimédia de l'opérateur : actualités, sports, culture, divertissements, infos locales, etc.

2.3.3. Les améliorations :

2.3.3.1. Envoi et réception de SMS et MMS :

Accès aux services multimédias : téléchargement de sonneries, logos, jeux, « chats » et messageries instantanées sur mobile.

Tous ces services, déjà proposés en connexion GPRS, continuent d'être développés sur les portails UMTS des opérateurs. Et qui dit débit plus important, dit confort d'utilisation et rapidité accrus.

2.3.3.2. Accès à l'Internet :

Que ce soit depuis un terminal mobile ou par un ordinateur portable associé une carte PCMCIA 3G ou à un téléphone mobile officiant comme modem, la 3G permet de disposer d'un accès rapide à sa messagerie, au web et à son environnement de travail (intranet, messagerie unifiée, etc), équivalent à un accès de base par l'ADSL ou le câble.

2.3.4. Les services du futur :

Voici un florilège de services qui pourraient émerger à moyen terme sur le téléphone mobile. Ils ne sont pas encore proposés par les opérateurs, car ils supposent une implantation plus mûre du réseau et l'arrivée de terminaux plus sophistiqués (processeurs plus puissants, capacités de mémoire et d'affichages plus importants) :

- écouter de la musique en streaming (la radio par exemple)
- acheter et télécharger de la musique en ligne
- jeux 2D et 3D en réseau
- surveillance vidéo à distance
- la télémédecine
- services d'achats et de paiements par téléphone, porte-monnaie électronique
- commercialisation de bouquets TV similaires à ceux proposés par le câble et le satellite
- navigation routière au GPS (solutions « offboard » avec des services de cartographie externalisés)
- gestion de la maison (commande à distance des lumières, de la télévision, ouverture d'une porte).

Le tableau suivant représente les quatre classes de services de l'UMTS :

Service	Délai	Exemples d'application	Débit	Tolérant à des erreurs
Conversationnel	<< 1 s	Visiophonie	32-384 kbit/s	Oui
		Jeux interactifs	1 kbit/s	Non
Streaming	< 10 s	Audio haute qualité	32-128 kbit/s	Oui
		Images fixes	Non garanti	Non
Interactif	Environ 1 s	Commerce électronique	Non garanti	Non
		Navigation sur Internet	Non garanti	Non
Arrière-plan (background)	> 10 s	Fax	Non garanti	Oui
		E-mail (avec acquittement)	Non garanti	Non

Tableau 2.02 : Les classes de services de l'UMTS

2.4. Le futur de l'UMTS : [9] [10] [13] [14] [16] [17]

❖ La première version de l'UMTS : release 99 (R3) a été approuvée en mars 2000 et définit un nouveau réseau d'accès UTRAN

- Technologie radio FDD/W-CDMA et TDD/TD-CDMA
- Transport ATM dans le réseau d'accès

  Son objectif était de faciliter la migration des services GSM existants.

  Les évolutions prévues pour l'UMTS sont :

❖ Release 4 :

- Introduction du NGN pour le domaine circuit
- Transport IP dans le réseau d'accès
- Introduction d'Edge comme 2ème réseau d'accès (GERAN)
- Mode TDD à bande étroite
- Compléments et amélioration de la R3

❖ Release 5 : vers une architecture « Tout IP »

- HSDPA (high speed downlink packet access) accès paquet haut debit sur canal DSCH

- Introduction du domaine IP multimédia (IMS : IP Multimedia Subsystem) dans le réseau cœur
- Nouvelles fonctionnalités IP (protocole SIP)
- Nouvelle architecture du réseau d'accès basée sur IP

❖ La Release 6 n'est autre que la définition de la phase 2 de l'IMS.

Le tableau suivant montre ses différentes étapes d'évolution :

	Publication de la première version	Principales modifications par rapport à la Release 99 de référence
Release 99	Mars 2000	Architecture de référence des premiers déploiements commerciaux
Release 4	Mars 2001	➢ Nouveaux éléments dans le domaine CS et proposition d'un transport IP à l'intérieur du réseau cœur. ➢ Introduction de la variante *low chip* de l'UTRA/TDD
Release 5	Mars 2002	➢ Définition du sous système multimédia IP (IMS) : introduction de SIP (voix sur IP). ➢ Modification du GERAN pour l'aligner avec l'UTRAN ➢ Proposition d'un transport IP dans l'UTRAN ➢ Introduction de HSDPA ➢ Introduction du codec AMR large bande
Release 6	Décembre 2003	➢ Définition de la phase 2 de l'IMS ➢ Interopérabilité avec des réseaux locaux large bande ➢ Harmonisation entre l'IMS 3GPP et l'IMS 3GPP2 ➢ Introduction de services *Multimedia Broadcast/Multicast*

Tableau 2.03 : Les différentes évolutions de l'UMTS

CHAPITRE 3. L'IMS (IP Multimedia Subsystem)

3.1. Généralités : [21] [22] [23] [24]

L'Internet supporte depuis déjà plusieurs années et avec une qualité très acceptable de nombreux services à succès tels que l'E-mail, le WEB, le streaming audio/vidéo, le « chat ».

Dans les domaines des applications de téléphonie et les communications multimédia, Microsoft MSN, Yahoo, AOL et Skype sont déjà présents sur ce marché mais proposent des solutions propriétaires.

La téléphonie devient donc une application sur Internet parmi tant d'autres et tout fournisseur d'applications sur Internet peut proposer le service de téléphonie sur IP à ses clients indépendamment du type d'accès à Internet utilisé par le client : ADSL, câble, UMTS, etc.

Dans ce contexte les opérateurs de télécommunication, dont le service de téléphonie était jusqu'à présent le business principal, se trouvent face à l'alternative suivante :

1. Repositionner leur business autour des applications sur IP incluant la téléphonie, devenant ainsi opérateur de services globaux. Les opérateurs qui feront ce choix devront rapidement développer une architecture IMS seule solution normalisée dans le monde des télécommunications et cela avant que des solutions propriétaires ne soient trop largement adoptées.
2. Abandonner le marché des applications y compris celui de la téléphonie et réduire leur business à celui de fournisseur d'accès et/ou de transporteur de paquets IP. Les opérateurs qui feront ce choix limiteront leurs champs d'action à celui d'opérateurs de réseaux. Parmi les risques de cette option, la difficulté à maintenir le revenu dans un contexte où l'accès comme le transport seront devenus des commodités sujettes à une très forte pression sur les prix.

L'IMS (IP Multimedia Subsytem) normalisé par le monde des télécommunications est une nouvelle architecture basée sur de nouveaux concepts, de nouvelles technologies, de nouveaux partenaires et un nouvel écosystème. L'IMS supporte sur un réseau tout IP les sessions applicatives temps réel (voix, vidéo, conférence, etc) et non temps réel (Push To Talk, Présence, messagerie instantanée, etc). L'IMS intègre de plus le concept de convergence de services supportés indifféremment par des réseaux de natures différentes : fixe, mobile ou Internet.

Déployer une architecture IMS est donc une décision stratégique qui peut être prise par un opérateur de télécommunication traditionnel dans le cadre du repositionnement de son activité sur le marché des services sur IP mais qui peut également être prise par toute entité qui déciderait, même sans posséder de réseaux d'accès ou de transport, de développer une activité de services à valeur ajoutée sur IP.

L’acquisition des fondements architecturaux et normatifs de l’IMS en particulier les spécifications de protocoles et interfaces spécifiques telles que SIP, Diameter, COPS, etc, et la connaissance des solutions déjà disponibles sur le marché sont donc essentielles pour tout acteur opérateur de réseaux ou de services, fournisseur d’équipements, ou clients qui souhaite prendre sa place dans le business émergeant des services sur IP.

3.1.1. Définition :

L’IMS (IP Multimedia Subsystem en anglais ou sous-système IP multimédia en français) est une partie structurée de l'architecture des réseaux de nouvelle génération (NGN : Next Generation Network) qui permet l’introduction progressive des applications voix et données multimédia dans les réseaux fixes et mobiles. L'IMS vise à assurer la compatibilité entre les réseaux mobiles 3G, les réseaux à commutation de circuits RTCP/RNIS et Internet pour les services vocaux et multimédia. Il peut s’agir de services de transfert de voix, de messagerie instantanée, de jeux interactifs, de partage de contenus, etc.

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

Séparant le contrôle des transactions de la gestion de leur transmission, l’IMS permet de gérer des échanges point à point en présentant toutes les garanties nécessaires à l’acheminement de services multimédia. Pour ce faire, il utilise notamment le protocole SIP (Session Initiation Protocol).

3.1.2. Historique de la normalisation de l'IMS :

3.1.2.1. IMS Forum :

1999 - Création de l’IMS Forum par des industriels de la téléphonie mobile (3GPP2) avec l’idée de réaliser la convergence de services mobiles et filaires voix et multimédia sur la base de IPv6.

2001 - Réalisation de prototypes et d'essais de compatibilité en IPv4.

2005 - Publication de la version 5 de la norme de l’IMS Forum.

2006 - Publication de la version 6.

3.1.2.2. TISPAN (ETSI) :

2003 - Fusion à l’ETSI des groupes de travail SPAN, Signaling System N°7, R1 et TIPHON (Telephony on Internet) en un seul groupe appelé TISPAN NGN (100, puis 300 membres).

Décembre 2005 - Publication de la première édition de la norme ETSI sur IMS, centralisée sur l'accès fixe à haut débit en DSL, la 3G et le GPRS en IPv4 (50 normes, dont certaines à finaliser). Il reste encore à traiter du transit, de l'encapsulation ISUP, des appels d'urgence, des interceptions légales, etc.

2006 - TISPAN travaille avec le DSL Forum, l'UIT-T, le 3GPP, l'IETF, le DVB Forum et les groupes OMA/Parlay spécialisés dans le Réseau Intelligent.

2007 - Sortie prévue de la version 2 de la norme IMS de l'ETSI avec IP/TV, VoD, QoS, accès « entreprise », etc.

2009 - Sortie annoncée de la version 3 relative à la mobilité généralisée et à la convergence.

3.1.2.3. UIT-T :

Début 2006, la Commission d'études 11 de l'UIT-T a reçu les travaux de l'ETSI/TISPAN en vue de leur incorporation dans les normes du NGN.

3.1.2.4. Autres actions de normalisation de l'IMS :

Pas d'informations reçues encore de la part des organismes américain ATIS et asiatique CJK, mais on sait que des réalisations IMS propriétaires ont été réalisées dans plusieurs réseaux.

3.2. Principes de l'IMS : [18] [21] [22] [23] [24]

Le but principal est de proposer une architecture réseau unifiée, basée sur les protocoles de type Internet, pour le support de services de communication convergents.

L'architecture IMS présente un double intérêt pour les opérateurs de réseau.

3.2.1. Une plateforme unifiée :

Les services proposés par l'opérateur sont supportés par une plateforme unifiée, qu'il s'agisse de services interactifs comme la navigation Internet ou la gestion d'e-mail, de services de téléphonie ou d'applications multimédia beaucoup plus exigeantes en termes de qualité de service. A terme, l'IMS est amené à supporter l'ensemble des services usager, du domaine PS comme du domaine CS. La gestion du réseau s'en trouve simplifiée dans la mesure où il n'existe plus de différentiation entre les services de ces deux domaines.

3.2.2. Le support de services Internet :

Grâce à l'IMS, les services basés sur Internet ne sont plus supportés de manière transparente par les réseaux sans fil. L'IMS donne ainsi la possibilité aux opérateurs cellulaires de créer et proposer à leurs abonnés tout un ensemble de services à valeur ajoutée et de tirer parti de la migration des services vers le monde IP. Si l'on considère que cette migration a été amorcée pour les abonnés

filaires bien avant la mise en service commercial des premiers réseaux IMS, ce point est d'une importance capitale pour le positionnement commercial à long terme des opérateurs cellulaires.

L'architecture IMS est constituée par un ensemble d'équipements et de protocoles dont les fonctions et les rôles se précisent. Les interfaces sur les différentes liaisons internes et externes à cette architecture font également l'objet de 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 plateforme unique pour toute une gamme de services et d'être en mesure d'offrir de nouvelles applications en un temps minimum.

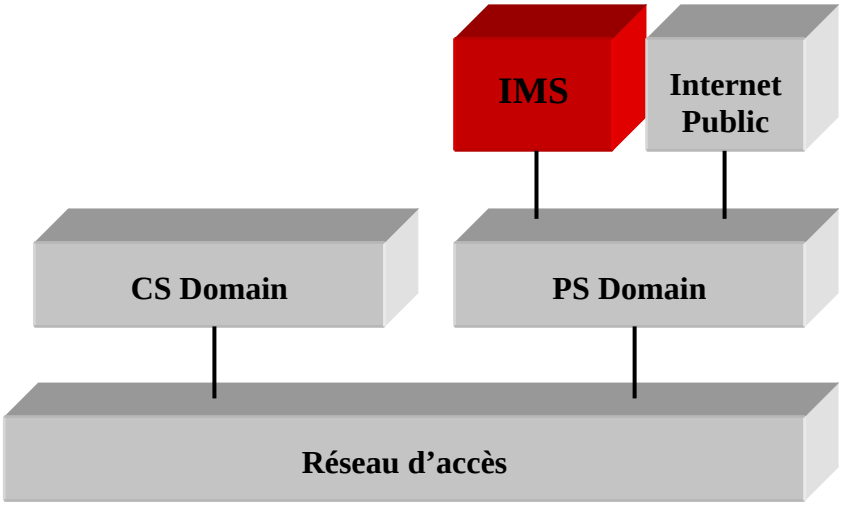

Figure 3.01 : Vue simplifiée de l'architecture UMTS avec IMS

3.3. Architecture IMS : [18] [21] [22] [23] [24]

L'introduction de l'IMS (IP Multimedia Subsystem) dans les réseaux fixe et mobile représente un changement fondamental dans les réseaux de télécommunication de type voix. Les nouvelles capacités des réseaux et des terminaux, le mariage entre l'Internet et la voix, le contenu et la mobilité donnent naissance à des nouveaux modèles de réseaux et surtout offrent un formidable potentiel pour développer de nouveaux services. Dans cet objectif, l'IMS est conçu pour offrir aux utilisateurs la possibilité d'établir des sessions multimédia en utilisant tout accès haut débit et une commutation de paquets IP.

L'IMS fournit un réseau IP multiservice, multi-accès, sécurisé et fiable :

- Multiservices : tous types de services délivrés par un réseau cœur supportant différents niveaux de QoS pourront être offerts à l'usager,

- Multi-accès: Tout réseau d'accès large bande, fixe et mobile pourra s'interfacer à l'IMS
- L'IMS n'est pas un unique réseau, mais différents réseaux qui inter opèrent grâce à des accords de roaming IMS fixe-fixe, fixe-mobile, mobile-mobile.

Pour les fournisseurs de service, l'IMS permet d'offrir :

- Des services de communication non temps réel, pseudo temps réel et temps réel suivant une configuration client-serveur ou entre entités paires.
- La mobilité des services / Mobilité de l'usager (Nomadisme).
- Plusieurs sessions et services simultanément sur la même connexion réseau.

3.3.1. Structuration en couche de l'architecture IMS :

L'architecture IMS peut être structurée en couches. Quatre couches importantes sont identifiées :

- la couche **ACCES** peut représenter tout accès haut débit tel que : UTRAN (UMTS Terrestrial Radio Access Network), CDMA2000 (technologie d'accès large bande utilisée dans les réseaux mobiles aux Etats-Unis), xDSL, réseau câblé, Wireless IP, WiFi, etc.
- la couche **TRANSPORT** représente un réseau IP. Ce réseau IP pourra intégrer des mécanismes de QoS avec MPLS, Diffserv, RSVP, etc. La couche transport consiste donc en des routeurs (edge router à l'accès et en core router en transit) 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.
- la couche **CONTROLE** consiste en des contrôleurs de session responsables du routage de la signalisation entre usagers et de l'invocation des services. Ces nœuds s'appellent des CSCF (Call State Control Function). IMS Introduit donc un environnement de contrôle de session sur le domaine paquet.
- la couche **APPLICATION** introduit les applications (services à valeur ajoutée) proposées aux usagers. L'opérateur peut se positionner grâce à sa couche CONTROLE en tant qu'agrégateur de services offerts par l'opérateur lui-même ou par des tiers. La couche application consiste en des serveurs d'application (AS, Application Server) et des MRF (Multimedia resource function) que les fournisseurs appellent serveurs de média IP (IP MS, IP Media Server).

L’architecture globale IMS est décrite à la figure suivante :

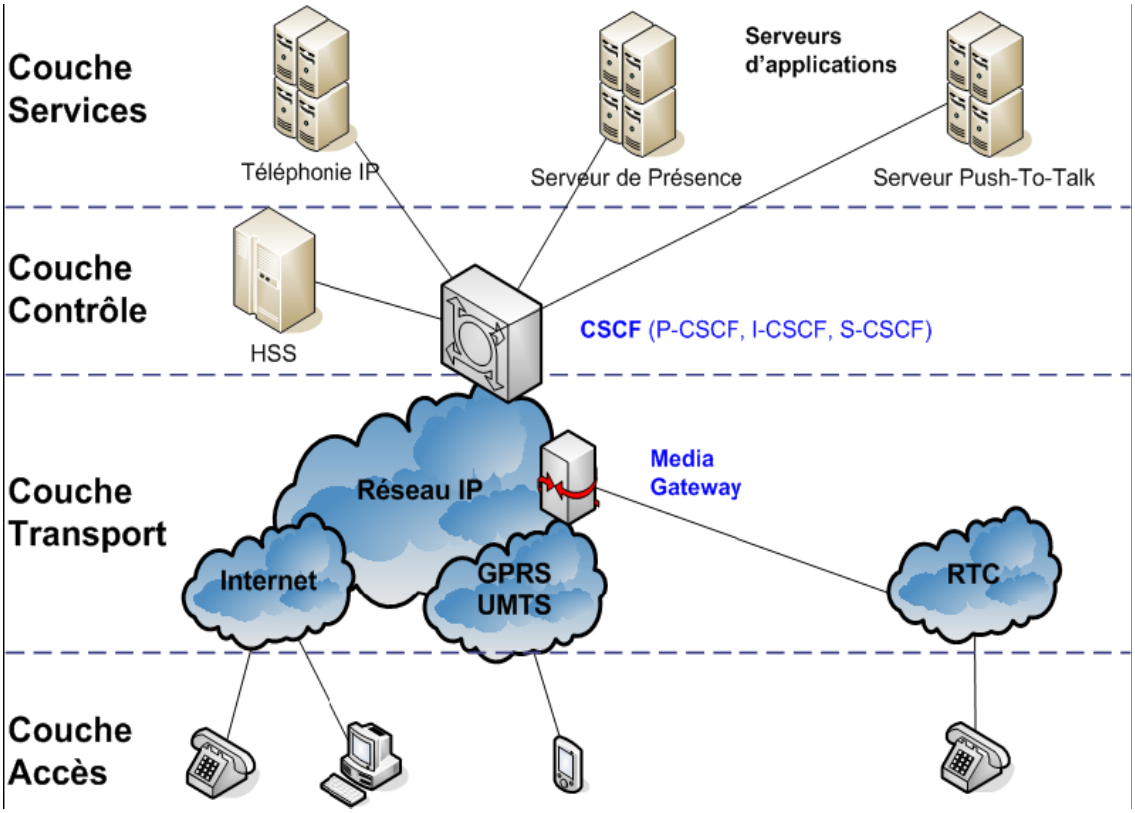

Figure 3.02 : Architecture IMS simplifiée

3.3.2. Déploiement d’une architecture IMS :

- L’IMS est indépendant de tout type d’accès. Aussi bien les usagers mobiles GPRS/UMTS que les usagers fixe large bande (xDSL, câble, etc) peuvent accéder à l’IMS.
- L’IMS fournit l’interface aux réseaux en mode circuit (exemple : RTCP, domaine circuit GSM).
- L’IMS fournit une interface normalisée (ISC, IMS Service Control) basée sur le protocole SIP pour l’accès aux services.

L ’IMS peut être déployé :

- Par un **opérateur mobile** pour offrir des services avancés et multimédia à ses usagers GPRS/EDGE/UMTS.
- Par un **opérateur d’accès filaire** (xDSL, câble).
- Par un **opérateur virtuel** qui déploie l’IMS en s’appuyant sur les réseaux d’accès d’opérateurs tiers.

Ces opérateurs peuvent déployer leurs propres services IMS et ouvrir leur architecture à des ASP qui interfacent alors leur propre serveur d'application à travers l'interface ISC.

3.3.3. Architecture de service IMS :

L'architecture de service IMS de base est constituée d'entités serveurs d'application, de serveurs de média IP et de S-CSCF équivalents à des serveurs d'appels.

Le serveur d'application SIP (AS, Application Server) exécute des services (exemples : Push To Talk, Présence, Prépaid, Instant messaging, etc.) et peut influencer le déroulement de la session à la demande du service. Le serveur d'application correspond à l'entité SCF (Service Control Function) du Réseau Intelligent.

Le serveur de média IP met en œuvre l'entité fonctionnelle MRF (Multimedia Resource Function). Il établit des conférences multimédias, joue des annonces vocales ou multimédia et collecte des informations utilisateurs. Il s'agit de l'évolution de l'entité SRF (Specialized Resource Function) du Réseau Intelligent dans le monde multimédia.

Le serveur d'appel SIP appelé S-CSCF (Serving - Call State Control Function) joue le rôle de point depuis lequel un service peut être invoqué. Il dispose du profil de service de l'abonné qui lui indique les services souscrits par l'abonné et sous quelle condition invoquer ces services.

3.3.4. Entités de l'architecture de service IMS :

L'architecture de service IMS consiste en un ensemble de serveurs d'application interagissant avec le réseau IMS (c'est-à-dire S-CSCF) à travers l'interface ISC (IP Multimedia Service Control) supportée par le protocole SIP.

Les serveurs d'application sont :

- Les serveurs d'application SIP (SIP AS) qui exécutent des services (exemple : Push To Talk, Présence, Prépaid, Instant messaging, vidéoconférence, Unified messaging, etc.) et qui peuvent influencer le déroulement de la session à la demande du service.
- Le point de commutation au service IM (IM-SSF, IP Multimedia Service Switching Function) qui est un type particulier de serveur d'application SIP qui termine la signalisation SIP sur l'interface ISC.
- La passerelle OSA (OSA SCS, OSA Service Capability Server) qui 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.

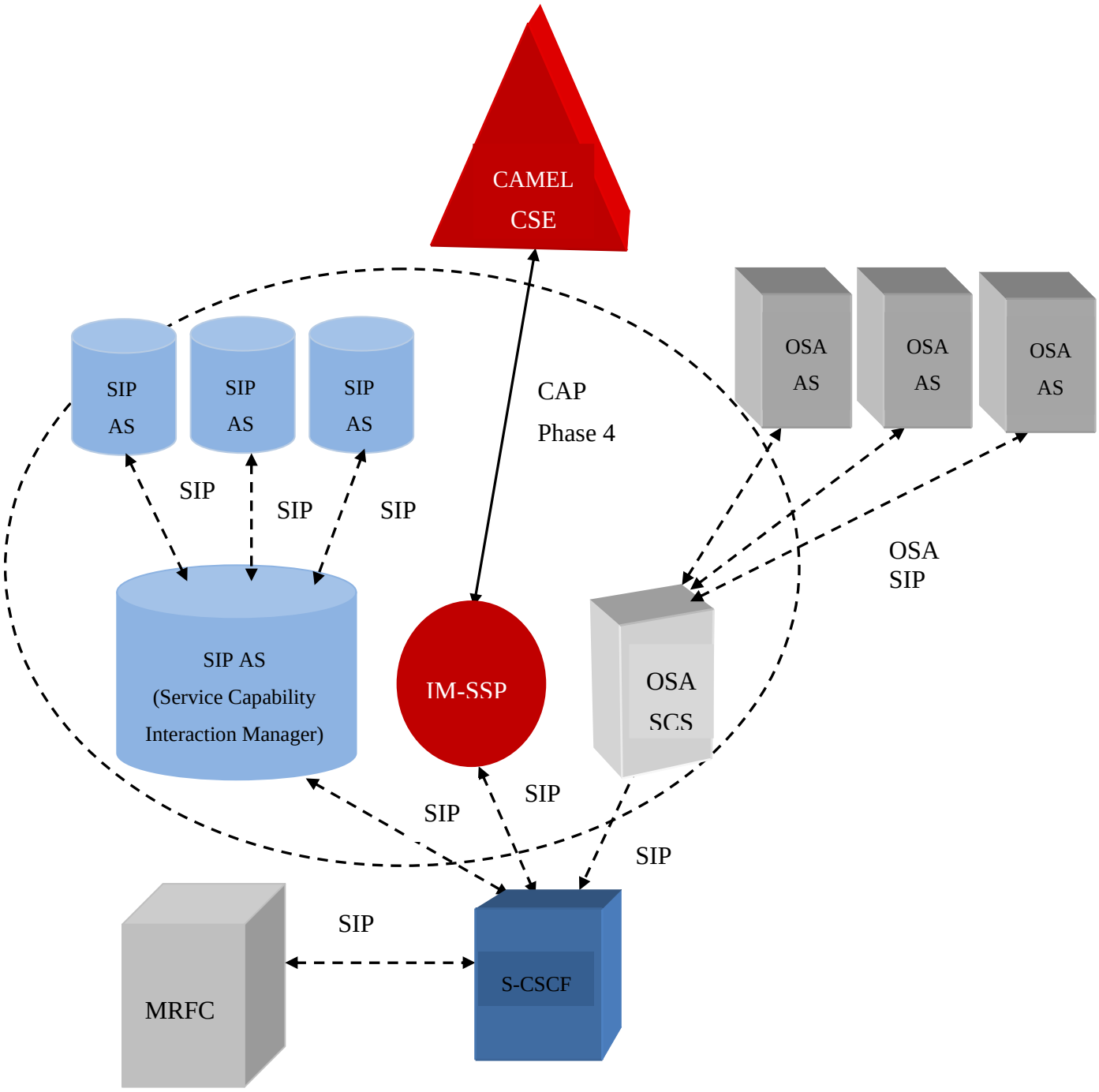

Figure 3.03 : Architecture de service IMS

3.4. Entités de Réseau IMS : [18] [21] [22] [23] [24]

3.4.1. Terminal IMS :

Il s'agit d'une application sur un équipement de l'usager qui émet et reçoit des requêtes SIP. Il se matérialise par un logiciel installé sur un PC, sur un téléphone IP ou sur une station mobile UMTS (UE ou User Equipment).

3.4.2. Home Subscriber Server (HSS) :

L'entité HSS (Home Subscriber Server) est la principale base de stockage des données des usagers et des services auxquels ils ont souscrit. Les principales données stockées sont les identités de l'usager, les informations d'enregistrement, les paramètres d'accès et les informations permettant l'invocation des services de l'usager. L'entité HSS interagit avec les entités du réseau à travers le protocole Diameter.

Le HSS est la somme des fonctions du HLR et de l'AuC (Authentification Center) et de toutes les fonctions nécessaires pour assister les serveurs CSCF dans le support des sessions IMS.

3.4.3. Call State Control Function (CSCF) :

Le CSCF occupe une position centrale dans l'architecture IMS. Il assure le contrôle des sessions IMS de chaque abonné, au travers des différentes phases comme l'enregistrement de l'usager auprès du sous-réseau IMS ou l'établissement d'une session avec un serveur d'application.

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

L'intelligence active de l'IMS est concentrée dans un serveur d'appel constitué d'un trio d'équipements appelés « CSCF » (Call Session Control Function). On distingue le « I-CSCF » (Interrogating) pour l'initialisation des connexions, le « S-CSCF » (Serving) pour la commutation vers l'application, le service ou le réseau (serving in charge) demandés et un P-CSCF (Proxy) pour les fonctions de liaison aux réseaux de paquets et au PDF (recherche des profils de l'usager). Dans la cinquième version de la norme TISPAN, le PDF est séparé de l'I-CSCF afin de permettre l'ouverture de nouvelles applications liées à la qualité de service hors IMS.

Cela a induit la définition de trois entités CSCF : P-CSCF (Proxy CSCF), I-CSCF (Interrogating CSCF) et S-CSCF (Serving-CSCF).

3.4.3.1. P-CSCF :

Le Proxy-CSCF (P-CSCF) est le premier point de contact entre le terminal et le réseau IMS dans le domaine IMS. Son adresse est découverte par le terminal lors de l'activation d'un contexte PDP pour l'échange de messages de signalisation SIP.

Le P-CSCF se comporte comme un Proxy Server SIP lorsqu'il relaye les messages SIP vers le destinataire approprié et comme un User Agent SIP lorsqu'il termine l'appel (exemple : suite à une erreur dans le message SIP reçu).

Les fonctions réalisées par l'entité P-CSCF comprennent :

- L'acheminement de la méthode SIP REGISTER émise par le terminal à l'entité I-CSCF à partir du nom du domaine nominal.
- L'acheminement des méthodes SIP émises par le terminal au S-CSCF dont le nom a été obtenu dans la réponse à la procédure d'enregistrement.
- Le routage des méthodes SIP ou réponses SIP au terminal.
- La génération de CDR (Call Detailed Records).
- La compression / décompression des messages SIP.

3.4.3.2. I-CSCF :

L'Interrogating-CSCF (I-CSCF) est le point de contact au sein d'un réseau d'opérateur pour toutes les sessions destinées à un utilisateur de cet opérateur. Il est chargé de déterminer, lors de la procédure d'enregistrement de l'usager, le S-CSCF qui se charge de la session IMS. Par ailleurs, lors de l'établissement d'une session à destination d'un abonné mobile, l'I-CSCF a pour fonction de retrouver le P-CSCF de l'abonné. Il peut exister plusieurs I-CSCF au sein d'un réseau.

Les fonctions réalisées par l'entité I-CSCF comprennent :

- L'assignation d'un S-CSCF à un utilisateur s'enregistrant.
- L'acheminement des méthodes SIP reçues depuis un autre réseau, au S-CSCF.
- L'obtention de l'adresse du S-CSCF auprès du HSS.
- La génération de CDR.

3.4.3.3. S-CSCF :

Le S-CSCF (ou Serving-CSCF) est le serveur IMS auprès duquel le terminal va effectivement s'enregistrer. Il est chargé de maintenir l'état de la session IMS établie avec l'usager et de fournir un accès direct aux serveurs d'applications.

Le S-CSCF prend en charge le contrôle de la session. Il maintient un état de session afin de pouvoir invoquer des services. Dans un réseau d'opérateur, différents S-CSCF peuvent présenter des fonctionnalités différentes.

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

- L'émulation de la fonction Registrar puisqu'il accepte les méthodes SIP d'enregistrement et met à jour le HSS.

- L’émulation de la fonction Proxy server puisqu’il accepte les méthodes SIP et les achemine.
- L’émulation de la fonction User Agent puisqu’il peut terminer des méthodes SIP par exemple lorsqu’il exécute des services complémentaires.
- L’interaction avec des serveurs d’application après avoir analysé les critères de déclenchement des services correspondants.
- La génération de CDR.

Avant de pouvoir utiliser les services du domaine IM, tels qu’établir une session multimédia ou recevoir une demande de session, un usager doit s’enregistrer au réseau. Que l’usager soit dans son réseau nominal ou dans un réseau visité, cette procédure fait intervenir un P-CSCF. Par ailleurs, tous les messages de signalisation émis par le terminal ou à destination du terminal sont relayés par le P-CSCF ; le terminal n’a jamais la connaissance des adresses des autres CSCF (i.e. I-CSCF et S-CSCF).

3.4.3.4. MGCF, IMS-MGW et T-SGW : Interfonctionnement avec le RTC :

Le domaine IMS doit inter-fonctionner avec le RTCP afin de permettre aux utilisateurs IMS d’établir des appels avec le RTCP. L’architecture d’interfonctionnement présente un plan de contrôle (signalisation) et un plan d’usager (transport). Dans le plan usager, des passerelles (IMS-MGW, IMS - Media Gateway) sont requises afin de convertir des flux RTP en flux TDM.

Ces passerelles ne traitent que le média. Des entités sont responsables de créer, maintenir et libérer des connexions dans ces passerelles; il s’agit de contrôleurs de passerelles (MGCF, Media Gateway Control Function). Par ailleurs, ce même MGC termine la signalisation ISUP du côté RTC qu’il convertit en signalisation SIP qui est délivrée au domaine IMS. Les messages ISUP provenant du RTC sont d’abord acheminés sur SS7 à une passerelle de signalisation (T-SGW, Trunking Signaling Gateway) qui les relaye au MGC sur un transport SIGTRAN.

L’interfonctionnement entre le domaine IMS et le RTCP est donc assuré par trois entités :

- L’IMS-MGW (IP Multimedia Subsystem Media Gateway Function),
- MGCF (Media Gateway Control Function)
- et T-SGW (Trunking Signaling Gateway Function).

3.4.3.4.1. L’IMS-MGW :

- Reçoit un trafic de parole du RTCP et l’achemine sur un réseau IP. Le trafic audio est transporté sur RTP/UDP/IP.
- Supporte généralement des fonctions de conversion du média et de traitement du média (annulation d'écho, pont de conférence).

- Est contrôlé par le MGCF à travers le protocole MEGACO/H.248.

3.4.3.4.2. Le MGCF :

- Comme les entités CSCF, n'appartient qu'au plan de contrôle et non au plan média.
- Contrôle l'IMS-MGW afin d'établir, maintenir et libérer des connexions dans l'IMS-MGW. Une connexion correspond par exemple à une association entre une terminaison TDM (terminaison du côté RTC) et une terminaison RTP/UDP/IP. Un transcodage de la parole doit aussi avoir lieu au niveau de l'lMS-MGW pour convertir la parole reçue et qui est encodée à l'aide du codec G.711, en parole encodée en utilisant le codec AMR (UMTS) si le terminal IMS est un mobile UMTS.
- Assure la conversion des messages ISUP (Signalisation RTC) en des messages SIP (Signalisation IMS).
- Sélectionne le CSCF approprié afin de remettre la signalisation SIP qu'il génère, au sous-système IMS.

3.4.3.4.3. Le T-SGW :

- Assure la conversion du transport pour l'acheminement de la signalisation ISUP entre le commutateur téléphonique et le MGCF. La signalisation ISUP est échangée :
  - Sur SS7 entre le commutateur et le T-SGW
  - Sur SIGTRAN entre le T-SGW et le MGCF
- Par contre, n'analyse pas les messages d'application ISUP.

La figure (3.04) représente un appel initié par le RTCP et à destination d'un terminal dans le sous-système IMS.

Le commutateur du RTC réserve un circuit de parole qu'il partage avec l'IMS-MGW et émet un message ISUP IAM sur un transport SS7 au T-SGW (Trunking Signaling Gateway). Le TSGW est responsable de la conversion du transport du message ISUP. Ce message est relayé à l'entité MGCF sur SIGTRAN.

Le MGCF crée un contexte dans l'entité IMS-MGW en utilisant le protocole MEGACO/H.248.

Ce contexte consiste en une association entre une terminaison TDM et une terminaison RTP. La terminaison TDM termine le circuit de parole que l'IMS-MGW partage avec le commutateur téléphonique. La terminaison RTP termine les canaux RTP entre l'IMS-MGW et le terminal IMS.

L'IMS-MGW retourne une réponse à l'entité MGCF ; cette réponse contient un « local descriptor » qui correspond à la description SDP associée à sa terminaison RTP.

L’entité MGCF génère une méthode SIP INVITE contenant la description SDP retournée par l’IMS-MGW. Cette méthode est envoyée au sous-système IMS qui se charge de la délivrer au terminal IMS appelé.

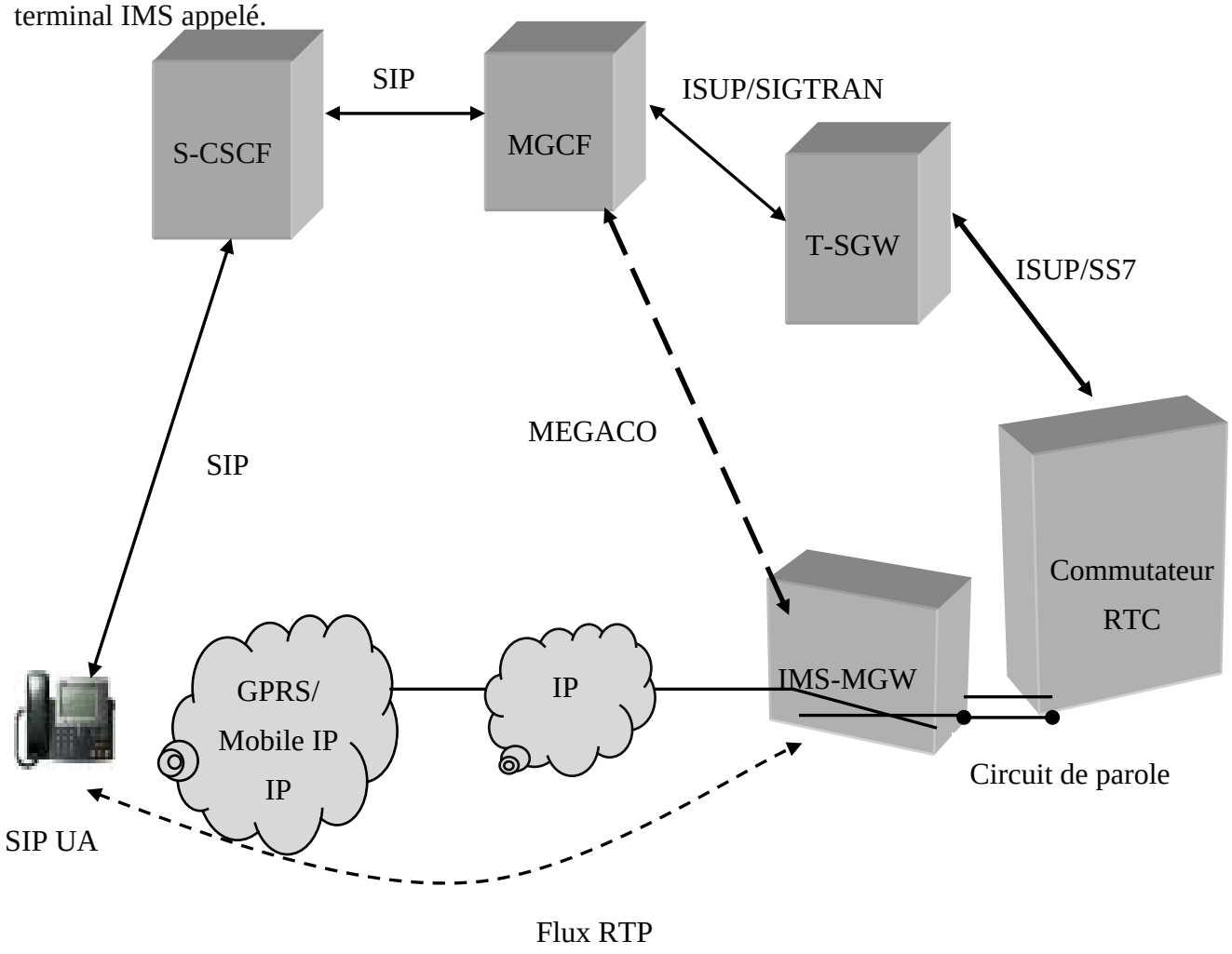

Figure 3.04 : Interfonctionnement entre RTC et IMS

3.5. Protocoles usagers de l’IMS : [18] [19] [20] [21] [22] [23] [24] [25]

Afin de s’intégrer au mieux dans le monde des services Internet existants, les protocoles mis en jeu dans l’architecture IMS pour l’établissement des sessions et le transport des données usagers sont tous issus des travaux de l’IETF (Internet Engineering Task Force).

Les trois principaux protocoles de l’IETF mis en œuvre dans l’IMS sont :

- SIP (Session Initiation Protocol) qui est le protocole d’établissement de session. C’est l’équivalent Internet des protocoles d’établissement d’appel CC (Call Control) du domaine CS.
- SDP (Session Description Protocol) est un protocole ou langage permettant de décrire les paramètres d’une session, c’est à dire les types de médias mis en jeu (audio et/ou vidéo) et la manière dont les informations sont encodées.

- RTP/RTCP (Real time Transport Protocol / Real time Transport Control Protocol) utilisés pour le support des applications à caractère temps réel comme les sessions de streaming audio et/ou vidéo ou la voix sur Internet.

La figure suivante donne une vue générale de l'organisation de ces différents protocoles dans un terminal usager.

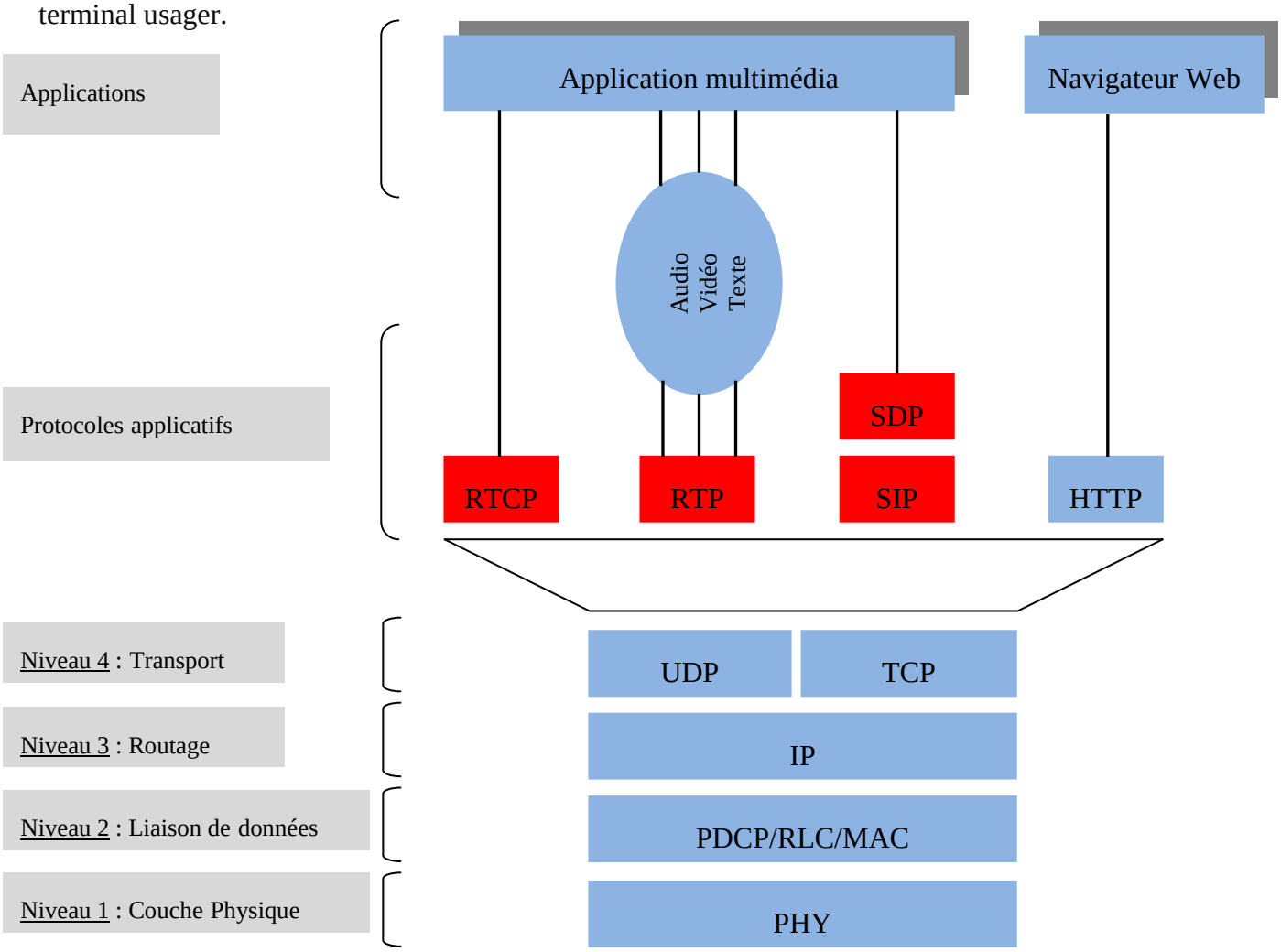

Figure 3.05 : Organisation des principaux protocoles Internet de l'IMS

Le but de la couche IP du niveau 3 est d'assurer le routage des paquets entre les nœuds du réseau, qu'il s'agisse du GGSN ou de tout autre routeur IP du réseau Internet.

Les autres couches de protocole de niveau 2 ou de la couche physique sont spécifiques à l'interface radio de l'UTRAN.

Le protocole SDP utilise les services de la couche SIP pour négocier et établir les paramètres de la session de communication avec l'entité distante. Les autres protocoles de la couche « Application », RTCP, RTP, SIP et HTTP, utilisent les services d'UDP (User Datagram Protocol) et TCP (Transmission Control Protocol). Ces deux protocoles appartiennent à la couche

« Transport » et sont chargés de maintenir un lien ou contexte de bout en bout entre les deux entités communicantes en mode connecté dans le cas de TCP, ou non connecté pour UDP.

3.5.1. Le protocole SIP :

3.5.1.1. Présentation :

SIP est un protocole de signalisation récent appartenant à la couche application qui permet d'ouvrir (ou d'établir), de modifier et de libérer les sessions multimédia (sessions IP) soit en mode point à point ou diffusion. Il est décrit dans le RFC 3261 et a été développé au sein de l'IETF MMUSIC (Multiparty Multimedia Session Control) en 1999 comme étant une alternative à H.323, jugé trop compliqué.

Il a été conçu dans la philosophie de l'Internet pour l'exploitation des protocoles HTTP (Hyper Text Transfert Protocol) utilisé pour naviguer sur le web, et SMTP (Simple Mail Transport Protocol) utilisé pour transmettre des messages ou courriers électroniques (E-mails). Il est utilisable avec les protocoles TCP/UDP, RTP, RTCP et pour les sessions, avec SDP (Session Description Protocol). Il permet d'établir une session entre deux (2) interlocuteurs identifiés par des adresses similaires à des adresses e-mail. Les messages SIP sont rédigés en mode « texte » (et non en binaire comme H.323) et donc plus facile à comprendre et à modifier. Il est indépendant de l'architecture de réseau sous-jacente et des flux multimédia.

La mobilité personnelle est une des fonctionnalités de SIP. Un utilisateur peut garder le même numéro malgré qu'il soit connecté à des terminaux d'adresses physiques différentes. Dans le monde SIP, les usagers sont connus par leur nom symbolique, ou URI (Uniform Resource Identifier) appelé encore adresse SIP. Le format d'un URI SIP est assez proche d'une adresse

E-mail. Son format général est sip : user@host, « user » étant le nom de l'usager, « host » étant le domaine auquel il est rattaché.

SIP est utilisé dans l'IMS comme protocole de signalisation pour le contrôle de sessions et le contrôle de service. Il remplace donc à la fois les protocoles ISUP (ISDN User Part) et INAP (Intelligent Network Application Part) du monde de la téléphonie en apportant la capacité multimédia. SIP s'appuie sur un modèle transactionnel client/serveur comme HTTP.

La responsabilité de SIP se limite à la mécanique d'établissement de la session. Les autres aspects de la session, comme les types de média employés (audio, vidéo) ou le format de codage des flux de données, sont du ressort de SDP.

3.5.1.2. Les clients et les serveurs SIP :

3.5.1.2.1. Le client SIP :

Le protocole SIP fonctionne en mode client/serveur, dans un même terminal client on trouve deux applications : UAC (User Agent Client) qui émet les requêtes et UAS (User Agent Server) qui reçoit les requêtes. Et le terminal fonctionne seulement comme l'un ou l'autre par transaction. Ces deux applications forment l'UA (User Agent). Un terminal A peut appeler directement un terminal B ou passer par des serveurs. Un client doit avoir un minimum de méthodes afin d'établir la connexion.

Le tableau ci-dessous résume les messages SIP :

Méthodes SIP	Descriptions
INVITE	Invite un utilisateur pour un appel
ACK	Message d'acquittement du message INVITE
BYE	Fin de communication ou refus d'un appel
CANCEL	Fin d'une requête ou recherche d'un utilisateur
OPTIONS	Demande d'informations sur le serveur
REGISTER	Enregistrement de la position d'un utilisateur
INFO	Information sur la session en cours

Tableau 3.01: Messages SIP

Les messages de réponse sont des numéros et sont classés suivant le premier chiffre :

- 1xx : messages d'information (100 pour essai, 180 pour sonne)
- 2xx : messages de succès (200 pour OK, 202 pour accepté)
- 3xx : messages de redirection (302 pour momentanément ailleurs)
- 4xx : messages d'erreur sur le client (404 pour pas accessible, 482 pour détection de boucle)
- 5xx : messages d'erreur sur le serveur (501 pour pas implémenté)
- 6xx : destination occupée, non accessible ou refusant la communication (603 pour refus).

3.5.1.2.2. Les serveurs SIP :

Les serveurs SIP sont des applications qui acceptent les requêtes d'un terminal SIP. Il y a quatre types de serveurs SIP :

- Le Proxy Server (serveur proxy) :

C'est un serveur d'appel auquel est relié un terminal fixe ou mobile. Il interprète et route l'appel en direction du destinataire. Il se peut que le proxy ne sache pas où se trouve le destinataire, c'est pourquoi dans ce cas là, il consulte un serveur de localisation. Il y a deux sortes de proxy, les

proxys « stateful » et « stateless », la différence est le fait que proxy « stateful » enregistre la position du destinataire tandis que le proxy « stateless » ne la mémorise pas. Ce qui fait que le proxy « stateful » consulte une seule fois le serveur de localisation par destination jusqu'à ce que la destination soit effacée de sa table de « routage ».

- Le Redirect Server (serveur de redirection) :

Il réalise une association d'adresses vers une ou plusieurs adresses. Le fonctionnement d'un tel réseau est le suivant : l'émetteur de l'appel envoie sa requête au serveur de redirection, celui-ci lui retourne la position du destinataire s'il la connaît sinon il va consulter le serveur de localisation. Une fois que la position du destinataire est connue par le serveur de redirection, il va la renvoyer à l'émetteur. Une fois l'émetteur en possession de l'adresse de destination, il la transmet au proxy afin de pouvoir joindre le destinataire.

- Le Location Server (serveur de localisation) :

C'est le serveur qui fournit la position courante des utilisateurs dont la communication passe par le proxy server et le serveur de redirection auxquels ils sont rattachés.

- Le Registar :

C'est un serveur qui accepte les requêtes REGISTER et offre la fonction de localisation. Chaque proxy ou serveur de redirection est généralement relié à ce serveur. Typiquement, il est implémenté dans un proxy ou un serveur de redirection et c'est la raison pour laquelle il peut fournir des fonctions de localisation.

3.5.1.3. Etablissement de session SIP :

La plupart du temps, l'établissement de sessions SIP implique des nœuds intermédiaires du réseau, également appelés proxy, car l'adresse Internet et la localisation des entités ne sont pas en général connues d'avance.

La figure suivante présente un cas simple d'établissement de session SIP entre deux usagers du réseau user1 et user2, au travers de deux serveurs proxy, le premier utilisé pour diriger la requête vers le bon réseau (le serveur DNS ou Domain Name Server permet de traduire l'adresse symbolique du serveur SIP du destinataire en adresse Internet), le deuxième servant à localiser le destinataire user2 dans son réseau.

Une fois la session établie au travers de Proxy1 et 2, les commandes SIP peuvent être envoyées directement d'user1 à user2, car chacun connaît l'adresse exacte de l'autre. De même, le flux de données échangées peut tout à fait transiter directement d'user1 à user2 sans passer par l'un des

deux serveurs. Dans la littérature, on évoque souvent le « SIP trapezoid » en raison de la similitude du tracé des routes avec la figure géométrique.

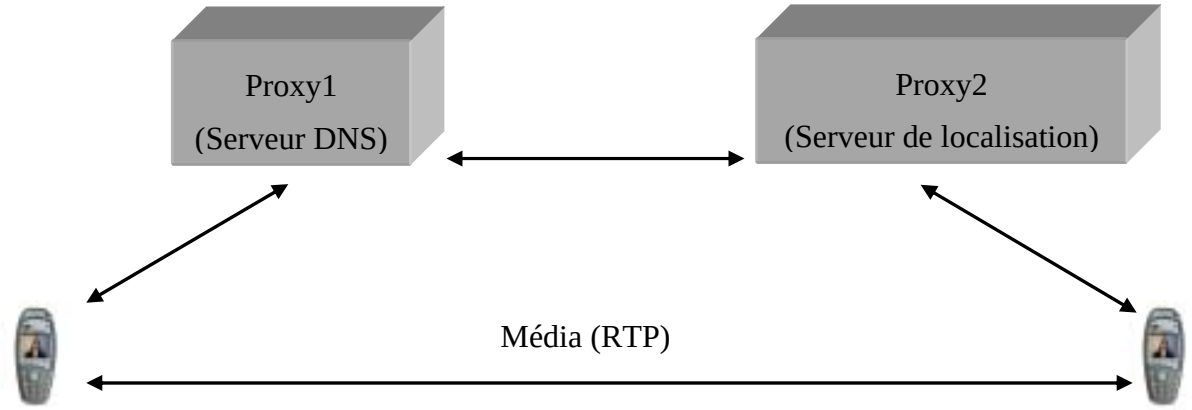

Figure 3.06 : L'architecture SIP (SIP trapezoid)

Une session de communication SIP peut se découper en trois grandes étapes :

- **1. L'initiation de la session**. Le message INVITE utilisé pour établir la session, contient l'adresse symbolique de user2 : user2@domain2.com. Ce message contient un descriptif SDP des paramètres de la session demandée par user1. Le Proxy1 traduit le domaine du destinataire (domain2.com) en adresse Internet, et transmet la requête vers le Proxy2. A son retour, Proxy2 va rechercher l'adresse Internet de user2 afin de lui faire parvenir le message INVITE. Le code réponse 180 indique à user1 que la requête est parvenue jusqu'au terminal de user2.
- **2. L'établissement**. Le code 200 est émis par le terminal de user2 lorsque la session est acceptée (équivalent du « décroché »). Ce message contient des paramètres SDP qui peuvent éventuellement différer de ceux demandés par user1, en fonction des capacités du terminal de user2. Le message « Ack » signifie que la session est finalement acceptée par user1, avec les paramètres SDP négociés entre les deux entités distantes.
- **3. La fin de la session de communication**, signifiée par user1 au travers du message BYE.

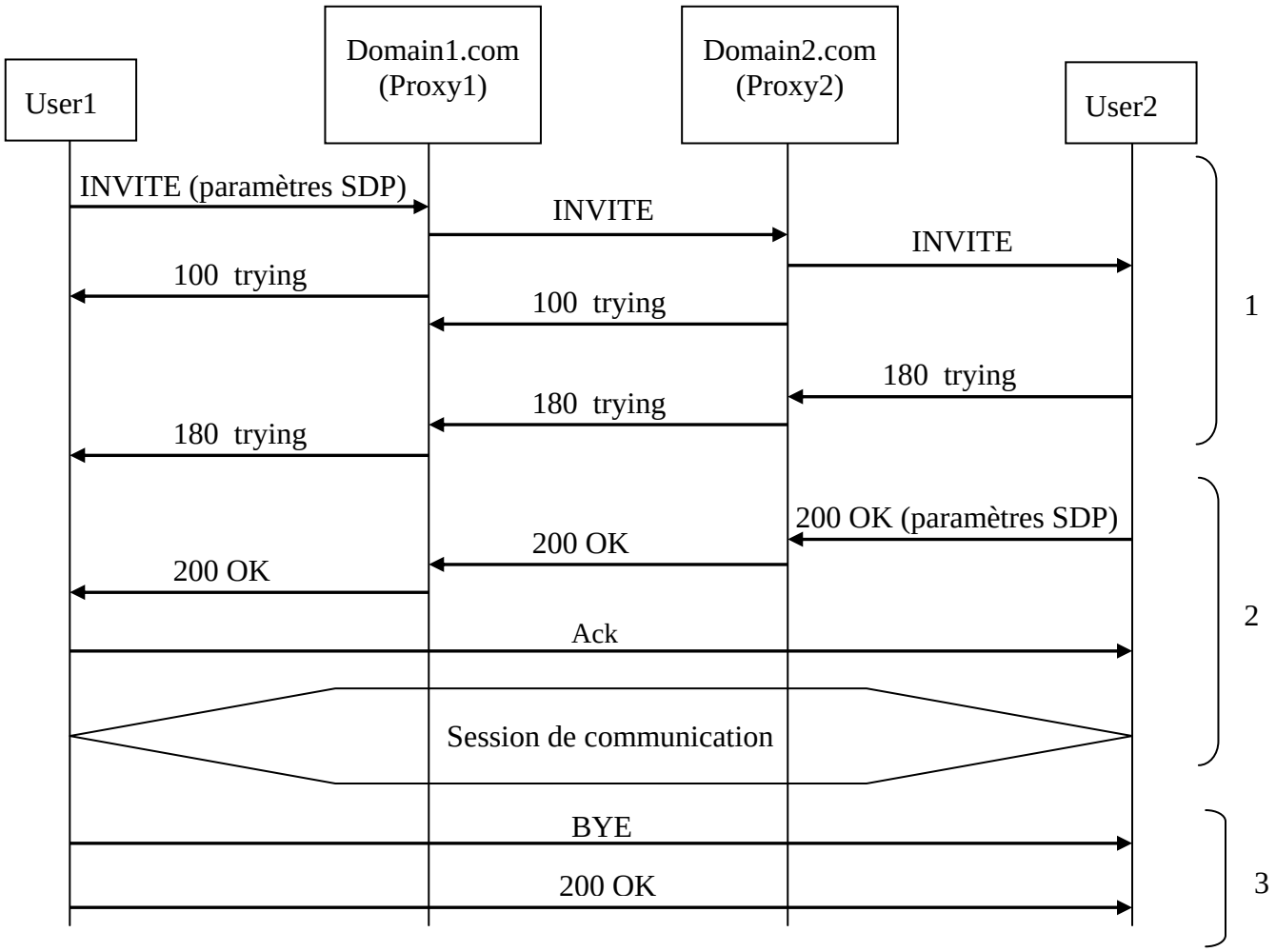

Figure 3.07 : Un exemple d'établissement de session SIP

3.5.2. Le protocole SDP :

Le protocole SDP est un protocole applicatif ayant pour fonction de décrire les paramètres d'une session multimédia, audio et vidéo. Le SDP donne les informations nécessaires à l'établissement d'une communication multimédia telles que l'identité de l'initiateur de la session, la bande passante disponible, etc.

Comme SIP, SDP est un protocole en mode texte. Son format est très simple, une session étant décrite par une succession de lignes de type <paramètre> = <valeur>. Les paramètres de SDP sont répartis en deux groupes : ceux de niveau session, et ceux associés à chaque flux de données.

- v : la version du protocole SDP utilisée pour décrire la session
- o : les références du créateur (Owner) de la session
- s : le nom de la session
- i : un champ informatif décrivant brièvement l'objet de la session

- u : contient un URI, ou adresse Web pointant sur une page donnant des informations supplémentaires sur la session
- e : l'adresse e-mail de la personne responsable de la session
- c : contient une information de connexion, typiquement une adresse Internet
- t : définit l'heure de début et de fin de session
- a : décrit un attribut de session, ou de média lorsqu'il est placé après une ligne « m= «
- m : décrit un flux d'information de la session.

Un exemple de session multimédia décrite par SDP est montré par la figure suivante.

	v = 0
	o = mhandley 2890844526 289042807 IN IP4 126.16.64.4
	s = SDP seminar
	i = A Seminar on the session description protocol
Paramètres de niveau session	u = http://www.cs.ucl.ac.uk/staff/M.Handley/sdp.03.ps
	e = mjh@isi.edu (Mark Handley)
	c = IN IP4 224.2.17.12/127
	t = 2873397496 2873404696
	a = recvonly
1er flux de données	m = audio 49170 RTP/AVP 0
2ème flux de données	m = video 51372 RTP/AVP 31
3ème flux de données	m = application 32416 udp wb
	a = orient : portrait

Figure 3.08 : Un exemple de session SDP

Comme indiqué par le paramètre « i = », il s'agit d'une session de formation au protocole SDP.
La session est composée de trois flux. Le premier est de type « audio », diffusé sur le port 49170. « RTP/AVP 0 » signifie que les paquets de voix sont transportés par le protocole RTP et le profil AVP (Audio/Video Profile) encodé suivant le format G.711 (profil « 0 »).
Le deuxième flux est de type « vidéo », diffusé sur le port 51372, également transporté par le protocole RTP avec un encodage de type H.261 (profil « 31 »).
Le format de troisième flux n'est pas décrit de manière précise, car son format exact dépend de l'application émettrice. Dans ce cas, il s'agit de dessins ou croquis (« wb » ou whiteboard) destinés à être diffusés à l'ensemble des participants de la session.

3.5.3. RTP / RTCP (Real-time Transport Protocol / Real -time Transport Control Protocol) :

Les protocoles RTP et RTCP garantissent la qualité des communications multimédia en mode paquet (gestion et contrôle des flux temps réel). Pouvant être mis en œuvre au-dessus d'IP ou d'ATM, ils sont utilisés par les deux protocoles de contrôle d'appel SIP et H.323.

3.5.3.1. Le protocole RTP (Real-time Transport Protocol) :

3.5.3.1.1. Présentation :

RTP est utilisé pour transporter des données multimédia comme l'audio, la vidéo, le texte. Ce protocole encode et partage les données en paquets et les transporte à travers Internet. Il a été développé au sein de l'IETF et est décrit dans le RFC 1889. RTP est un protocole qui se situe au niveau de l'application et qui utilise le protocole UDP afin de gagner en termes de temps.

3.5.3.1.2. Les fonctions de RTP :

Le protocole RTP, standardisé en 1996, a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. Ceci de façon à reformer les flux avec ses caractéristiques de départ. RTP est un protocole de bout en bout qui permet de s'adapter aux besoins des applications et sera par conséquent, intégré dans le noyau de celles-ci. RTP laisse la responsabilité du contrôle aux équipements d'extrémité.

RTP permet de :

- Reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur)
- Mettre en place un séquencement des paquets par une numérotation, et ce, afin de permettre la détection des paquets perdus (il est nécessaire de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte, par exemple le remplacement par un paquet qui se compose d'une synthèse des paquets précédent et suivant) ;
- Identifier le contenu des données pour leurs associer un transport sécurisé.
- L'identification de la source c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast, l'identité de la source doit être connue et déterminée.
- Transporter les applications audio et vidéo dans des trames. Ces trames sont incluses dans des paquets afin d'être transportées et doivent de ce fait être récupérées facilement au moment de la phase de paquétisation afin que l'application soit décodée correctement.

En revanche, il ne peut pas assurer à lui seul le temps réel sur IP puisqu'il ne procure pas d'action sur le réseau (réservation des ressources), la fiabilité des échanges (retransmission automatique,

régulation automatique du débit, garantie de délai de livraison car seules les couches de niveau inférieur le peuvent).

3.5.3.2. Le protocole RTCP (Real -time Transport Control Protocol) :

3.5.3.2.1. Présentation :

RTCP est le protocole complémentaire à RTP, effectuant les services de contrôle et de signalisation. Il est décrit dans le RFC 3550. Sa principale fonction est d'offrir un feedback sur la qualité de la distribution des données. L'une des particularités de RTCP est de permettre la synchronisation sur les récepteurs de données audio et vidéo sur un flux RTP.

3.5.3.2.2. Les fonctions de RTCP :

Le protocole RTCP est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP. Le protocole RTP utilise le protocole RTCP, qui transporte les informations supplémentaires suivantes pour la gestion de la session :

- Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS (le nombre de paquets perdus, la gigue, le délai aller-retour). Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir la QoS.
- Une synchronisation supplémentaire entre les médias. Les applications multimédias sont souvent transportées par des flots distincts.
- L'identification car en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Le contrôle de la session, car RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. On peut dire que les paquets RTP ne transportent que les données des utilisateurs tandis que les paquets RTCP ne transportent, que de la supervision. On peut détailler les paquets de supervision en 5 types : 200, 201, 202, 203, 204. Ces différents paquets de supervision fournissent aux nœuds du réseau les instructions nécessaires à un meilleur contrôle des applications temps réel.

CHAPITRE 4. REALISATION D'UN SYSTEME DE GESTION DES DOSSIERS PATIENTS D'UNE CLINIQUE (OU D'UN HOPITAL) SUR UN RESEAU IP EN SE BASANT SUR LES PRINCIPES DE L'IMS

4.1. But de la simulation :

Notre but est de développer une application permettant de gérer les dossiers patients d'une clinique (ou d'un hôpital) dans le réseau local de la clinique (ou de l'hôpital) via une interface web. Cette application est écrite sous Java avec l'API JSP pour l'affichage côté client. Le développement de cette application a pour conséquence d'aider et de faciliter grandement les médecins dans l'exécution de leur fonction et ainsi optimiser leur capacité de travail. Les utilisateurs cibles de cette application sont surtout les médecins et leurs assistants. Afin de garantir la sécurité de l'application, il s'avère nécessaire de restreindre l'accès à la ressource et de ce fait, une authentification est nécessaire avant l'accès à tous les services proposés (la fiche du patient, etc). Pour cela, on fait appel à une base de données qui stockera la liste des médecins qui travaillent dans la clinique (ou dans l'hôpital) qui auront le privilège d'accéder à la page d'inscription des patients et à la page agenda pour suivre l'évolution de l'état des patients. C'est à l'application donc de vérifier auprès de la base de données si le demandeur est réellement un médecin travaillant dans la clinique (ou l'hôpital) ou non. Pour l'accès à la base de données, Java utilise l'API JDBC. L'accès à la base ne se fait donc pas nativement mais on a recours à un middleware.

Dans notre réalisation pratique, on dispose de deux ordinateurs reliés à un concentrateur :

- Un serveur pour pouvoir écouter les ordinateurs clients (ordinateurs utilisés par les médecins). Le serveur possède une base de données des médecins utilisant ces ordinateurs.
- Un ordinateur client qui peut se communiquer avec la machine serveur.

4.2. Langage de programmation : [26] [27] [28] [29]

4.2.1. Choix du langage Java :

Java est un langage de Programmation Orienté Objet. Dérivé du C++, il jouit des avantages de ce dernier sans en posséder ses défauts. Java est portable, robuste et parfaitement fiable. La force de Java, c'est surtout sa gratuité et sa bonne structuration ce qui fait de lui un langage très populaire auprès des développeurs.

Tous ces paramètres ont conforté le choix du langage sans négliger qu'il a été appris depuis la troisième année.

4.2.2. Choix de la base de données MySQL:

On trouve divers SGBD sur le marché, et ils utilisent tous le langage non procédural SQL. Ce langage permet d'effectuer des requêtes sur une base de données telles que la manipulation (mise à jour, suppression d'enregistrement, extraction) la création (table, vue, base de données) mais quelques uns se démarquent du reste. On pourra citer : Oracle, PostGre, MySql, DB2, MS SQL SERVER etc. On a choisi MySql car ce SGBD est avant tout gratuit, de plus il propose un système de gestion assez simplifié des bases de données.

4.3. Présentation de l'API utilisé :

4.3.1. Développement Web avec Java : les pages JSP

Bien que Java propose d'autres approches pour le développement web, dans notre cas, les pages JSP feront l'affaire. L'API JSP permet de mettre en œuvre la création de page web dynamique à base d'un squelette html et des données incluses dynamiquement par du code Java. Quand un client http effectue une requête et que la réponse contient des données dynamiques du genre JSP, le conteneur JSP compile le fichier en question et génère un Servlet puis la réponse de la requête est renvoyée au client de façon à ce que l'existence de la page JSP lui soit inconnue.

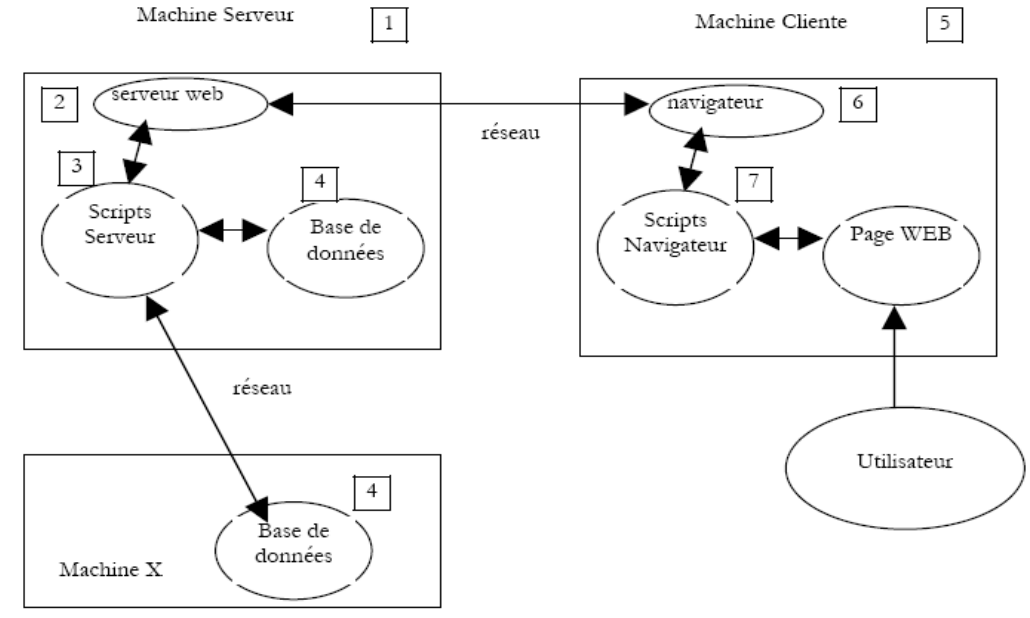

Figure 4.01 : Illustration des composantes d'une application web.

L'API JSP peut être classé parmi les scripts côté serveur. Pour le mettre en œuvre, il faut que la machine, qui sera donc considérée comme serveur, possède un conteneur JSP. Il en existe beaucoup sur le marché, mais Apache Tomcat se démarque du fait de sa fiabilité et de sa gratuité.

Apache Tomcat est gratuit et une fois installé, il suffit de placer les fichiers *.jsp dans la racine du site.

4.3.2. Configuration de Tomcat :

Le conteneur Tomcat impose certaines règles. Pour pouvoir déployer une application développée en JSP, il faut suivre certaines procédures.

Modification de contexte :

Tomcat propose une administration centralisée par un site web. Ainsi, pour effectuer une quelconque modification il suffit de lancer le navigateur web et de taper comme URL :

http://localhost:8080 où 8080 est le port d'écoute de Tomcat. Remarquons que cette page correspond au répertoire : $_CATALINA_HOME/webapps/ROOT/index.html où $_CATALINA_HOME est le répertoire d'installation de Tomcat.

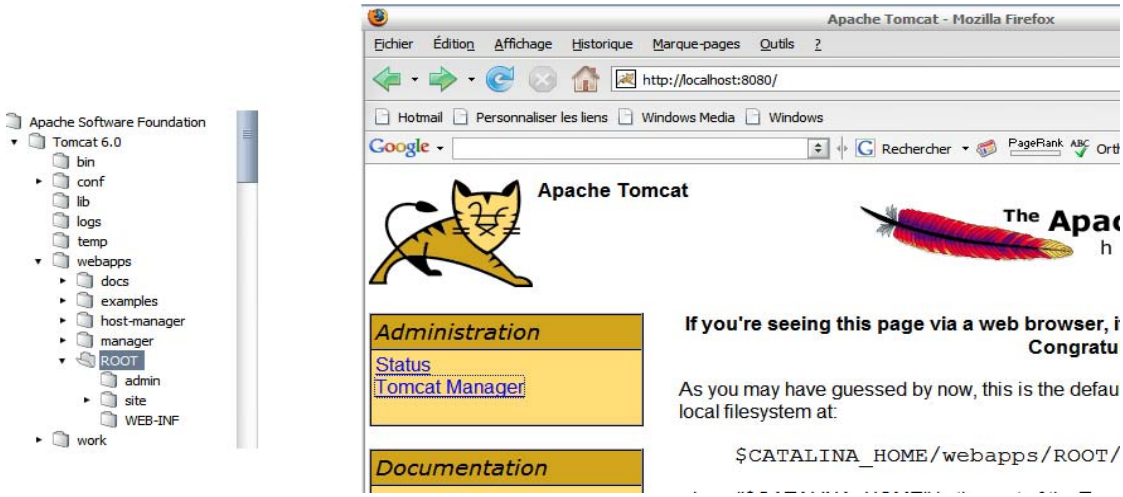

Figure 4.02 : Correspondance entre l'adresse URL et le répertoire ROOT

En fait, pour déployer un projet Tomcat il suffit de lancer le Tomcat Manager et de spécifier le contexte d'accès à l'URL ainsi que le chemin absolu du répertoire où se trouve le projet Tomcat.

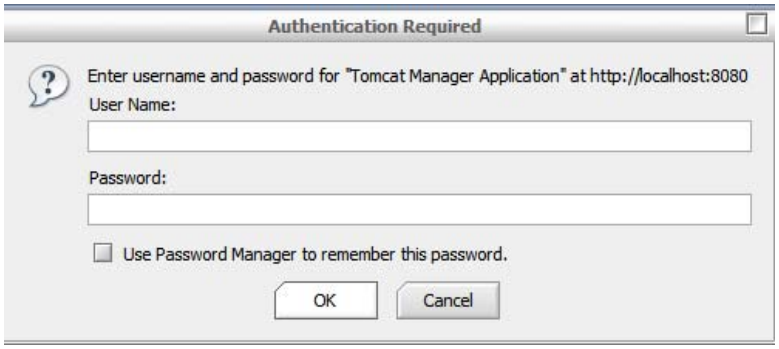

Figure 4.03 : Authenfication de l'utilisateur

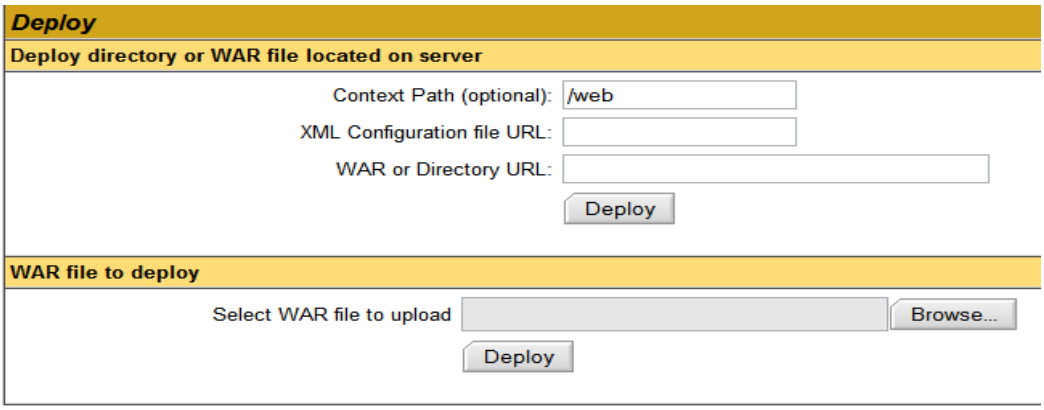

Figure 4.04 : Déploiement du projet Tomcat en utilisant Tomcat Manager.

Si l'opération a réussi il suffit alors de lancer l'application en appuyant sur le lien /web, toujours dans Tomcat Manager dans le tableau des applications.

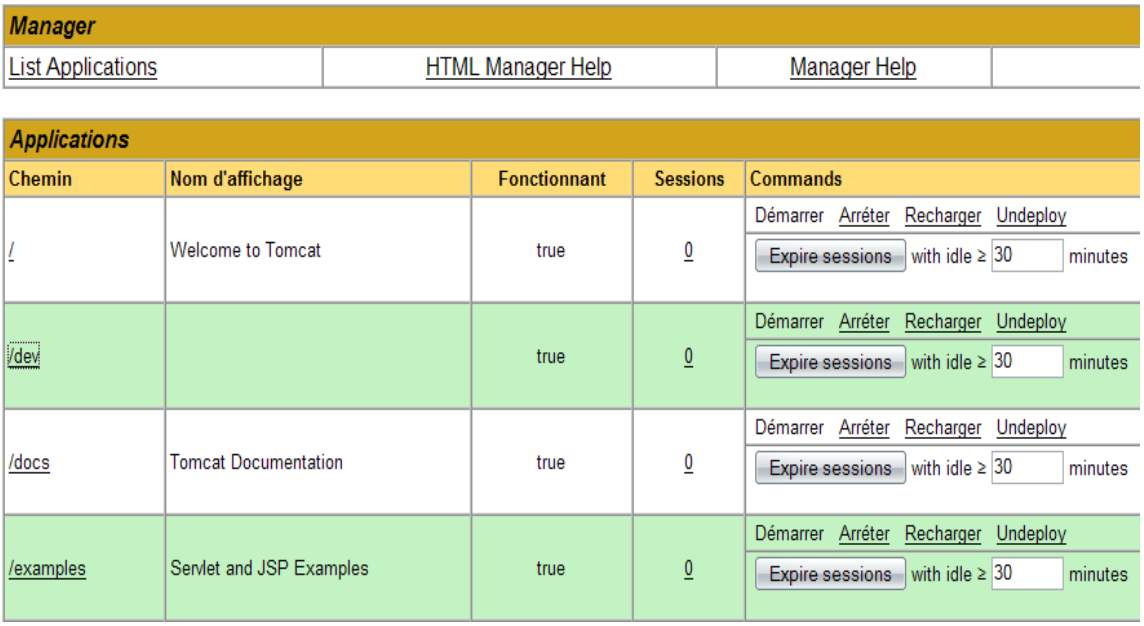

Figure 4.05 : liste des applications déployées dans Tomcat

4.4. Organisation de l'application :

Comme nous l'avons dit auparavant, nous adopterons une architecture client/serveur pour la réalisation de notre simulation. De ce fait, nous utiliserons un ordinateur qui servira de serveur et qui contiendra les bases de données patients et médecins, et un ordinateur client, utilisé par les médecins, qui communiquera avec le serveur (enregistrement de nouveau patient, consultation des dossiers patients, consultation de la liste des médecins travaillant dans la clinique, etc).

L’organisation côté serveur est assez simple. Le serveur, après avoir authentifié le médecin qui veut accéder au site de gestion des dossiers patient, permet l’ouverture d’une ou plusieurs sessions. Après que le médecin ait effectué toutes les opérations qui lui sont permises, le serveur ferme la ou les session(s) quand il demande une fermeture de session(s).

L’organisation côté client se présente suivant l’organigramme qui suit :

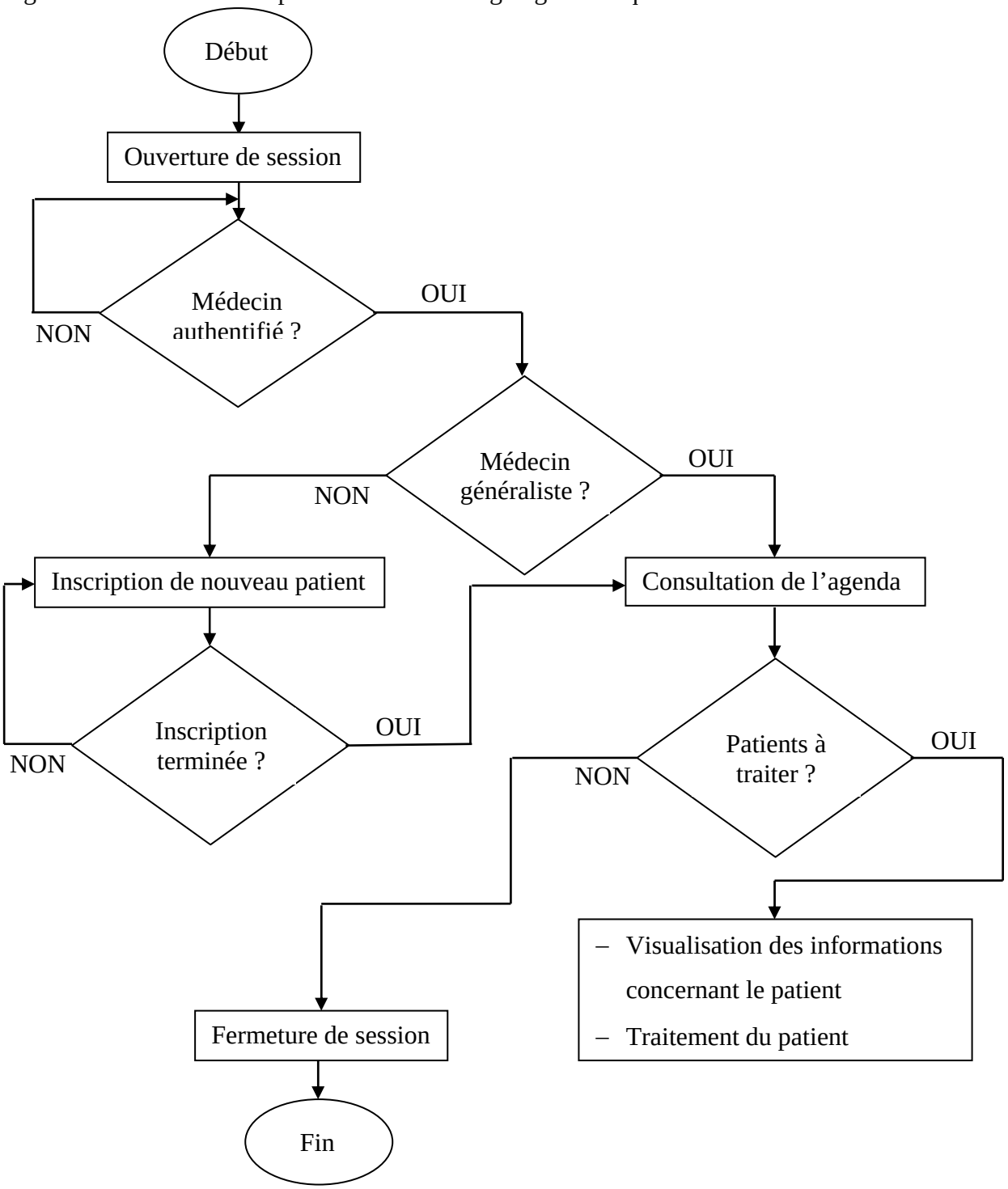

Figure 4.06 : Organigramme de l’application côté client

4.5. Description et présentation de l'application :

Ce paragraphe explicite la description et la manipulation effective de l'application. Il sera question d'interface utilisateur qui comprendra les interactions accessibles à l'utilisateur, à savoir l'authentification, pour les médecins déjà inscrits dans la base de données du personnel de la clinique (ou de l'hôpital), l'accès à l'inscription de nouveaux patients, la consultation d'agenda et de la liste des médecins dans la clinique (ou l'hôpital) pour les médecins authentifiés.

Avant toute manipulation, il faut ouvrir une session dans le réseau de la clinique (ou de l'hôpital). Nous utiliserons un navigateur web (Mozilla Firefox par exemple) pour ouvrir une session dans ce réseau.

Pour notre simulation, nous suivrons le cas d'un patient victime d'un accident depuis son arrivée à la clinique (ou l'hôpital) jusqu'à sa sortie.

A chaque ouverture de session, la page d'accueil suivante s'ouvrira.

Bienvenue sur le site de gestion des dossiers patients de la clinique. Ce site a été fait dans le but de faciliter le travail du personnel de la clinique dans la gestion des dossiers patients de la clinique. Les dossiers patients seront stockés dans une base de données centralisée sur un serveur central.

Avant d'effectuer une quelconque opération, veuillez d'abord vous authentifier en cliquant sur le bouton login. Ceci dans le but de protéger les dossiers confidentiels de la clinique.

Après avoir effectué l'authentification, vous pouvez maintenant faire les opérations dont vous avez le privilège d'effectuer.

Pour inscrire un nouveau patient, cliquer sur le bouton Enregistrement. Veuillez remplir le formulaire de nouveau patient et cliquer sur le bouton Enregistrement.

Pour consulter votre agenda journalier, cliquer sur le bouton Agenda. Vous y trouverez la liste des patients dont vous devez traiter ou consulter.

Pour visualiser la liste des médecins et des spécialités, cliquer sur le bouton Docteurs. Vous y trouverez la liste des médecins travaillant dans la clinique ainsi que la liste des spécialités disponible dans la clinique.

Note : Dans le cas général, les médecins généralistes effectuent l'inscription de nouveau patient dans une clinique. De ce fait, seuls les médecins généralistes effectuent cette opération dans notre site.

Figure 4.07 : Page d'accueil

4.5.1. L'authentification :

La mise en commun d'une ressource requiert la restriction de l'accès à cette ressource. En effet pour protéger l'application propre à la clinique (ou à l'hôpital) des piratages, il est d'usage de restreindre l'accès aux ressources sensibles. On fait donc appel à un SGBD qui stocke la liste des médecins pouvant accéder à la ressource.

Chaque médecin qui veut accéder à la ressource doit s'authentifier par rapport à la liste des médecins de la base de données, l'accès est permis dans le cas où le médecin y est identifié sinon il est redirigé vers la page d'authentification.

La page d'authentification se présente comme suit :

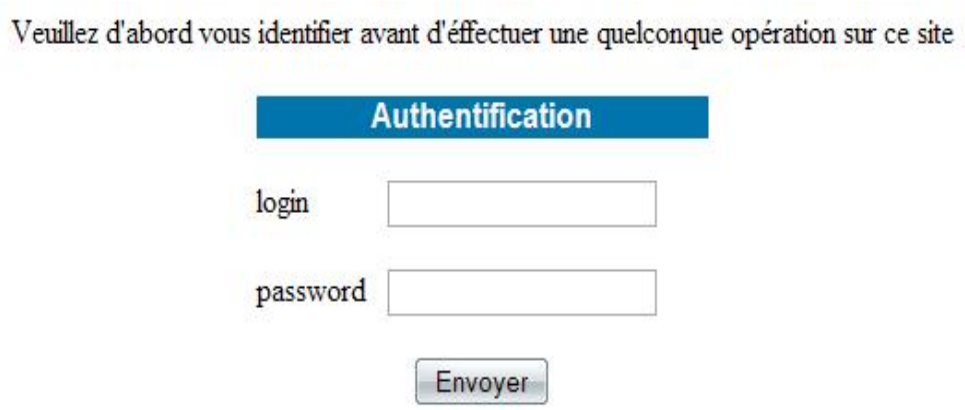

Figure 4.08 : Page d'authentification

Après avoir été authentifié, le médecin pourra accéder au formulaire d'inscription de nouveaux patients, ou consulter son agenda ou la liste des médecins inscrits dans la base de données du personnel ainsi que leurs spécialités respectives.

4.5.2. Le formulaire d'inscription de nouveau patient :

A partir de ce formulaire, le médecin pourra inscrire le patient dans la base de données patient de la clinique et aussi rendre un premier diagnostic après avoir effectué une consultation.

Deux cas peuvent se présenter :

- Premier cas : le patient rentre directement chez lui après avoir reçu les soins convenables à sa maladie. Il sera inscrit dans la base de données patient de la clinique en tant que patient traité mais il ne figurera dans aucun agenda des médecins.
- Deuxième cas : le patient devra rester dans la clinique car il devra subir plusieurs traitements pour soigner sa maladie. Il sera inscrit dans la base de données patient de la clinique en tant que patient traité et il sera présent dans les agendas journaliers des médecins le traitant. Et lorsque son traitement est terminé et qu'il est autorisé à rentrer, son

dossier sera effacé dans tous les agendas des médecins mais figurera toujours dans la base de données patient en tant qu'archives de la clinique.

Remarque : Dans notre cas, seul le médecin généraliste pourra accéder au formulaire d'inscription de nouveaux patients car c'est lui en général qui prend en charge les nouveaux patients avant de les trier suivant leurs maladies.

Le formulaire d'inscription de nouveaux patients se présente comme suit :

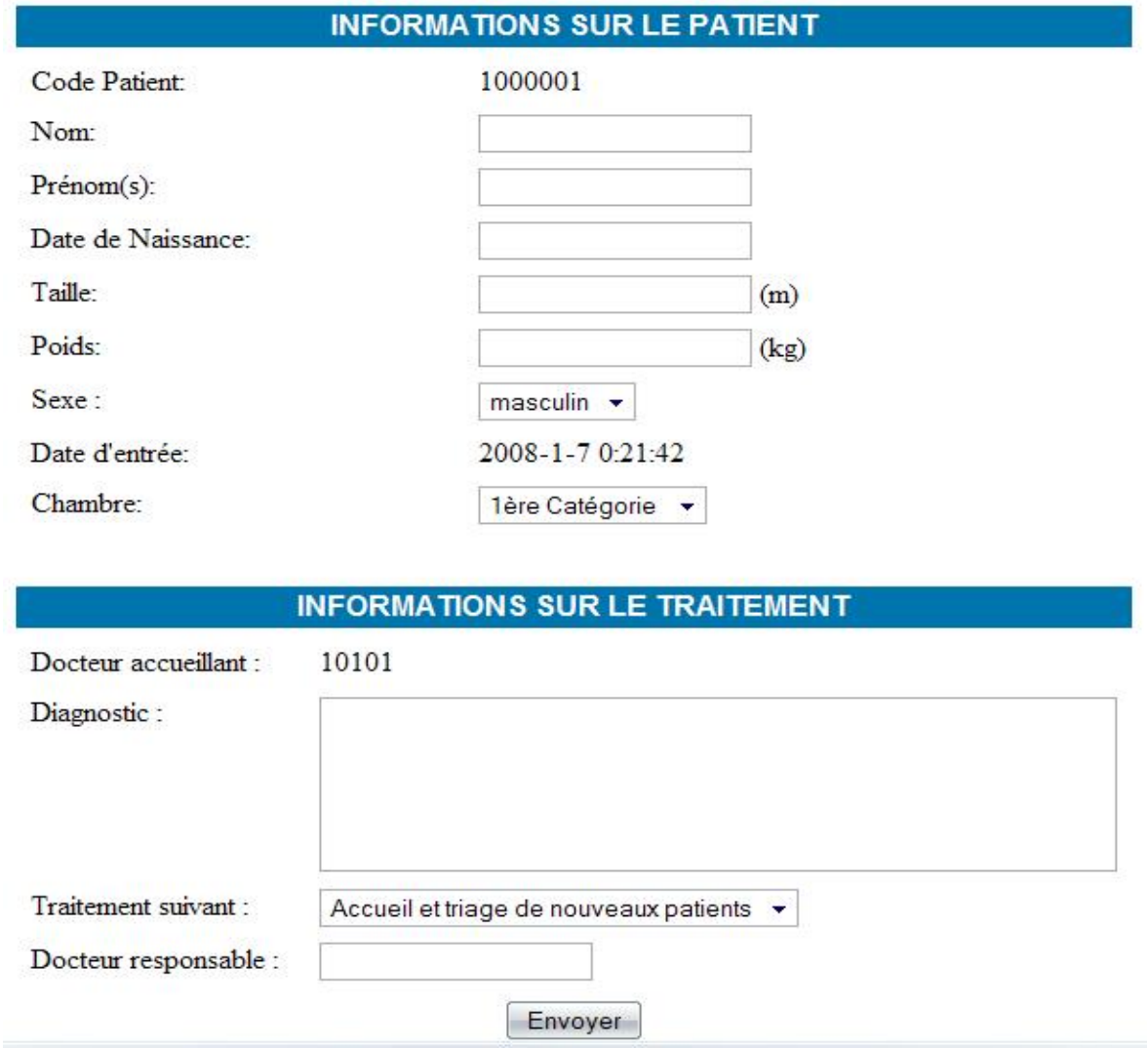

Figure 4.09 : Formulaire d'inscription de nouveaux patients

4.5.3. L'agenda :

Les médecins authentifiés pourront consulter la liste des patients qu'ils devront traités ou des patients dont ils devront suivre l'évolution de leurs états de santé.

En consultant son agenda, un médecin pourra visualiser la liste des patients qu'il doit traiter ou consulter. Et en choisissant un patient dans la liste, il pourra choisir de visualiser les informations

concernant le patient ainsi que les diagnostics faits par d'autres médecins qui l'ont traité auparavant, ou de commencer le traitement du patient qu'il devra effectuer et ainsi rendre son diagnostic.

Remarque : Seuls les patients dont il devra traiter que le médecin verra sur son agenda. Il ne peut en aucun cas visualiser ou traiter les patients des autres médecins sauf autorisation de ceux-ci.

Figure 4.10 : Agenda d'un médecin

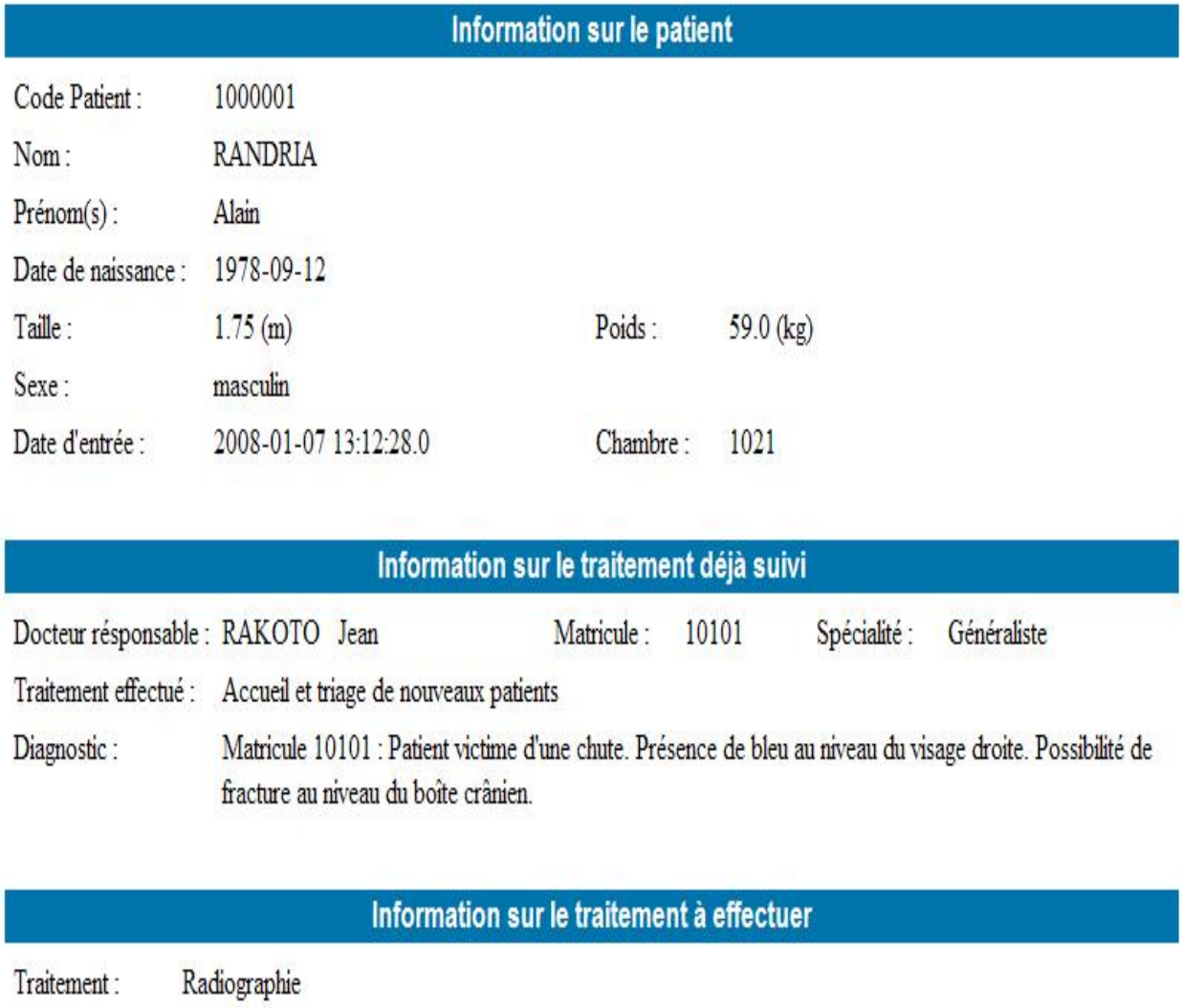

Figure 4.11 : Visualisation des informations concernant le patient choisi

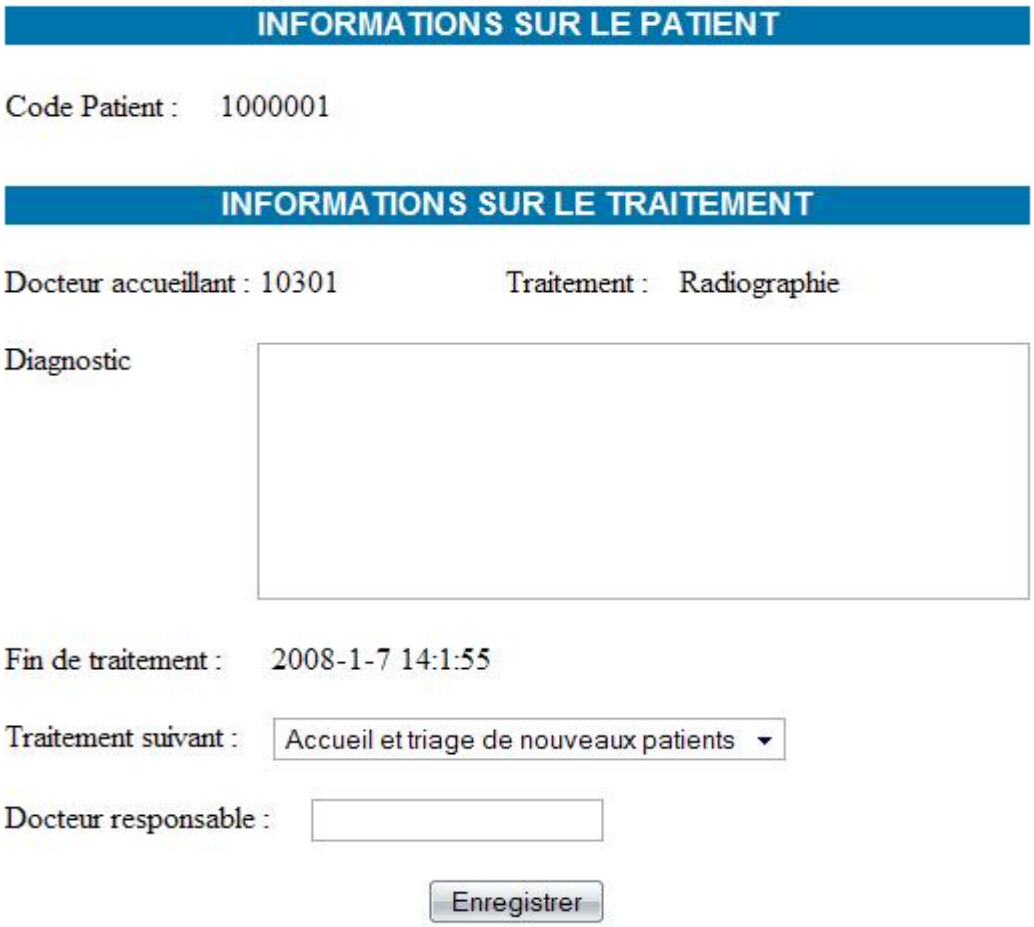

Figure 4.12 : Fiche de traitement du patient choisi

4.5.4. La liste des médecins :

Les médecins accueillant les nouveaux patients ou traitants les patients actuels pourront consulter la liste des médecins ainsi que leurs spécialités respectives afin de les aider à diriger ces patients pour leurs prochains traitements.

Tout médecin authentifié et ayant ouvert une session sur le réseau de la clinique (ou de l'hôpital) pourra visualiser cette liste.

Liste des médecins

MATRICULE	NOM	PRENOM
10101	RAKOTO	Jean
10102	RANDRIA	José
10201	RAVALISOA	Agnès
10202	RAVELOSON	Roger
10301	ANDRIANTSEHENO	Mamy
10302	RAKOTOMALALA	Lalaina
10401	ROBINSON	Tahina
10501	RAHARIMANANA	Nirina
10601	RAZAFIMAHANDRY	Claude
10602	RAHARIVELO	Liva
10701	RAMANAMPAMONJY	Rado
10801	RAJAONARISON	Misa
10802	RANDRIAMARO	Herizo
10901	RANTOMALALA	Hary
11001	ANDRIANJATOVO	Annick
11002	RABARIJAONA	Hery
11101	RAHARISON	Gabrielle
11201	RAKOTOMANANA	Solofo

Liste des spécialités

CODE SPECIALITE	NOM SPECIALITE
101	Généraliste
102	Chirurgien
103	Radiologue
104	Pédiatre
105	Pneumologue
106	Traumatologue
107	Hépato-gastro-entéro
108	Scanner
109	Ophtalomologue
110	Anesthésiste-réanimateur
111	Gynécologue
112	Cardiologue

Figure 4.13 : Liste des médecins et spécialités

4.5.5. La déconnexion :

Enfin, après avoir effectué les traitements de tous les patients figurant sur son agenda, le médecin devra fermer sa session du réseau de la clinique (ou de l'hôpital) pour que d'autres utilisateurs malveillants ne puissent pas consulter les données confidentielles de la clinique (ou de l'hôpital) et d'en faire un usage malveillant. Ceci est donc une mesure de sécurité pour la clinique afin de préserver ses données confidentielles des piratages.

Chaque médecin traitant un patient suit ses directives jusqu'à la sortie du patient.

CONCLUSION GENERALE

L'IMS vient du monde des mobiles, mais les réseaux fixes ont besoin de l'IMS. L'IMS pourrait permettre de mieux gérer les réseaux mobiles, compte tenu de la pénurie en ressources en débits dans les cellules (le débit disponible y est divisé par le nombre d'utilisateurs actifs).

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

L'IMS présente de nombreux avantages. Le mode session est la grande force d'IMS. IMS fournit une couche intermédiaire au cœur des réseaux pour passer du mode appel classique (circuit) au mode session. Autrement dit, il permet d'ouvrir plusieurs sessions au cours d'une même communication. Ceci permettra de mélanger les composants multimédias, par exemple rajouter une session de chat à celle de la vidéo, envoyer une photo pendant la conversation, etc.

L'IMS permet de disposer d'une plateforme unique capable de gérer un grand nombre d'applications multimédia (dont la voix sur IP) avec une très bonne qualité de services sur les réseaux de circuits et de paquets, et entre réseaux fixes et mobiles. L'IMS est un Internet amélioré qui permet la convergence de réseaux associés. La construction de nouvelles applications est facile et immédiate.

Malgré ces nombreux avantages, l'IMS présente aussi des inconvénients. Il faut parvenir à créer des applications qui ne nécessitent pas de manipulations complexes sur les claviers des terminaux. L'IMS, résultant de la conjonction d'un grand nombre d'éléments à intégrer, suscite des inquiétudes quant aux coûts et à la fiabilité globale. L'adaptation de l'IMS à l'accès fixe est coûteuse.

Pour notre part, ce travail nous a permis d'avoir des notions sur les principes de l'IMS, les différents avantages que l'on peut obtenir de son utilisation sans pour autant minimiser ses inconvénients. Dans la partie pratique du mémoire, nous avons vu la facilité de la mise en œuvre des services personnalisés nous permettant d'avoir une idée sur les avantages des réseaux opérant sous IP. Une pratique toutefois limitée dans son utilisation sur un réseau local. Cette pratique nous a aussi permis de développer notre connaissance sur le langage de programmation Java.

Nous souhaitons vivement que cette étude que nous venons d'aborder soit approfondie et améliorée. Un exemple d'amélioration est l'élargissement de l'application de gestion des dossiers patients sur un ensemble de cliniques, hôpitaux, ou centres de santé pour permettre la facilitation

de traitement des patients nécessitant des soins extrêmement rigoureux qui ne sont possibles que dans des hôpitaux ou cliniques sophistiqués.

Nous n’avons pas de prétention à l’exhaustivité ou à la perfection, mais vos remarques et suggestions nous seront les bienvenues.

ANNEXE 1 : LE MODELE OSI [1] [2] [3] [4]

Le modèle OSI (Open System Interconnection) a été développé en 1978 par l'ISO (International Organization Standardization) afin que soit défini un standard utilisé dans le développement de système ouvert. L'ISO a du réagir face à la croissance des réseaux. En effet, plus les réseaux augmentaient et plus des techniques propriétaires étaient utilisées par les différentes sociétés qui s'en servaient. Cela a posé très vite un problème lorsque deux de ces réseaux propriétaires voulaient communiquer entre eux, c'était tout bonnement impossible puisque les langages étaient incompatibles et les réseaux ne se comprenaient pas.

L'ISO a donc mis au point des règles qui assurent une compatibilité entre les réseaux, que la communication entre tous les réseaux soit possible. Ce modèle s'est très vite imposé comme le plus utilisé bien qu'il en existe d'autres.

Ce modèle OSI présente pas mal d'avantages : il est plus simple pour comprendre l'acheminement informations, il rend les interfaces compatibles, il permet d'évoluer, simplifie la transmission des connaissances réseau ainsi que le dépannage réseau, puisqu'on dit usuellement qu'il faut toujours commencer par la première couche et remonter vers la dernière pour dépanner efficacement un réseau.

En effet, si vous commencez à chercher un problème réseau dans un programme, alors que c'est la prise réseau qui n'est pas branchée derrière le PC, vous risquez de chercher longtemps dans le vide.

Voici les différentes couches du modèle OSI, qui vont du média physique (carte réseau par exemple sur un PC) aux applications :

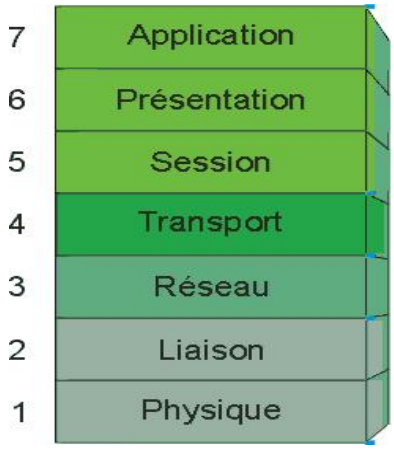

Figure A1.1 : Les différentes couches du modèle OSI

La couche Physique

La couche Physique définit les interfaces mécanique et électrique pour l'échange des signaux d'informations sur les médias physiques. Elle est responsable de la transmission des bits de données sur le média physique en utilisant le signal approprié compatible avec les périphériques de communication. La couche Physique reçoit aussi des signaux et les convertit en bits de données qu'elle délivre à la couche Liaison de données. Elle gère le type de transmission (synchrone ou asynchrone) et effectue la modulation et démodulation des signaux.

L'élément d'information dans cette couche est le bit.

La couche Liaison de données

La couche Liaison de données prend les données de la couche Physique et fournit ses services à la couche Réseau. Elle contrôle l'établissement, le maintien et la libération de la liaison logique sur le réseau. Elle définit les règles d'émission et de réception des blocs d'information à travers la connexion physique des deux systèmes. Elle doit transmettre les données sans erreur et déterminer la méthode d'accès au support. Elle est donc la première couche qui gère les erreurs de transmission.

L'élément d'information dans cette couche est la trame.

Exemple de protocole utilisé dans cette couche : HDLC (High level Data Link Protocol).

La couche Réseau

La couche Réseau est chargée de l'acheminement des données sur l'ensemble du réseau en utilisant les informations d'adressage. Elle gère aussi les connexions entre les nœuds du réseau, la façon de router les paquets de données entre ces nœuds (choix des trajets), les multiplexages et le contrôle de flux entre tous les nœuds du réseau.

L'élément d'information dans cette couche est le paquet.

Exemples de protocole utilisé dans cette couche : IP (Internet Protocol), X.25.

La couche Transport

La couche Transport est une couche charnière (ou pivot) entre les trois (03) couches basses appelées couches de communication et les trois (03) couches hautes appelées couches de applications.

La couche Transport fournit un service de transport des informations de bout en bout transparent pour l'utilisateur. Elle assure la fiabilité et le contrôle des transmissions et est responsable de la création de plusieurs connexions logiques par multiplexage sur la même connexion réseau (le multiplexage se produit quand plusieurs connexions logiques partagent la même connexion physique).

L'élément d'information dans cette couche est le message.

Exemples de protocole utilisé dans cette couche : TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

La couche Session

La couche Session gère les sessions entre les applications coopérantes (elle permet l'ouverture et la fermeture d'une session de travail entre deux (02) systèmes distants). Elle assure la synchronisation et le contrôle du dialogue, la gestion des jetons (essentiel à la détermination du côté qui peut lancer une opération) et la gestion d'activité (une activité consiste en une ou plusieurs unités de dialogue).

On décide dans cette couche le mode de transmission utilisé : simplex, half duplex, full duplex.

La couche Présentation

La couche Présentation représente les données de façon compréhensible (format, lisibilité, etc) pour que deux systèmes puissent se comprendre. Elle est donc chargée de transcrire les données dans syntaxe compréhensible par les systèmes en relation. Elle effectue aussi la compression, le cryptage et le décryptage des données.

La couche Application

La couche Application fournit les protocoles et les fonctions nécessaires aux applications utilisateurs qui doivent accomplir des taches de communication. Elle fournit aussi des services utilisables pour les applications installées sur le réseau.

Exemples de protocole utilisé dans cette couche : FTP (File Transfer Protocol), http (Hypertext Transfert Protocol), TELNET (Terminal Emulator Protocol), DNS, SMTP.

La figure suivante représente la correspondance entre le modèle OSI et le modèle DOD utilisé par l'architecture TCP/IP :

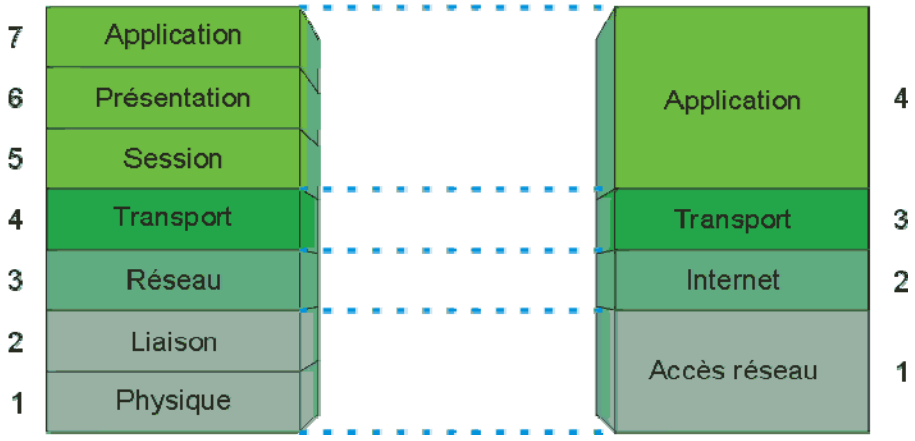

Figure A1.2 : Correspondance des couches du modèle OSI et du modèle DOD

ANNEXE 2 : IPv6 (RFC 1752) [5]

La nouvelle version du protocole IP s'inscrit comme l'évolution naturelle et normale du protocole IP. Cette évolution supportée par les grands constructeurs se fera progressivement, ceci pour supplanter les faiblesses d'IPv4. IPv6 est conçu pour fonctionner aussi bien sur des réseaux à très hauts débits comme ATM que sur des réseaux à faible bande passante tels que les réseaux sans fils.

Principales Caractéristiques

Bien que représentant une très forte évolution par rapport à la version précédente, les principales fonctionnalités d'IPv4 sont conservées. Ainsi huit (08) changements majeurs sont à prendre en compte :

- Des possibilités étendues d'adressage et de routage : la taille de l'adresse IP augmente de 32 à 128 bits afin de supporter un plus grand nombre de nœuds adressables. Quand les réfrigérateurs seront capables de commander les produits manquants directement sur Internet, il sera nécessaire d'avoir une possibilité d'adressage conséquente.
- Un format d'en-tête simplifié : l'en-tête IPv6 est simplifié et réduit à un traitement commun dans tous les routeurs ce qui diminue donc le coût de traitement.
- Des capacités d'extension des en-têtes et des options : les options sont rangées dans des en-têtes supplémentaires situés entre l'en-tête IPv6 et l'en-tête du paquet de transport (T-PDU, Transport Protocol Data Unit).
- Des droits d'authentification et de confidentialité : IPv6 intègre des extensions permettant l'authentification des usagers et l'intégrité des données grâce à des outils de cryptographie.
- Des potentialités d'auto-configuration : IPv6 dispose de plusieurs formes d'auto-configuration comme la configuration « plug and play » d'adresses de nœuds sur un réseau isolé grâce aux caractéristiques offertes par DHCP.
- Des moyens pour le « Source Route » : IPv6 intègre une fonction étendue de source routing grâce à SDRP afin d'étendre le routage à des routes inter-domaine et intra-domaine.
- Une transition d'IPv4 à IPv6 simple et flexible : la transition d'IPv4 à IPv6 répond à quatre objectifs essentiels :
  - ❖ un besoin de modernisation,
  - ❖ un besoin de redéploiement,
  - ❖ un adressage facile,

- une diminution du coût de démarrage.

- Des possibilités de qualité de service : l'introduction de flux étiquetés (avec des priorités), les services de contraintes « temps réel » sont de nouveaux éléments rendant possible la qualité de service.

Après cette énumération succincte des principales caractéristiques d'IPv6, il convient de reprendre un certain nombre de ces éléments afin d'apporter quelques éclaircissements sur les nouvelles possibilités d'IPv6.

Format de l'en-tête (40 octets)

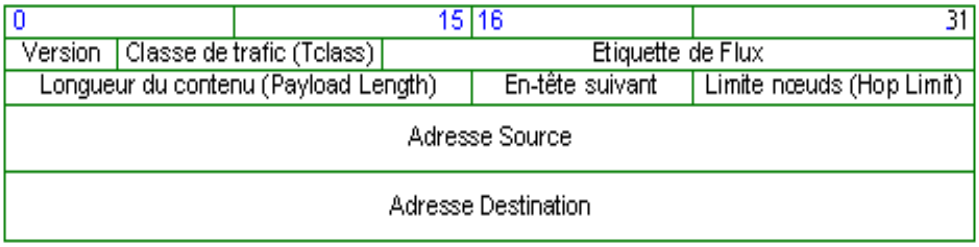

Figure A2.1 : En-tête IP V6

Le tableau suivant montre la description de l'en-tête IPv6

Champ	**Nombre de bits**	**Fonction**
Version	4	Définit le numéro de version du protocole IP : IP v6 est la version 6
Classe de trafic	8	Indice permettant d'affecter des priorités
Étiquette de flux	20	Peut être utilisé par une station pour « marquer » certains paquets afin qu'ils suivent un routage (service) particulier dans un réseau. Par exemple un service de qualité sans défaut ou un service « temps réel »
Longueur du contenu	16	Représente la longueur des données après l'en-tête IPv6
En-tête suivant	8	Identifie l'en-tête suivant immédiatement l'en-tête IPv6 (idem IP v4)
Limite nœuds	8	Utilisé pour détruire les paquets qui pourraient rester dans le réseau à la suite de boucles dues à la table de routage, ce champ est décrémenté d'une unité à chaque nœud qui retransmet le paquet (équivalent de Time to live d'IPv4)
Adresse source	128	Adresse de l'émetteur du datagramme
Adresse destination	128	Adresse du destinataire du paquet. Il est possible que l'adresse ne soit pas celle du destinataire finale si une option de routage est présente.

Tableau A2.1: Description de l'en-tête IP v6

ANNEXE 3 : CODE JSP DE L'AUTHENTIFICATION

```
<%@ page contentType="text/html; charset=iso-8859-1" language="java" import="java.sql.*"
errorPage="" %>
<%@ include file="Connections/connect.jsp" %>
<% // *** Validate request to log in to this site.
String MM_LoginAction = request.getRequestURI();
if (request.getQueryString() != null && request.getQueryString().length() > 0)
{       String queryString = request.getQueryString();
        String tempStr = "";
         for (int i=0; i < queryString.length(); i++)
        {       if (queryString.charAt(i) == '<') tempStr = tempStr + "&lt;";
                else if (queryString.charAt(i) == '>') tempStr = tempStr + "&gt;";
                else if (queryString.charAt(i) == "") tempStr = tempStr +  "&quot;";
                else tempStr = tempStr + queryString.charAt(i);
        }
        MM_LoginAction += "?" + tempStr;
}
String MM_valUsername=request.getParameter("login");
if (MM_valUsername != null)
{       String MM_fldUserAuthorization="CODESPEC";
        String MM_redirectLoginSuccess="index.jsp";
        String MM_redirectLoginFailed="login.jsp";
        String MM_redirectLogin=MM_redirectLoginFailed;
        Driver MM_driverUser = (Driver)Class.forName(MM_connect_DRIVER).newInstance();
        Connection MM_connUser =
        DriverManager.getConnection(MM_connect_STRING,MM_connect_USERNAME,MM_
        connect_PASSWORD);
        String MM_pSQL = "SELECT NOMMED, MATRICULE";
        if (!MM_fldUserAuthorization.equals("")) MM_pSQL += "," +
        MM_fldUserAuthorization;
```

```
        MM_pSQL += " FROM memoire.medecin WHERE NOMMED=\'" +
        MM_valUsername.replace('\'', ' ') + "\' AND MATRICULE=\'" +
        request.getParameter("password").toString().replace('\'', ' ') + "\'";
        PreparedStatement MM_statementUser = MM_connUser.prepareStatement(MM_pSQL);
        ResultSet MM_rsUser = MM_statementUser.executeQuery();
         boolean MM_rsUser_isNotEmpty = MM_rsUser.next();
         if (MM_rsUser_isNotEmpty)
        {          // username and password match - this is a valid user
                   session.putValue("MM_Username", MM_valUsername);
                  session.putValue("MM_Matricule",request.getParameter("password"));
                  if (!MM_fldUserAuthorization.equals(""))
                  {         session.putValue("MM_UserAuthorization",
                            MM_rsUser.getString(MM_fldUserAuthorization).trim());
                  } else
                  {session.putValue("MM_UserAuthorization", "");}
                  if ((request.getParameter("accessdenied") != null) && false)
                  {MM_redirectLoginSuccess = request.getParameter("accessdenied");}
                  MM_redirectLogin=MM_redirectLoginSuccess;
        }
        MM_rsUser.close();
        MM_connUser.close();
        response.sendRedirect(response.encodeRedirectURL(MM_redirectLogin));
        return;
}%>
```

ANNEXE 4 : CODE JSP DU FICHE DE TRAITEMENT DU PATIENT CHOISI

```
<%@ page contentType="text/html; charset=iso-8859-1" language="java" import="java.sql.*"
import="java.util.Calendar" errorPage="" %>
<%@ include file="Connections/connect.jsp" %>
<%      String mat_act=request.getParameter("matricule_act");
String codpat=request.getParameter("patient_cod");
String trait_act=request.getParameter("traitact_cod"); %>
<% // *** Restrict Access To Page: Grant or deny access to this page
String MM_authorizedUsers="";
String MM_authFailedURL="login.jsp";
boolean MM_grantAccess=false;
if (session.getValue("MM_Username") != null &&
!session.getValue("MM_Username").equals("")){
  if (true || (session.getValue("MM_UserAuthorization")=="") ||
        (MM_authorizedUsers.indexOf((String)session.getValue("MM_UserAuthorization")) >=0))
{MM_grantAccess = true ;}
}
if (!MM_grantAccess) {
  String MM_qsChar = "?";
  if (MM_authFailedURL.indexOf("?") >= 0) MM_qsChar = "&";
  String MM_referrer = request.getRequestURI();
  if (request.getQueryString() != null) MM_referrer = MM_referrer + "?" +
request.getQueryString();
  MM_authFailedURL = MM_authFailedURL + MM_qsChar + "accessdenied=" +
java.net.URLEncoder.encode(MM_referrer);
  response.sendRedirect(response.encodeRedirectURL(MM_authFailedURL));
  return;
}%>
<% Driver DriverRecordset2 = (Driver)Class.forName(MM_connect_DRIVER).newInstance();
```

```
Connection ConnRecordset2 =
DriverManager.getConnection(MM_connect_STRING,MM_connect_USERNAME,MM_connect
_PASSWORD);
PreparedStatement StatementRecordset2 = ConnRecordset2.prepareStatement("SELECT * FROM
memoire.traitement");
ResultSet Recordset2 = StatementRecordset2.executeQuery();
boolean Recordset2_isEmpty = !Recordset2.next();
boolean Recordset2_hasData = !Recordset2_isEmpty;
Object Recordset2_data;
int Recordset2_numRows = 0;
Statement stmt = ConnRecordset2.createStatement(ResultSet.TYPE_SCROLL_SENSITIVE,
ResultSet.CONCUR_UPDATABLE);
ResultSet rs1 = stmt.executeQuery("SELECT * FROM memoire.agenda WHERE
CODEPATIENT ="+"\""+codpat+"\""+" AND matricule = "+"\""+mat_act+"\"");
rs1.first();
int patient_cod=rs1.getInt("CODEPATIENT");
String debut=rs1.getString("date_debut");
String diag_prec=rs1.getString("diagnostic");
ResultSet rs2 = stmt.executeQuery("SELECT NOMTRAITEMENT FROM memoire.traitement
WHERE CODETRAITEMENT ="+"\""+trait_act+"\"");
rs2.first();
String nomtrait=rs2.getString("NOMTRAITEMENT");
%>
 <% Calendar aCalendar=Calendar.getInstance(); %>
 <%PreparedStatement StatementRecordset1 = ConnRecordset2.prepareStatement("SELECT *
FROM memoire.medecin  where matricule="+session.getValue("MM_Matricule")+" ORDER BY
matricule");
ResultSet Recordset1 = StatementRecordset1.executeQuery();
boolean Recordset1_isEmpty = !Recordset1.next();
boolean Recordset1_hasData = !Recordset1_isEmpty;
Object Recordset1_data;
int Recordset1_numRows = 0;%>
```

BIBLIOGRAPHIE

[1] G.Pujolle, *Les Réseaux*, Eyrolles : Paris, 2003

[2] Y. Duchemin, *TCP/IP*, version 1.0, publié en Avril 2000

[3] A. Ratsimbazafy, *Technologie des réseaux*, Cours 3ème année, Dép.Tél-E.S.P.A., A.U. : 2004-2005

[4] L.E. Randriarijaona, *Réseaux TCP/IP*, Cours 4ème année, Dép.Tél.-E.S.P.A., A.U. : 2005-2006

[5] http://www.viageni.qc.ca/en/ipv6forum.pdf

[6] http://gregory.kokanosky.free.fr/files/ip.pdf

[7] http://www.ibiblio.org/pub/Linux/docs/HOWTO/translations/fr/pdf/IP-Subnetworking.pdf

[8] http://www.laissus.fr/cours/node9.html

[9] P. Picard, *Comprendre l'UMTS pour s'y préparer*, publié en Octobre 2001

[10] J. Sanchez, *UMTS*, Hermès : 2004

[11] http://www.petrusrex.com/Divers/UMTS/index.html

[12] http://users.info.unicaen.fr/mguillet/Expose_UMTS/src/CCreseau.html

[13] http://jtr2002.unilim.fr/fichiers-presentation/umts-limoges.pdf

[14] http://www-lor.intevry;fr/~vincent/expArad/arad2004/umts

[15] http://www2.univ_reunion.fr/panelli/enseignement/Formations/RapportMINF005/COUFFINHAL_SYNAPAYEL_MINF.pdf

[16] http://fr.computers.toshiba_europe.com/Contents/Toshiba_fr/FR/WHITEPAPER/files/whitepaper_180701_gc2_umts.pdf

[17] X. Lagrange, *Principes et évolutions de l'UMTS*, Hermès : 2005

[18] P. Lescuyer, *Réseaux 3G : Principes, architectures et services de l'UMTS*, Dunod : Paris, 2006

[19] M.A. Rakotomalala, *Réseaux Intelligents & NGN*, Cours 5ème année, Dép.Tél.-E.S.P.A., A.U. :2006-2007

[20] http://www.multimediapromotion.com/r_tutoriels/NGN_EFFORT.pdf

[21] http://www.mobilein.com/what_is_IMS.htm

[22] http://www.multimediapromotion.com/r_tutoriels/IMS_EFFORT.pdf

[23] http://fr.wikipedia.org/wiki/IP_Multimedia_Subsystem

[24] http://www.audiocodes.com/objects/IMS_application_note.pdf

[25] http://phoenix.labri.fr/documentation/sip/Documentation/Papers/Internet_Telephony/Presentation/chassagne.pdf

[26] J. M. Doudoux, *Développons en Java*, Version 0.90 du 11 Septembre 2006

[27] L.E. Randriarijaona, *Programmation Orientée Objet*, Cours 3ème année, Dép.Tél.-E.S.P.A., A.U. : 2004-2005

[28] http://tecfa.unige.ch/guides/tie/pdf/files/java-mysql.pdf

[29] http://www.mysql.com

RENSEIGNEMENTS

Nom : RABOANARIVOLA

Prénoms : Tojo Nirina

Adresse de l'auteur : Lot IVL 84 Anosivavaka Ambohimanarina ANTANANARIVO 101

Tél : 0324177520

E-mail : tojoraboanarivola@yahoo.fr

Titre du mémoire :

« IMS - IP MULTIMEDIA SUBSYSTEM : EVOLUTION VERS LE TOUT-IP »

Nombre de pages : 76

Nombre de tableaux : 08

Nombre de figures : 34

Mots clés : IP, adresses IP, datagrammes IP, RIP, OSPF, UMTS, architecture UMTS, UTRAN, réseau cœur, IMS, principes de l'IMS, architecture IMS, SIP, SDP, RTP/RTCP, NGN.

Directeur de mémoire : Monsieur RATSIHOARANA Constant.

RESUME

L'évolution des réseaux de télécommunication, surtout des réseaux cellulaires, résulte des besoins grandissants en débit et en bande passante essentiels pour faciliter la création de services intégrant le multimédia et pour transmettre ces services. Ce qui demande un réseau capable de satisfaire ces besoins et de permettre ainsi le transport d'une grande quantité d'informations en un temps assez court. Dans cet ouvrage, une solution proposée est l'utilisation et l'intégration d'un sous système multimédia : l'IMS dans un réseau existant : l'UMTS pour permettre plus tard la convergence vers le réseau Tout-IP qui est un réseau capable de transporter beaucoup d'informations en un temps suffisamment court et permettre la création et la transmission des services incluant le multimédia. La bonne compréhension de l'architecture et des principes de ce réseau nous a permis de développer une application qui suit ces principes et respectant cette architecture.

ABSTRACT

The evolution of the telecommunication networks, especially of the cellular networks, result from the growing needs in debit and in a group passing essential to facilitate the creation of services integrating the multimedia and to transmit these services. What asks a network capable to satisfy these needs and to permit the transportation of a great deal of information thus in one short enough time. In this work, a proposed solution is use and the integration of one coins multimedia system: the IMS in an existing network: the UMTS to permit the convergence later toward the All - IP network that is a network capable to transport a lot of information in one sufficiently short time and to permit the creation and the transmission of the services including the multimedia. The good understanding of the architecture and the principles of this network permitted us to develop an application that follows these principles and respecting this architecture.