



Université Abou Bekr Belkaid
Tlemcen Algérie



جامعة أبي بكر بلقايد

تلمسان الجزائر



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

Mémoire

A L'UNIVERSITÉ DE TLEMEN
FACULTÉ DE TECHNOLOGIE

DÉPARTEMENT DE GÉNIE ÉLECTRIQUE ET D'ELECTRONIQUE

Pour l'obtention du diplôme de

MASTER

Spécialité : " Réseaux et Systems de télécommunication "

THEME

Application mobile de la voIP sur un réseau Wifi

Présenté par :

- **ABDELLAOUI MOHAMMED EL AMIN**
- **BENHAMOU ABOUBAKR**

Soutenu en Juin 2014 devant le Jury :

Mr M.I. Smahi	Maitre Assistant class A à l'Université de Tlemcen	Président
Mr O. Bekkadour	Maitre Assistant class A à EPST de Tlemcen	Examineur
Mr F.T. Bendimerad	Professeur à l'université de Tlemcen	Encadreur
Mr G. Abdellaoui	Maitre Assistant class A à EPST de Tlemcen	Co-Encadreur

Dédicaces

La vie n'est qu'un éclair,

Et un jour de réussite est un jour très cher.

A mon cher père Lakhder,
et ma chère mère Yamna ,

Pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance.

Et pour leurs patiences et leurs sacrifices.

A mes chers frères : Fouzi, Abdelhalim, Ismail ;

A mes chères sœurs : Nadia, Souhila, Amina ;

A les petits enfants Nihal, Zineb, Guizlene, Asma et Islam ;

A tous mes proches ;

A mon ami Boukli Hacene Tani Omar (رحمه الله);

A tous ceux qui m'aiment ;

A tous mes ami (e) s;

A tous ceux que j'aime.

Je dédie ce Mémoire.

Abdellaoui Mohammed El amin

Dédicaces

La vie n'est qu'un éclair,

Et un jour de réussite est un jour très cher.

A mon cher père Said,
et ma chère mère Radia,

Pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance.

Et pour leurs patiences et leurs sacrifices.

A mes chers frères : Read, Ibrahim;

A mes chères sœurs : Hanan ;

A les petits enfants Khadija, Fethi et Cherifa ;

A tous mes proches ;

A mon ami Boukli Hacen Tani Omar (رحمه الله);

A tous ceux qui m'aiment ;

A tous mes ami (e) s;

A tous ceux que j'aime.

Je dédie ce Mémoire.

❧ *BENHAMOU Aboubakr* ❧

Remerciements

Nous remercions tout d'abord le Dieu Tout Puissant de nous avoir armés de force et de courage pour mener à terme ce projet.

C'est avec un grand plaisir que nous réservons cette page en signe de gratitude et de profonde reconnaissance à tous ceux qui nous aidés de près ou de loin à la réalisation de ce travail. Nous tenons à exprimer nos sincères gratitudes et respects à nos encadreurs Mr **ABDELAOUI Ghouti** Maîtres-assistants Classe A ,a avoir permis de bénéficier de son grand savoir dans la matière, pour sa pédagogie, ses compétences, sa modestie et son aide précieuse tout au long de ce projet même pendant les moments les plus difficiles. Vraiment merci pour une qualité d'encadrement si sérieuse et si consistante.

Et Mr le Professeur **Fathi Tarek BENDIMERADE**, responsable du laboratoire de Télécommunications de Tlemcen (**LTT**), Pour leur encouragements et les précieux conseils qu'il a cessé de nous prodiguer tout au long de ce projet. Nous profitons de cette occasion pour remercier tous les enseignants de l'université de Tlemcen généralement et de spécialité RST spécialement, pour leurs aides considérables et leurs orientations. Enfin nos meilleurs et vifs remerciements s'adressent aux membres du jury pour avoir accepté d'évaluer ce projet.

TABLE DES MATIÈRES

TABLE DES MATIÈRES	i
LISTE DES FIGURES.....	vii
LISTE DES TABLEAUX	viii
LISTE DES ACRONYMES	ix
INTRODUCTION GÉNÉRALE	

CHAPITRE I : Généralités sur les réseaux informatiques

Introduction	1
I.1 Intérêts d'un réseau	1
I.2 Définition d'un réseau informatique	2
I.3 Les différents types des réseaux	2
I.3.1 Les PANs	2
I.3.2 Les LANs	3
I.3.3 Les MANs	3
I.3.4 Les WANs	3
I.4 Les différentes catégories des réseaux	4
I.4.1 Le réseau (Peer to Peer) P2P	4
I.4.2 Le réseau Server/Client	4
I.5 Les topologies de réseaux	5
I.5.1 Topologie en bus	5
I.5.2 Topologie en étoile	6
I.5.3 Topologie en anneau.....	6
I.5.4 Topologie Point-à-Point	7
I.6 Les équipements réseau	7
I.6.1 Le répéteur (Repeater).....	8
I.6.2 Le pont (Bridge)	8
I.6.3 La passerelle (Gateway)	8
I.6.4 Le routeur (Router).....	8
I.6.5 Le concentrateur (HUB).....	8
I.6.6 Le commutateur (Switch).....	9
I.7 Les techniques de Commutation	9
I.7.1 La commutation de circuits	9
I.7.2 La commutation de message	9
I.7.3 La commutation de paquets	10
I.8 Techniques de transmission	10
I.8.1 Transmission série et parallèle	10

I.8.2 Sens de transmission	11
I.9 Supports et Equipements Réseaux Locaux	11
I.9.1 Supports de transmission	11
I.10 Architecture des réseaux	14
I.10.1 Le modèle de référence OSI de ISO	15
I.10.2 Modèle TCP/IP	16
I.10.2.1 Les protocoles de la couche application.....	17
I.10.2.2 Les protocoles de la couche transport	19
I.10.2.3 Les protocoles de la couche Internet	21
I.11 TCP/IP et le modèle OSI	22
Conclusion.....	23

CHAPITRE II :La voix sur IP

Introduction	24
II.2 Définitions	24
II.3 Définitions importantes	24
II.4 Le Réseau Téléphonique Commuté	25
II.4.1 -Principe du RTC	25
II.5 PABX et PABX-IP	25
II.5.1 -PABX Ou PBX ?	25
II.5.2 -Le PABX-IP.....	25
II.6 Architecture	26
II.6.1-Modèles du VOIP	26
II.7 Protocoles de transport utilisés en voix sur IP	27
II.8 La VOIP : avantages et inconvénients	28
II.8.1 Les avantages	28
II.8.2- Les inconvénients	30
II.9 Les différents éléments pouvant composés un réseau VoIP.....	30
II.9.1 Terminaux VOIP	30
II.9.2 Le serveur de communications.....	30
II.9.3 La passerelle (Gateway).....	30
II.9.4 Le routeur	31
II.9.5 Le Switch	31
II.9.6 Gatekeeper	31
II.9.7 Le MCU	31
II.9.8 Soft-Phone.....	31
II.10 Qualité de service de la voix sur IP.....	31
II.10.1 Qualité de codage	31
II.10.2 Délai d'acheminement	32
II.10.3 Gigue (jitter)	32
II.10.4 Perte des paquets	33
II.10.5 Echo	33
II.11 Les protocoles de la VOIP	33
II.11.1 Le Protocole H323.....	34
Introduction	34
II.11.1.1 Architecture et composants de la normeH323	34

II.11.1.2 Les avantages et inconvénients du protocole H.323	35
II.11.2 Protocole SIP	37
II.11.2.1 Historique	37
II.11.2.2 Architecture de SIP	40
II.11.2.3 La connexion à des réseaux non-IP	45
II.11.2.4 L'adressage SIP	46
II.11.2.5 Structure de message SIP	48
II.11.2.6 Les Requêtes SIP	51
II.11.2.7 Les réponses SIP	52
II.11.2.8 Scénarios de communication	53
II.11.2.9 Les modes de communication dans le protocole SIP	53
II.11.2.10 Avantage et inconvénients protocole SIP	58
II.12 Comparaison entre le protocole SIP et H.323	58
Conclusion	60

CHAPITRE III : Environnement matériel et logiciel

INTRODUCTION	61
III.1 Principes de base d'un PABX	61
III.2 Quelles sont les gammes ?	62
III.3 Les Principes De Bases	62
III.4 Asterisk	63
III.4.1 Historique	63
III.4.2 Définition	63
III.4.3 Rôle	64
III.4.4 Les principes de fonctionnement d'Asterisk	64
III.4.5 Protocole IAX/IAX2	65
III.4.6 Architecture d'asterisk	66
III.4.7 Les Composants d'asterisk	66
III.4.7.1 Le noyau	66
III.4.7.2 Les APIs	67
III.5 Java Media Framework	68
III.5.1 Les formats supportés par l'API	69
III.6 le logiciel X-Lite	70
III.6.1 Configuration du logiciel X-Lite	71
Conclusion	74

CHAPITRE IV :Application

Introduction	75
IV.1 Environnement de développement	75
Environnement matériel	75
Environnement logiciel	75
IV.2 Description du travail réalisé	76
IV.3 Méthode et application	76
IV.3 .1 Pourquoi Java comme langage de programmation ?	76
IV.3 .2 L'architecture	76
IV.3.3 Description du prototype de test	77
IV.3.3.1 Scénarios de communication	77
IV.3.4 Réalisation	78
Conclusion	83

CONCLUSION GÉNÉRALE

Bibliographie

LISTE DES FIGURES

Figure I.1 Classification de réseaux	2
Figure I.2 Topologie en bus	5
Figure I.3 Topologie en étoile	6
Figure I.4 Topologie en anneau	6
Figure I.5 Topologie point à point	7
Figure I.6 Les constituants du Câble STP	12
Figure I.7 Les constituants du Câble UPT	12
Figure 1.8 Le model OSI en détail	15
Figure I.9 La couche application	17
Figure I.10 La couche transport	18
Figure I.11 l'entête UDP	20
Figure I.12 La couche internet	21
Figure II.1 Le réseau téléphonique commuté RTC	25
Figure II.2 Le scénario PC à PC	26
Figure II.3 Le scénario PC à Téléphone	28
Figure II.4 Le scénario téléphone à téléphone	28
Figure II.5 Architecture d'un réseau VoIP	30
Figure II.6 Les composants de l'architecture H.323	34
Figure II.7 Architecture de SIP	41
Figure II.8 UAC et UAS	42
Figure II.9 Le trapèze SIP	45
Figure II.10 Syntaxe d'une adresse SIP	47
Figure II.11 Format générique d'un message SIP	49
Figure II.12 Les paquets de Mode Point à Point	54
Figure II.13 Les paquets de Mode diffusif	56
Figure III.1 PBX pour la gestion des appels	62
Figure III.2 Architecture interne d'Asterisk	66
Figure III.3 la décomposition de JMF	69
Figure III.4 Principales fonctionnalités	70

Figure III.5 Affichage des comptes SIP de X-Lite	72
Figure III.6 Menu de configuration SIP	73
Figure III.5 Interface de Logiciel X-lite.....	74
Figure IV.1 Architecture de notre application	76
Figure IV.2 Schéma descriptif d'une communication mobile en mode diffusif	77
Figure IV.3 Interface d'exécution le programme client A (Amin)	79
Figure IV.4 Interface d'un terminal Java.....	79
Figure IV.5 L'affichage des coordonnées de client A	80
Figure IV.6 L'affichage des coordonnées des clients A et B	80
Figure IV.7 Interface de l'appelant (client A).	81
Figure IV.8 Etablissement un appel (T.java, X-lite)	82
Figure IV.9 Etablissement un appel (T.java, T.java).....	82

LISTE DES TABLEAUX

Tableau I.1 Comparaison entre TCP/IP et modèle OSI	22
Tableau II.1 Les services à valeur ajoutée par la VOIP	29
Tableau II.2 Liste des codecs avec leur débit correspondant	32
Tableau II.3 Champs SDP les plus courants.....	51
Tableau II.4 Les requêtes SIP.....	52
Tableau II.5 Les réponses SIP	53
Tableau II.6 Tableau de comparaison entre le protocole SIP et H.323	61

LISTE DES ACRONYMES

PAN	Personal Area Network	PABX	Private Automatic Branch Xchange
LAN	Local Area Network	IAX	Inter Asterisk eXchange
MAN	Metropolitan Area Network	MGCP	Media Gateway Control Protocol
WAN	Wide Area Network	SCCP	Skinny Client Control Protocol
FDDI	Fiber Distributed Data Interface	API	Interface de Programmation d'Applications
P2P	Peer to Peer	JMF	Java Media Framework
OSI	Open Systems Interconnections	JDK	Java Development Kit
RTC	Réseau Téléphonique Commuté	MCU	Multipoint Control Unit
IP	Internet Protocol		
STP	Shielded Twisted Pair		
UTP	Unshielded Twisted Pair		
TCP	Transmission Control Protocol		
ICMP	Internet Control Message Protocol		
IGMP	Internet Group Management Protocol		
UDP	User Datagram Protocol		
FTP	File Transfert Protocol		
SMTP	Simple Mail Transfert Protocol		
HTTP	Hyper Text Transfert Protocol		
POP3	Post Office Protocol version 3		
ARP	Address Resolution Protocol		
VOIP	Voice Over IP		
ToIP	Téléphone Over Internet Protocol		
VoN	Voice Over the Net		
PSTN	Public Switched Telephone Network		
RTP	Real Time Transport Protocol		
RTCP	Real Time Transport Control Protocol		
SIP	Session Initiation Protocol		

Introduction générale

Le domaine de la télécommunication ne cesse d'évoluer et chaque jour on entend parler de nouvelles technologies qui envahissent notre quotidien, parmi ces nouvelles révolutions on trouve la téléphonie sur IP ou, mieux connue sous le nom, voix sur IP (VoIP, Voice over Internet Protocol) qui représente une technologie récente qui s'impose rapidement dans le domaine de la communication vocale. Elle utilise les réseaux Internet omniprésents pour généraliser l'utilisation, dans le monde entier et dans un nombre croissant de foyers et d'entreprises.

Au lieu de disposer à la fois d'un réseau informatique et d'un réseau téléphonique commuté (RTC), l'entreprise peut donc, grâce à la VoIP, tout fusionner sur un même réseau. Les nouvelles capacités des réseaux à haut débit devraient permettre de transférer de manière fiable des données en temps réel. Ainsi, les applications de vidéo ou audioconférence ou de téléphonie vont envahir le monde IP.

Comme toute innovation technologique qui se respecte, la VoIP doit non seulement simplifier le travail mais aussi faire économiser de l'argent, aussi la téléphonie sur IP utilise jusqu'à dix fois moins de bande passante que la téléphonie traditionnelle, Cette technologie exige des protocoles spécialisés dédiés à ce genre d'applications, comme le protocole de transport en temps réel RTP utilisé en parallèle avec d'autres protocoles qui concernent surtout la signalisation, la demande de réservation de ressources, la négociation de capacité comme le standard H323 et le protocole d'Initiation de sessions (SIP). L'importance de cette technologie et l'avenir qui lui est réservé nous a encouragés à s'impliquer dans ce domaine avec enthousiasme.

Avant présenté les outils et la méthode adoptée, nous allons maintenant exposer le plan du mémoire qui se subdivisera en quatre principaux chapitres.

Dans le premier chapitre intitulé ' Généralités sur les réseaux informatiques ' nous permet de prendre une idée sur les réseaux informatiques, sans oublié à avoir un bref aperçu sur les architectures d'un réseau, les différents équipements et les techniques de transmission sur ses réseaux.

Puis, au sein de ‘La voix sur IP’, deuxième chapitre de ce travail qui se divise en deux parties : nous commençons à présenter les différents principes de bases et l'architecture de la voix IP, ces avantages et ces inconvénients, la qualité de service, ensuite, on a détaillé et précis les différents protocoles de la signalisation dédiés à ce genre d'applications.

Le troisième chapitre ‘Environnement matériel et logiciel’ on a discuté sur les principes de bases et l'architecture des PABX, et spécifiquement asterisk: son architecture, principe de fonctionnement, une petite présentation sur Java Media Framework et les différentes étapes de la configuration de soft phone X-lite.

Finalement dans le dernier chapitre qu'on a nommé ‘Application’ nous présentons les outils de développement qui nous ont servi pour le développement de notre application, l'architecture et les résultats obtenus.

Objet d'étude

Nous sommes parvenus à imaginer qu'avec la réalisation d'une application mobile de la voix IP sur un réseau wifi, nous espérons adapter la politique de diffusion des informations de celle-ci à la nouvelle technologie. D'une manière simple, le choix de ce thème trouve sa justification dans le fait que la téléphonie au travers d'un réseau «par paquets» offre des avantages en termes de réduction des coûts élevés de communication contrairement au réseau téléphonique commuté (RTC).

Ce mémoire s'inscrit dans une démarche informatique et télécommunications visant à approfondir nos connaissances dans le domaine de voix sur IP, cette œuvre intellectuelle nous permet de rapprocher les notions théoriques accumulées pendant toute notre formation à la pratique, et constitue une source d'approvisionnement incontestable pour les futurs chercheurs qui aborderont le même thème.

Chapitre I

Généralités sur les réseaux informatiques

Introduction

Les réseaux existent depuis longtemps, destinés à transporter de l'information, ils peuvent être classés en trois catégories, principales, selon le type et l'origine de cette l'information :

- Réseaux téléphoniques des opérateurs de télécommunications.
- Réseaux informatiques nés de posemètre de communique des ordinateurs.
- Réseaux de diffusion acheminant les programmes audiovisuels.

Chacune de ces catégories présente des caractéristiques, liées aux applications téléphone, informatique, et de vidéo transportées par les différents réseaux.

I.1 Intérêts d'un réseau

Un ordinateur est une machine permettant de manipuler des données. L'homme, un être de communication, a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre-eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseau est utile, un réseau permet:

- Le partage de fichiers, d'applications.
- La communication entre personnes (grâce au courrier électronique, la discussion en direct, ...).
- La communication entre processus (entre des machines industrielles).
- La garantie de l'unicité de l'information (bases de données).
- Le jeu à plusieurs, ...
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).

Les réseaux permettent aussi de standardiser les applications, on parle généralement de groupware. Par exemple la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

Avantages de tels systèmes :

- Diminution des coûts grâce aux partages des données et des périphériques.
- Standardisation des applications.
- Accès aux données en temps utile.
- Communication et organisation plus efficace [1].

I.2 Définition d'un réseau informatique

Le réseau informatique est un ensemble d'équipements informatiques ou systèmes digitaux interconnecté entre eux via un milieu de transmission de données en vue partage de ressources informatiques et de la communication [2].

I.3 Les différents types des réseaux

On distingue différents types de réseaux (privés) selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On fait généralement quatre catégories de réseaux:

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

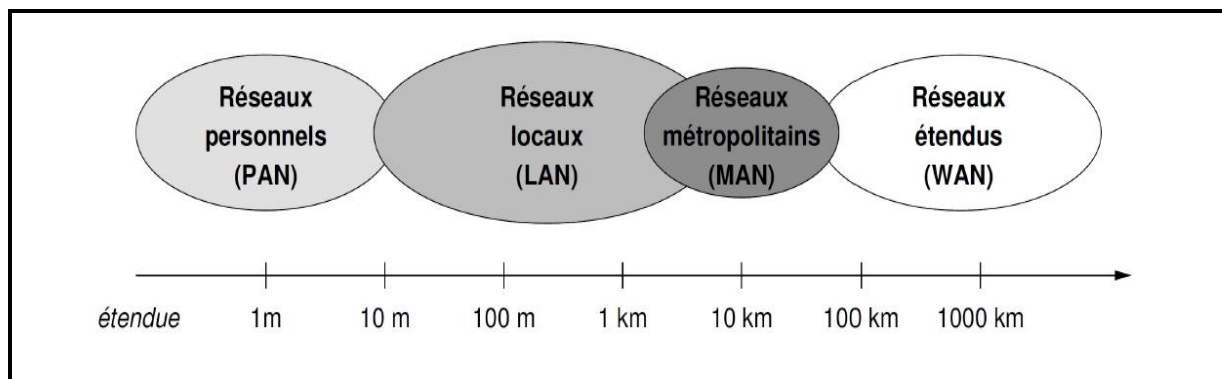


Figure 1.1 Classification de réseaux

I.3.1 Les PANs

La plus petite taille de réseau ces réseaux personnels interconnectent sur quelques mètres les équipements personnels tels que GSM, portable, organiseur etc.... d'un même utilisateur [1].

I.3.2 Les LANs

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s (pour un réseau Ethernet par exemple) et 1 Gbit/s (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs [2].

I.3.3 Les MANs

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.

Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique) [2].

I.3.4 Les WANs

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet [2].

I.4 Les différentes catégories des réseaux

On distingue également deux catégories de réseaux :

- Réseaux poste à poste (Peer to Peer= P2P).
- Réseaux avec serveur dédié (Server/client).

I.4.1 Le réseau (Peer to Peer) P2P

Chaque poste ou station fait office de serveur et Les données ne sont pas centralisées, l'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines (>10 postes) il devient impossible à gérer.

Par exemple : Si on a 4 postes et 10 utilisateurs, chaque poste doit contenir les 10 mots de passe afin que les utilisateurs puissent travailler sur n'importe lequel des postes. Mais si maintenant il y a 60 postes et 300 utilisateurs, la gestion des mots de passe devient périlleuse [2].

I.4.2 Le réseau Serveur/Client

Ils ressemblent un peu au réseau poste à poste mais cette fois-ci, on y rajoute un poste plus puissant, dédié à des tâches bien précises.

Cette nouvelle station s'appelle serveur. Le serveur Centralise les données relatives au bon fonctionnement du réseau.

Dans l'exemple précédant, C'est lui qui contient tous les mots de passe. Ainsi ils ne se trouvent plus qu'à un seul endroit. Il est donc plus facile pour l'administrateur du réseau de les modifier ou d'en créer d'autres.

L'avantage de ce type de réseau est sa facilité de gestion des réseaux comportant beaucoup de postes. Son inconvénient majeur est son coût souvent très élevé en matériel.

En effet, en plus des postes de travail il faut se procurer un serveur qui coûte cher car c'est une machine très puissante et perfectionnée. De plus la carte réseau que l'on y met est de meilleure qualité que Celle des postes de travail [2].

I.5 Les topologies des réseaux

La topologie d'un réseau recouvre tout simplement la manière dont sont reliés entre eux ses différents composants et dont ils interagissent. Nous ne séparerons pas les topologies physiques et logiques à des fins de simplification. On distingue principalement quatre types: en étoile, en bus, en anneau, et point-à-point. Nous allons définir ces types et envisager leurs avantages et leurs inconvénients [1].

I.5.1 Topologie en bus

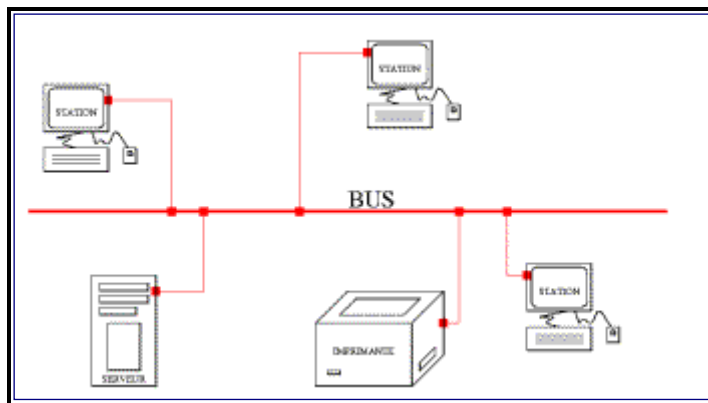


Figure I.2 Topologie en bus.

Un réseau en bus relie ses composants par un même câble et l'information envoyée par un poste est diffusée en même temps vers tous les postes. Seul le poste destinataire est censé la prendre en compte. Le câble coaxial sert typiquement à faire ce type de réseaux. On ajoute alors un bouchon à chaque extrémité du câble. En cas de coupure du câble, plus aucun poste ne peut dialoguer avec qui que ce soit, c'est la panne ! [1].

I.5.2 Topologie en étoile

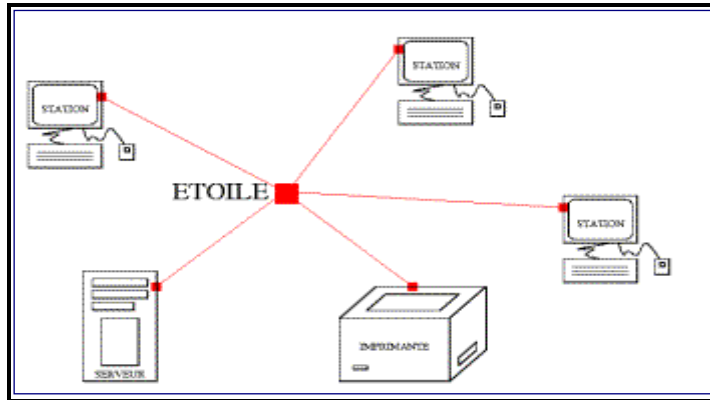


Figure I.3 Topologie en étoile.

Dans un réseau en étoile, tous les composants sont reliés à un même point central et l'information ne va que de l'émetteur vers le récepteur en transitant par ce point central. On trouve typiquement un Switch au niveau du nœud central. Si à la place du switch on met un hub, alors la topologie physique reste en étoile puisque tout le matériel est bien relié à un même point, mais la topologie logique est alors en bus.

En effet le hub ne sait que diffuser l'information à tous ses ports sans exception, on retombe donc dans le schéma typique du bus. Dans une étoile une panne ne touche qu'une seule branche (sauf si c'est le point central qui est touché) [1].

I.5.3 Topologie en anneau

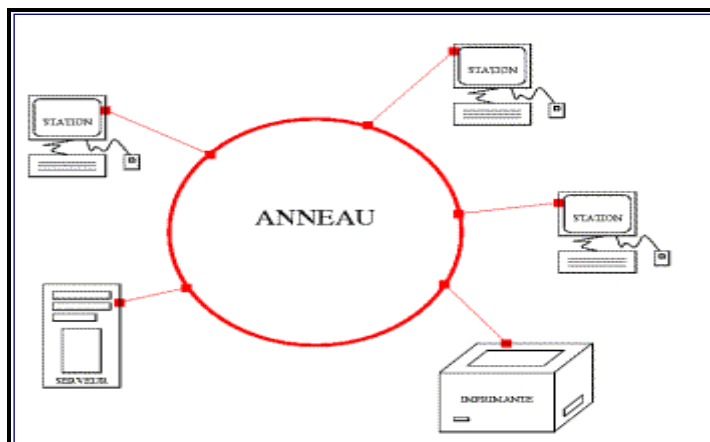


Figure I.4 Topologie en anneau.

Un réseau en anneau a lui aussi tous ces composants liés par le même câble, mais celui-ci n'a pas d'extrémité. De plus, l'information ne circule que dans un sens bien déterminé. Dans le cas du FDDI (Fiber Distributed Data Interface), réseau à base de fibre optique, on a deux anneaux indépendants.

Chaque machine doit donc posséder deux interfaces. En cas de rupture des anneaux entre deux machines, ces dernières reforment un unique anneau en assurant le transit de l'information entre leurs deux interfaces [1].

I.5.4 Topologie Point à Point

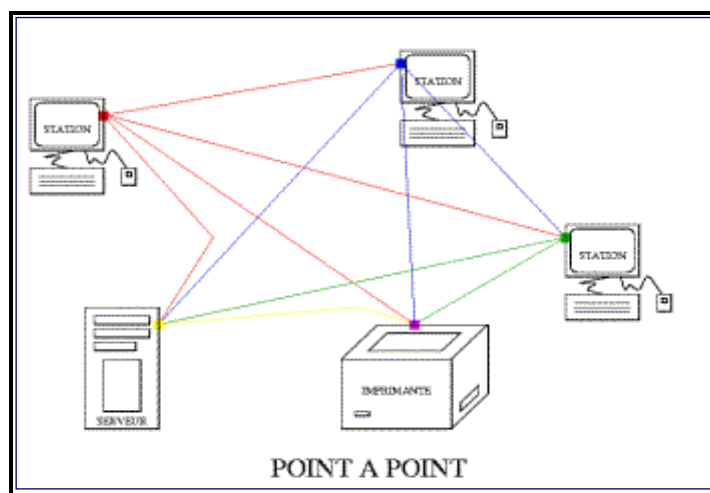


Figure I.5 Topologie point à point.

Dans un réseau point à point, chaque interface possède une liaison spécifique avec chacun des autres points. Ceci n'est utilisé que sur de tous petits réseaux ou pour des raisons de robustesse des liaisons, la redondance diminuant la sensibilité aux pannes [1].

I.6 Les équipements réseau

L'interconnexion de réseaux peut être locale: les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (Répéteur, routeur ...etc.) Fit à réaliser physiquement la liaison.

L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc..).

I.6.1 Le répéteur (Repeater)

Le répéteur permet d'interconnecter deux segments d'un même réseau.

- Il est passif au sens où il ne fait qu'amplifier le signal.
- Il ne permet pas de connecter deux réseaux de types différents
- Il travaille au niveau de la couche 1 de model OSI.

I.6.2 Le pont (Bridge)

Les ponts ne peuvent connecter que deux réseaux utilisant le même protocole. Capables de mémoriser un "carnet d'adresses" des machines composant le réseau.

Ils reconnaissent la provenance des données qui leur parviennent, et ne traitent que celles qui transitent d'un réseau à un autre, les trames échangées au sein d'un même réseau n'étant pas transmises, ce qui assure une confidentialité accrue entre les réseaux reliés.

I.6.3 La passerelle (Gateway)

La passerelle assure la connexion de deux réseaux hétérogènes, puisqu'il s'agit de systèmes matériels intégrant des applications de traduction des données à transmettre afin de les adapter au protocole du réseau de destination.

I.6.4 Le routeur (Router)

Les routeurs peuvent être comparés à des "carrefours" de réseaux, n'étant pas, contrairement aux deux dispositifs précédents, limités à la connexion de deux réseaux au maximum (ils comportent généralement de 4 à 16 ports).

Le chemin emprunté par les données est prédéfini dans une table de routage, et optimisé selon des critères de longueur de chemin (nombre de sauts pour atteindre la machine visée), ou de temps (encombrement du réseau).

I.6.5 Le concentrateur (HUB)

Le concentrateur est un boîtier qui a la fonction de répéteur. Mais sa fonction principale, est de pouvoir concentrer plusieurs lignes en une seule.

On peut y connecter plusieurs stations, dont le nombre dépend du type de HUB. Un HUB sera connecté sur un autre HUB ou sur un serveur qu'avec une seule et unique ligne.

I.6.6 Le commutateur (Switch)

Le commutateur (ou Switch) est un système assurant l'interconnexion de stations ou de segments d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage.

Les commutateurs ont donc été introduits pour augmenter la bande passante globale d'un réseau d'entreprise et sont une évolution des concentrateurs Ethernet (ou HUB) [2].

I.7 Les techniques de Commutation

Pour transporter des informations, il faut déterminer une technique de transfert. En d'autres termes, il faut savoir comment transférer un paquet depuis la machine source jusqu'à la machine réceptrice.

La commutation est l'établissement d'une connexion temporaire entre deux points d'un réseau. On peut faire de la commutation de circuit qui utilise le réseau téléphonique (RTC), et de la commutation de paquets qui utilise le réseau (IP) Internet....

I.7.1 La commutation de circuits

Elle consiste à créer dans le réseau un circuit particulier entre l'émetteur et le récepteur avant que ceux ci ne commencent à échanger les informations. Ce circuit est propre aux deux entités communicantes et sera libérer en fin de communication.

Si pendant un certains les deux entités ne s'échangent pas de données, le circuit reste quand même attribué.

Toutes les données suivent le même chemin tout au long de la communication.

Exemple : Le réseau RTC.

I.7.2 La commutation de message

Un message est une suite d'informations formant un tout, par exemple un fichier ou une ligne de commande tapée au clavier d'un ordinateur.

La commutation de message consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de nœud de commutation à un nœud de commutation. Chaque nœud de commutation attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant.

Cette technique nécessite de prévoir de grandes zones mémoire dans chaque nœud du réseau ou un contrôle de flux pour ne pas saturer le réseau.

I.7.3 La commutation de paquets

Un paquet est une suite d'octets, dont le contenu n'a pas forcément une signification et ne pouvant pas dépasser une taille fixée par avance. Apparu dans les années 70 pour résoudre le problème d'erreur de commutation de messages.

Un message émis est découpé en paquets. On parle de segmentation du message, les paquets sont commutés dans le réseau comme dans le cas des messages.

La bonne liaison vers le destinataire est trouvée grâce à une table dite de commutation (ou de routage pour la couche 3). Le message est reconstitué à partir du réassemblage des paquets reçus par le destinataire [2].

I.8 Techniques de transmission

I.8.1 Transmission série et parallèle

Le mode de transmission désigne le nombre d'unités élémentaires d'informations (bits) pouvant être simultanément transmises par le canal de communication.

- On désigne par liaison parallèle la transmission simultanée de N bits. Ces bits sont envoyés simultanément sur N voies différentes.
- Dans une liaison en série, les données sont envoyées bit par bit sur la voie de transmission. Toutefois, étant donné que la plupart des processeurs traitent les informations de façon parallèle, il s'agit de transformer des données arrivant de façon parallèle en données en série au niveau de l'émetteur, et inversement au niveau du récepteur.

I.8.2 Sens de transmission

- **Mode simplex** : La transmission ne peut se faire que de A vers B (ex : radio, télévision).
- **Mode semi-duplex** : La transmission peut se faire dans les deux sens, mais pas en même temps (ex : talkie-walkie).
- **Mode duplex intégral** : La transmission peut se faire dans les deux sens simultanément (ex : téléphone) [1].

I.9 Supports et Equipements Réseaux Locaux

I.9.1 Supports de transmission

Les supports de transmissions peuvent être décrits comme le moyen d'envoi des signaux ou données d'un ordinateur à l'autre. Les signaux peuvent être transmis via un câble, mais également à l'aide des technologies sans fil. Nous traiterons les types de support suivants:

Cuivre : coaxial et paire torsadée ;

Verre : fibre optique ; Ondes : sans fil.

a) Câble à paire torsadé

Le câble à paire torsadée est utilisé pour les communications téléphoniques et pour la plupart des réseaux Ethernet récents. Une paire de fils forme un circuit qui peut transmettre des données. Les paires sont torsadées afin d'empêcher la diaphonie, c'est-à-dire le bruit généré par les paires adjacentes.

Il existe deux types de pair torsadé:

Paire torsadée blindée (STP).

Paire torsadée non blindée (UTP).

1. Paire torsadée blindée

Le câble à paire torsadée blindée (STP) allie les techniques de blindage, d'annulation et de torsion des fils. Chaque paire de fils est enveloppée dans une feuille métallique afin de protéger davantage les fils contre les bruits. Les quatre paires sont elles-mêmes enveloppées dans une tresse ou une feuille métallique. Le câble STP réduit le bruit électrique à l'intérieur du câble (diaphonie), mais également à l'extérieur du câble (interférences électromagnétiques et interférences de radiofréquences). La figure I.6 représente le câble blindé.

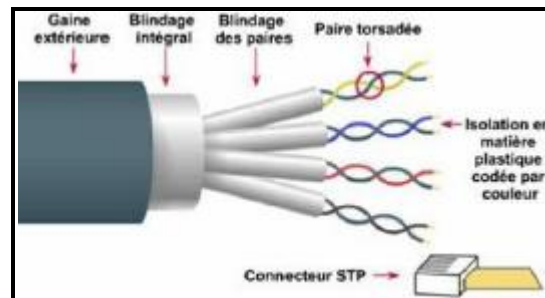


Figure I.6 Les constituants du Câble STP.

2. Paire torsadée non blindée

Le câble à paire torsadée non blindée (UTP) est utilisé sur différents réseaux. Il comporte deux ou quatre paires de fils. Ce type de câble compte uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal due aux interférences électromagnétiques et aux interférences de radiofréquences. Le câble UTP est le plus fréquemment utilisé pour les réseaux Ethernet. La figure I.8 représente le câble UTP.

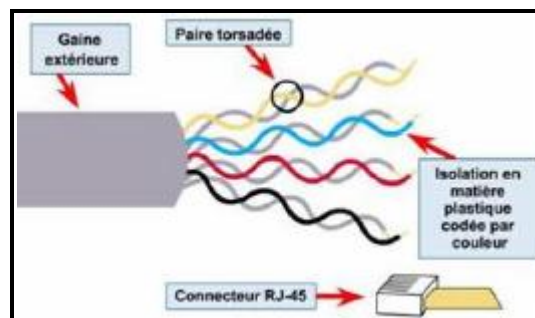


Figure I.9 Les constituants du Câble UTP.

b) Le câble coaxial

Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.

c) Câble à fibre optique

Le câble à fibre optique est un réseau capable d'acheminer des impulsions lumineuses modulées. La modulation de la lumière consiste à manipuler la lumière de telle sorte qu'elle transmette des données lors de sa circulation. Les fibres optiques comportent un cœur de brins de verre ou de plastique (et non de cuivre), à travers lesquels les impulsions lumineuses transportent les signaux.

Elles présentent de nombreux avantages par rapport au cuivre au niveau de la largeur de bande passante et de l'intégrité du signal sur la distance. Tandis que, le câblage en fibre est plus difficile à utiliser et plus coûteuse que le câblage en cuivre.

d) Supports sans fil

La communication sans fil s'appuie sur des équipements appelés émetteurs et récepteurs. La source interagit avec l'émetteur qui convertit les données en ondes électromagnétiques, puis les envoie au récepteur. Le récepteur reconvertit ensuite ces ondes électromagnétiques en données pour les envoyer à la destination. Dans le cadre de la communication bidirectionnelle, chaque équipement nécessite un émetteur et un récepteur. La plupart des fabricants d'équipements de réseau intègrent l'émetteur et le récepteur dans une même unité appelée émetteur-récepteur ou carte réseau sans fil.

Tous les équipements d'un réseau local sans fil doivent être dotés de la carte réseau sans fil appropriée.

Quatre normes de communications de données courantes s'appliquent aux supports sans fil à savoir:

Norme IEEE 802.11 : la technologie de réseau local sans fil (WLAN), couramment appelée Wifi, utilise un système de contention ou système non déterministe basé sur un processus d'accès au support par accès multiple avec écoute de porteuse/éviterment de collision (CSMA/CA).

Norme IEEE 802.15 : la norme de réseau personnel sans fil (PAN), couramment appelée Bluetooth, utilise un processus de jumelage de périphériques pour communiquer sur des distances de 1 à 100 mètres.

Norme IEEE 802.16 : la technologie d'accès couramment appelée Wi MAX (World wide Interoperability for Microwave Access) utilise une topologie point-à-multipoint pour fournir un accès à large bande sans fil [3].

I.10 Architecture des réseaux

Le but d'un système en couches est de séparer le problème en différentes parties (les couches) selon leurs niveaux d'abstraction. Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle du dessous). Chaque couche utilise ainsi les services des couches inférieures et en fournit à celle de niveau supérieur [1].

I.10.1 Le modèle de référence OSI de ISO

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux si une norme internationale n'était pas établie.

Cette norme établie par l'international standard organization (**ISO**) est la norme open system interconnection (OSI, interconnexion de systèmes ouverts).

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des l'information avec d'autres équipements hétérogènes et issus de constructeurs différents.

La première objectif de la norme OSI a été de définir un modèle de toute architecture de réseau basé sur découpage en *sept couches* chacun de ces couches correspondant à une fonctionnalité particulière d'un réseau.

Les couches 1, 2,3 et 4 sont dites basses et les couches 5,6 et 7 sont dites hautes.

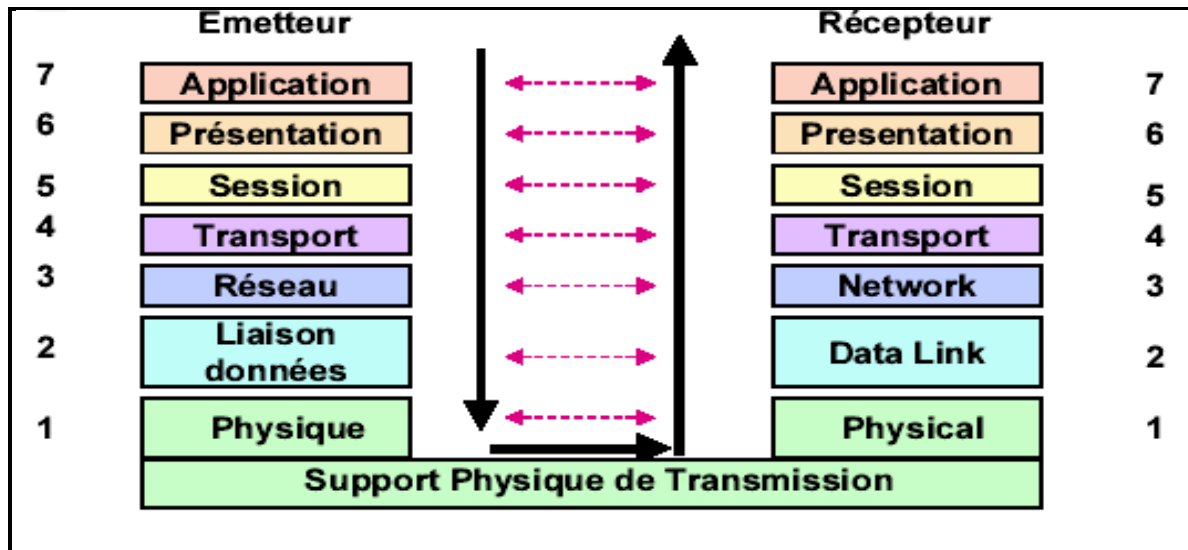


Figure I.10 Le modèle OSI en détail.

- **La couche physique**

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédure les nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entre deux entités de la leçons de données.

- **La couche liaison**

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de données entre les entités du réseau.

Cette couche détecte et corrige, quand cela est possible, les erreurs de la couche physique et signale à la couche réseau les erreurs irrécupérables.

- **La couche réseau**

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

- **La couche transport**

Cette couche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'OSI et le support de transmission).

Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requise par la couche session.

- **La couche session**

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données.

Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

- **La couche présentation**

Cette couche assure la transparence du format des données à la couche application.

- **La couche application**

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tout les services directement utilisables par l'application (transfert e données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications) [2].

I.10.2 Modèle TCP/IP

Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle.

- **La couche de liens** ou couche accès réseau est l'interface avec le réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.

- **La couche réseau** ou couche IP (Internet Protocol) gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol)
- **La couche transport** assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas de UDP (User Datagram Protocol).
- **La couche application** est celle des programmes utilisateurs comme Telnet (connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), etc... [1].

I.10.2.1 Les protocoles de la couche application

Les protocoles d'application sont des protocoles de haut niveau, adaptés aux besoins d'applications spécifiques. Ils s'appuient sur UDP et TCP pour permettre le transfert d'informations entre une application serveur et ses applications clientes.

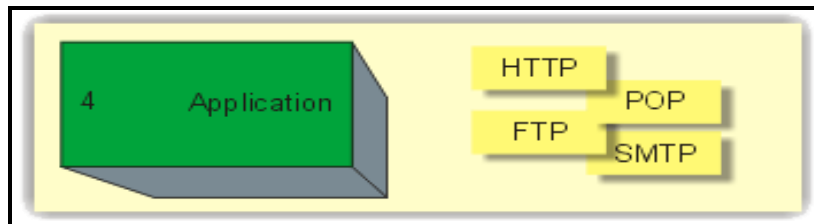


Figure I.11 La couche application.

■ -Le protocole HTTP (Hyper Text Transfert Protocol)

Ce protocole est utilisé pour la navigation web entre un serveur HTTP et un butineur. Le protocole assure (normalement) qu'un client comme : Internet Explorer ou Netscape peut envoyer des requêtes et recevoir les réponses de serveurs HTTP sans problèmes particuliers.

■ -Le protocole FTP (File Transfert Protocol)

Protocole qui permet d'assurer le transfert de fichiers de façon indépendante des spécificités des OS (Operating System). Ainsi, un client FTP sous Windows peut télécharger un fichier depuis un serveur UNIX.

■ -Le protocole SMTP (Simple Mail Transfert Protocol)

Le protocole qui permet d'acheminer le courrier depuis le serveur SMTP de l'émetteur, jusqu'au serveur SMTP du destinataire, qui le classe dans les Boîtes aux lettres de ses clients.

■ -Le protocole POP3 (Post Office Protocol version 3)

Le protocole qui permet au client de relever à distance le courrier classé dans sa boîte aux lettres.

■ -Le protocole TELNET (Tele Network)

C'est le "couteau suisse" du travail à distance. En fait, un client TELNET est une console en mode texte, capable de se connecter sur la plupart des serveurs, comme POP3 ou SMTP. Il devient alors possible d'envoyer et de lire des messages, si l'on connaît les commandes inhérentes aux protocoles SMTP et POP3.

Un serveur TELNET permet cependant des choses bien plus puissantes et "dangereuses" puisqu'il devient possible de prendre à distance le contrôle d'un hôte. C'est un outil qui permet l'administration distante d'une machine, du moment que l'on est capable d'ouvrir une session et d'acquérir les droits de "super utilisateur".

I.10.2.2 Les protocoles de la couche transport :



Figure I.12 La couche transport.

■ -Le Protocole UDP (USER DATAGRAM PROTOCOL)

Le protocole UDP est basé en couche 4. Il n'ouvre pas de session et n'effectue pas de control d'erreur. Il est alors appelé "mode non connecté". Il est donc peut fiable, cependant, il permet aux applications d'accéder directement à un service de transmission de Datagrammes rapide.

UDP est utilisé pour transmettre de faibles quantités de données où le coût de la création de connexions et du maintient de transmissions fiables s'avèrent supérieur aux données à émettre. UDP peut également être utilisé pour les applications satisfaisant à un modèle de type "interrogation réponse". La réponse étant utilisée comme un accusé de réception à l'interrogation. On y trouve classiquement Snmp et Dns. UDP est aussi utilisé dans un second cas, tel que la voix sur IP.

L'envoi en temps réel est primordial, donc si une trame n'arrivait pas, la retransmission serait inutile. Chaque machine contient un ensemble de points de destination abstraits appelés protocole ports, identifiés par un entier positif codé sur deux octets. Une application qui souhaite communiquer sur le réseau avec une autre application doit se raccorder à un port. Une application est donc identifiée sur le réseau par :

- L'adresse IP de la station sue laquelle elle se trouve.
- Le protocole TCP ou UDP.
- Le port number auquel elle s'est raccordée.

Cette connexion logique entre deux ports est appelée : **Socket**. UDP est un protocole de transport utilisant directement IP ce qui entraîne qu'il offre un service de transport :

- Non fiable (sans acquittement).
- Sans connexion.
- Sans contrôle de flux.

C'est aux applications de prendre en charge l'acquittement, la connexion et la remise dans l'ordre des messages. Voici la structure de l'entête UDP basé sur 8 octets.

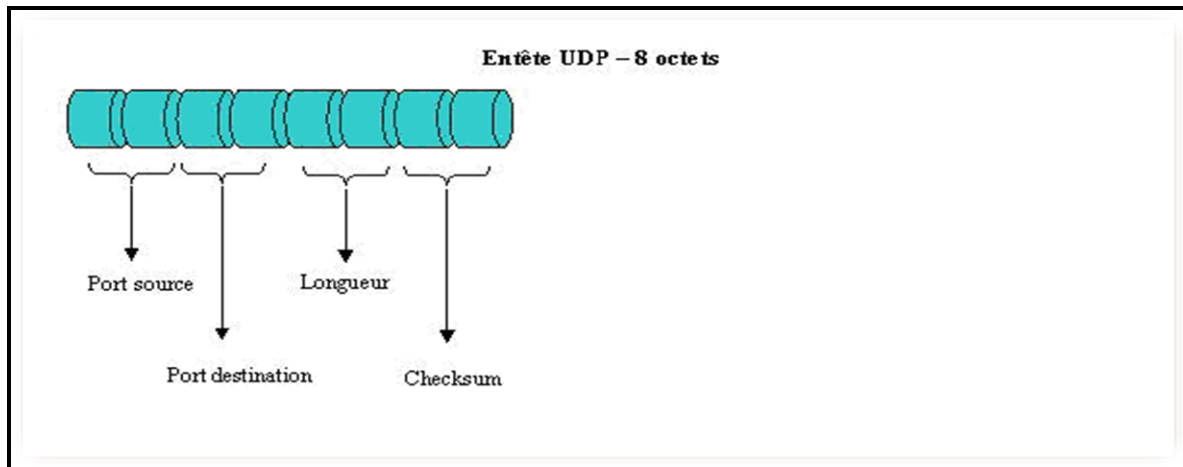


Figure I.13 l'entête UDP.

- **Port source** : Le champ Port source est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine source.
- **Port destination** : Le champ Port destination est codé sur 16 bits et il correspond au port relatif à l'application en cours sur la machine de destination.
- **Longueur** : Le champ Longueur est codé sur 16 bits et il représente la taille de l'entête et des données. Sont unité est l'octet et sa valeur maximale est 64 Ko (2^{16}).
- **Checksum** : Le champ Checksum est codé sur 16 bits et représente la validité du paquet de la couche 4 UDP. Le Checksum est constitué en calculant le complément à 1 sur 16 bits de la somme des compléments à 1 des octets de l'en-tête et des données pris deux par deux (mots de 16 bits).

■ -Le protocole TCP (Transfert Control Protocol)

Le protocole TCP est basé en couche 4. Il ouvre une session et effectue lui-même le control d'erreur. Il est alors appelé "mode connecté".

TCP fournit un service :

- Fiable (canal sans erreurs).
- Avec contrôle de flux.
- Ordonné.

- En mode full duplex.
- En mode connecté.

TCP tout comme UDP utilise la notion de port excepté que TCP utilise la connexion comme abstraction de port. Une connexion est identifiée par une paire de « End points » : Host (@IP d'une station) et Port (port TCP). Voici la structure de l'entête TCP basé sur 20 octets.

I.10.2.3 Les protocoles de la couche Internet



Figure I.14 La couche internet.

■ -Le protocole IP (Internet Protocol)

IP signifie "Internet Protocol", protocole Internet. Il représente le protocole réseau le plus répandu. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée. Ce protocole utilise ainsi une technique dite de commutation de paquets.

Au niveau IP, les données des utilisateurs ou des applications sont encapsulées à l'intérieur d'unités de transfert appelées datagrammes IP. Le protocole IP fournit un service d'acheminement des datagrammes IP sans connexion et non fiable.

Un datagramme se compose d'un en tête et de données. Avant transmission sur un réseau physique, le datagramme IP est encapsulé dans une trame physique. Voici la structure de l'entête IP basé sur 20 octets.

■ -Le protocole ARP (Address Resolution Protocol)

Le protocole Arp, signifiant Address Resolution Protocol, fonctionne en couche Internet du modèle TCP/IP correspondant à la couche 3 du modèle Osi. L'objectif de Arp est

de permettre de résoudre une adresse physique par l'intermédiaire de l'adresse IP correspondante d'un host distant.

Le protocole Arp apporte un mécanisme de « translation » pour résoudre ce besoin. Il permet d'obtenir l'adresse physique (MAC, niveau 2) d'une machine connaissant son adresse IP (logique, niveau 3). Voici l'entête du protocole ARP dans le cadre spécifique d' IP sur Ethernet.

■ -Le protocole IGMP (Internet Group Message Protocol)

Le protocole IGMP (Internet Group Management Protocol) permet de gérer les déclarations d'appartenance à un ou plusieurs groupes auprès des routeurs Multicast. Les inscriptions sont soit spontanées soit après requête du routeur. Pour cela, l'hôte envoie une trame IGMP destinées à ce ou ces groupes. Voici la structure de l'entête IGMP V2 basé sur 8 octets [2].

I.11 TCP/IP et le modèle OSI

Le modèle TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre :

Modèle TCP/IP	Modèle OSI
Couche Application	Couche Application
	Couche Présentation
	Couche Session
Couche Transport (TCP)	Couche Transport
Couche Internet (IP)	Couche Réseau
Couche Accès réseau	Couche Liaison données
	Couche Physique

Tableau I.1 Comparaison entre TCP/IP et modèle OSI.

Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI.

Conclusion

La connaissance préalable d'une infrastructure réseau et différents matériels utilisé dans le réseau est une étape nécessaire pour acquérir la maîtrise globale d'un environnement réseau.

Ce chapitre vient de décrire les types de réseaux, les supports de transmission ainsi que les composants matériels qui les constituent. Le chapitre suivant va aborder les considérations générales sur la VoIP.

Chapitre II

La voix sur IP

Introduction

La voix sur IP (Voice over IP) est une technologie de communication vocale en pleine émergence. En effet, la convergence du triple Play (voix, données et vidéo) fait partie des enjeux principaux des acteurs de la télécommunication aujourd'hui.

Plus récemment l'Internet s'est étendu partiellement dans l'Intranet de chaque organisation, voyant le trafic total basé sur un transport réseau de paquets IP surpasser le trafic traditionnel du réseau voix (réseau à commutation de circuits). Il devenait clair que dans le sillage de cette avancée technologique, les opérateurs, entreprises ou organisations et fournisseurs devaient, pour bénéficier de l'avantage du transport unique IP, introduire de nouveaux services voix et vidéo.

Les premières technologies de VoIP imaginées étaient propriétaires et donc très différentes les unes des autres. Pourtant, un système qui est censé mettre des gens et des systèmes en relation exige une certaine dose de standardisation. C'est pourquoi sont apparus des protocoles standards, comme le H323 ou le SIP.

II.2 Définition

C'est un nom générique définit le transport de trafic Vocal au moyen de la transmission par paquets sur le protocole Internet (Internet Protocol), Le trafic VoIP peut être acheminé sur un réseau privé contrôlé ou le réseau Internet public Ou une combinaison des deux.

II.3 Définitions importantes

- **Téléphone over Internet Protocol (ToIP)** : également appelée téléphonie Internet, est un service spécifique de VoIP utilisant la transmission par paquets sur le réseau public Internet, par définition ouverte et non contrôlable.
- **Voice over the Net (VoN)** : définit le transport de trafic vocal au moyen de la transmission par Paquets sur le réseau Internet public uniquement [2].

II.4 Le Réseau Téléphonique Commuté

Le RTC est tout simplement le réseau téléphonique que nous utilisons dans notre vie de tous les jours et qui nous donne accès à de multiples fonction. En effet outre le fait de pouvoir téléphoner, le RTC nous permet d'utiliser de multiples services tel que la transmission et réception de fax, l'utilisation d'un minitel, accéder à Internet etc.... Il représente donc l'un des protocoles de discussion utilisé sur la paire de cuivre boucle locale.

II.4.1 Principe du RTC

Le réseau téléphonique public (RTPC, Réseau Téléphonique Public Commuté ou simplement RTC) a essentiellement pour objet le transfert de la voix. Utilisant le principe de la commutation de circuits, il met en relation deux abonnés à travers une liaison dédiée pendant tout l'échange [2].

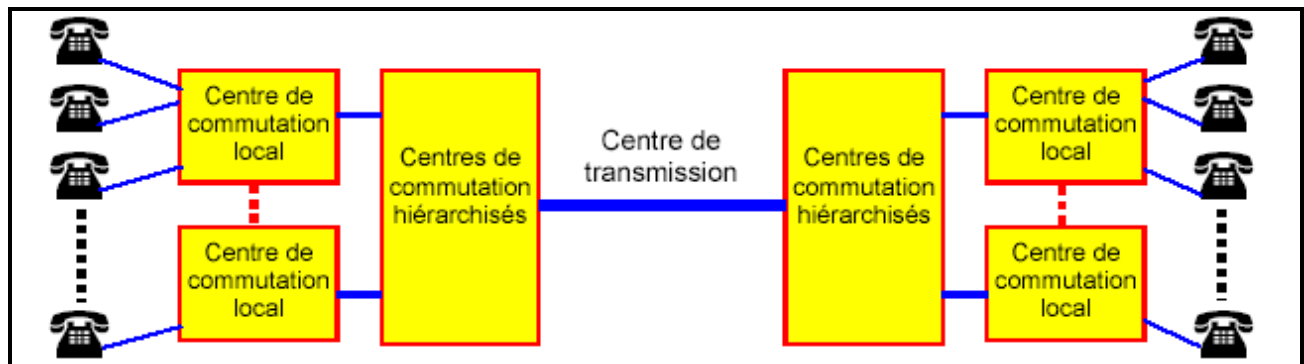


Figure II.1 Le réseau téléphonique commuté RTC.

II.5 PABX et PABX-IP

II.5.1 PABX Ou PBX ?

C'est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur et le réseau RTC. Une mise à jour du PABX est aussi nécessaire. Si tout le réseau devient IP, il n'y a plus besoin de ce matériel.

II.5.2 Le PABX-IP

C'est lui qui assure la commutation des appels et leurs autorisations, il peut servir aussi de routeur ou de Switch dans certains modèles, ainsi que de serveur DHCP. Il peut posséder des interfaces de type analogiques (fax), numériques (postes), numériques (RNIS, QSIG) ou opérateurs (RTC-PSTN ou RNIS). Il peut se gérer par IP en intranet ou par un logiciel serveur spécialisé que ce soit en interne ou depuis l'extérieur.

Il peut s'interconnecter avec d'autres PABX-IP ou PABX non IP de la même marque (réseau homogène) ou d'autres PABX d'autres marques (réseau hétérogène) [2].

II.6 Architecture

II.6.1 Modèles du VOIP

Il existe trois modèles différents de VOIP: La VOIP de PC à PC, la VOIP de PC à téléphone et la VOIP de téléphone à téléphone.

Modèles de PC à PC :

Dans ce modèle, chaque ordinateur est équipé d'une carte de son, microphone et haut-parleur. Il connecte directement le réseau Internet grâce au modem ou avec une carte NIC. Les ordinateurs installent le logiciel VOIP pour faire des appels.

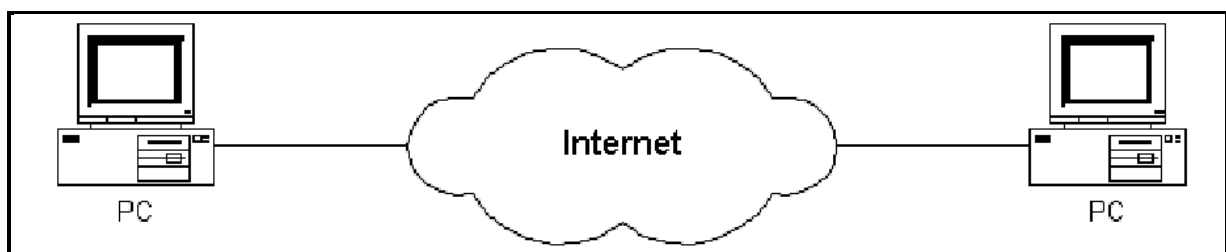


Figure II.2 Le scénario PC à PC.

Modèles de PC à Téléphone :

Ce modèle développe plus que le modèle PC à PC. Il permet l'utilisateur de faire des appels vers le réseau RTC et inversement. Dans ce modèle, le réseau IP et le réseau RTC se connectent grâce à la passerelle.

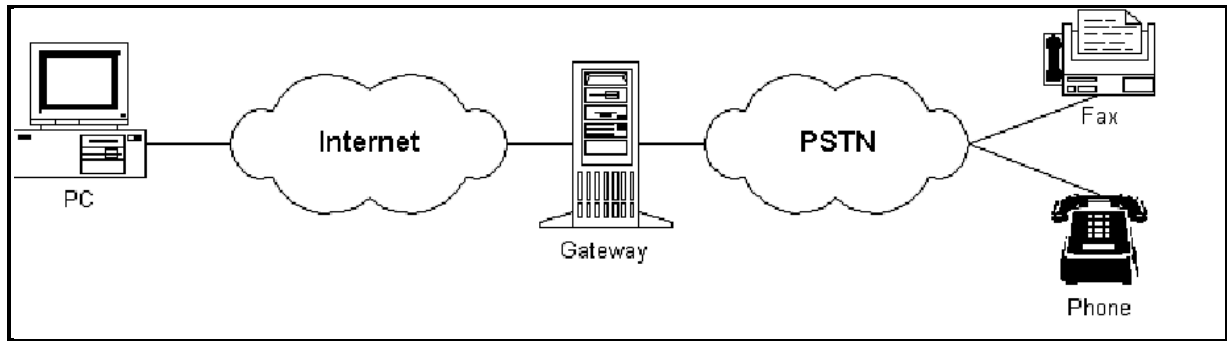


Figure II.3 Le scénario PC à Téléphone.

Modèles de téléphone à téléphone :

Élargir le modèle PC à téléphone, ce modèle utilise le réseau Internet pour communiquer entre les réseaux PSTN. Pour faire d'appel, le réseau PSTN va connecter avec la passerelle la plus proche et puis la passerelle va convertir le numéro de téléphone à l'adresse IP pour cheminer les paquets vers destination [4].

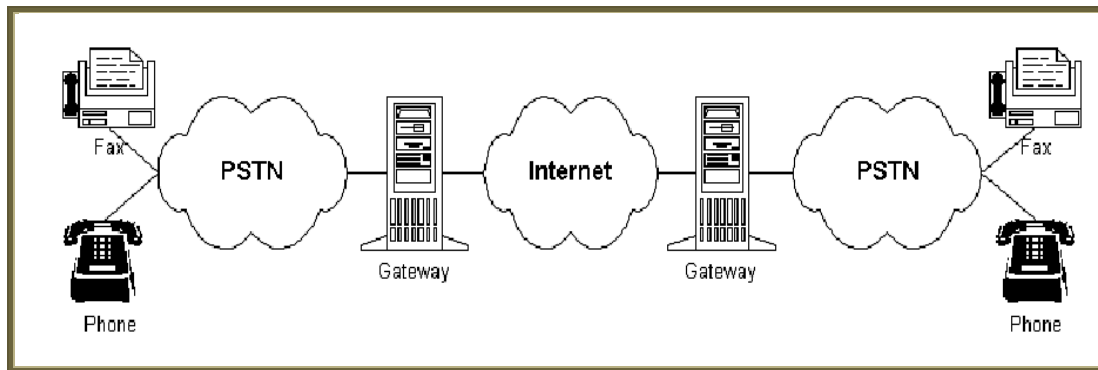


Figure II.4 Le scénario téléphone à téléphone.

II.7 Protocoles de transport utilisés en voix sur IP

RTP/RTCP sont deux protocoles qui ont été utilisés pour le transport de flux média sur le réseau IP. Les réseaux utilisant le multiplexage statistique pour transmettre la voix introduit de la gigue qui doit être compensée par le récepteur. Les routeurs IP sont dispositifs de multiplexage statistique et alors toutes les applications de voix et vidéo sur IP doivent résoudre ce problème de gigue. Le protocole RTP a été conçu pour permettre à récepteur de compenser la gigue et les changements d'ordre des paquets. RTP peut être utilisé pour n'importe type de donnée temps réel. RTP définit un formatage particulier des données pour le paquet IP.

- Une information sur le type de données transportées(le payload)
- Des marques temporelles
- Des numéros de séquence

Le protocole RTP est presque toujours utilisé avec le protocole RTCP. Il permet de transporter de l'information concernant la qualité effective de la transmission (gigue mesuré, taux moyen de perte de paquets...). Les protocoles RTP/RTCP ne contrôlent tout à fait pas la qualité de service. Le réseau IP peut détruire, retarder ou changer l'ordre des paquets RTP. En général RTP est utilisé au-dessus de UDP qui est le protocole de transport non fiable le plus utilisé sur les réseaux IP. UDP assure seulement l'intégrité des données en utilisant une somme de contrôle (checksum). Il ne gère pas la récupération de données perdues [4].

II.8 La VOIP : avantages et inconvénients

II.8.1 Les avantages

Avec un réseau basé sur l'IP (Internet Protocol), de nombreuses possibilités sont offertes aux utilisateurs et opérateurs. Les avantages que l'on trouve sont les suivants:

- **La réduction des coûts :**

En utilisant la VOIP à la place du réseau RTC (Réseau Téléphonique Commuté), les entreprises peuvent réduire leur coût de communication surtout dans le cadre de communication internationale. Dans l'utilisation de réseaux WAN/IP inter-sites, les réductions de coût sont plus intéressantes surtout s'il existe de nombreux sites distants. De manière plus simple, la communication entre deux personnes utilisant la VOIP pourrait réduire leurs coûts de communication entre 60 et 70%.

- **Standardisation et interopérabilité entre les fournisseurs :**

L'architecture utilisée est unique vu que le réseau téléphonique est intégré au réseau de données pour former un seul réseau de communication.

- **Mobilité :**

Contrairement à un téléphone classique, le téléphone IP peut rester avec son utilisateur. La seule obligation est d'avoir une connexion Internet (accès au réseau de données). Le numéro de téléphone peut être conservé quelque soit l'endroit où l'on se trouve.

- **De nouveaux services :**

Les services à valeur apportée par la VOIP	
Application	Description
Téléphonie	Service de téléphonie Vocal et fax
Messagerie unifiée	Convergence des messages (e-mails, messages vocaux, fax, SMS)
Audio /vidéo conférence	Echange simultané et en temps réel du son, des images et de documents
Click to dial	Communication directe avec un centre d'appels depuis un ordinateur
Messagerie instantanée	Gestion de présence et communication en temps réel (texte et voix)

Tableau II.1 Les services à valeur apportée par la VOIP.

II.8.2 Les inconvénients

Cette technologie possède aussi des inconvénients. Son coût, son architecture, la qualité et la fiabilité de cette technologie sont des inconvénients à prendre en compte.

➤ **Le coût de la VOIP :**

Dans une entreprise en investissant directement dans la VOIP ne sera pas forcément gagnant. Le passage à la VOIP a un coût dû à l'installation de l'infrastructure et l'achat des équipements. Pour passer progressivement à la VOIP, les entreprises passent en général via des adaptateurs.

Au final, les entreprises existantes passent à la VOIP de manière progressive, contrairement aux entreprises naissantes qui ont la possibilité d'installer dès le départ une structure reposant sur la VOIP.

➤ **L'architecture :**

En utilisant un réseau de données existant, c'est aussi retrouver les problèmes de sécurité existants déjà sur les réseaux informatiques.

➤ **La qualité et la fiabilité :**

Les flux de données (voix) utilisent un réseau existant sur lequel existent déjà des problèmes pouvant nuire à la qualité du service téléphonique. En effet les problèmes de latence, de délais, perte de paquets peuvent beaucoup faire baisser la qualité et la fiabilité du service.

Il faut un délai de moins de 150 ms de latence pour une bonne qualité et toutes les connexions aujourd'hui ne respectent pas encore cette moyenne.

II.9 Les différents éléments pouvant composés un réseau VoIP

Pour l'établissement des services utiliser VOIP on doit avoir les infrastructures, le logiciel, et les systèmes nécessaires. La figure II.5 décrit, de façon générale, la topologie d'un réseau de téléphonie IP.

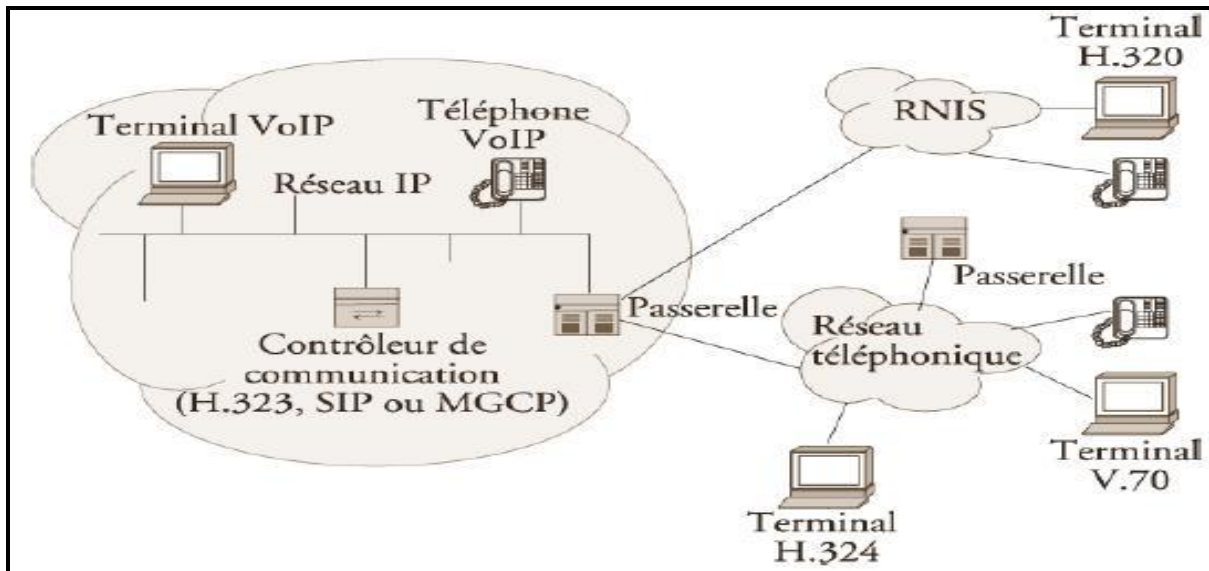


Figure II.5 Architecture d'un réseau VoIP.

II.9.1 Terminaux VOIP

Ils sont des ordinateurs installant les logiciels supportant VOIP, des téléphones IP. Ils établissent, terminent des appels [4].

II.9.2 Le serveur de communications

Il gère les autorisations d'appels entre les terminaux IP ou soft phones et les différentes signalisations du réseau. Il peut posséder des interfaces réseaux opérateurs (RTC-PSTN ou RNIS), sinon les appels externes passeront par la passerelle dédiée à cela (Gateway). Exemple : (Call Manager de Cisco)

II.9.3 La passerelle (Gateway)

C'est un élément de routage équipé de cartes d'interfaces analogiques et/ou numériques pour s'interconnecter avec soit d'autres PABX (en QSIG, RNIS ou E&M), soit des opérateurs de télécommunications local, national ou international. Plusieurs passerelles peuvent faire partie d'un seul et même réseau, ou l'on peut également avoir une passerelle par réseau local (LAN).

La passerelle peut également assurer l'interface de postes analogiques classiques qui pourront utiliser toutes les ressources du réseau téléphonique IP (appels internes et externes, entrants et sortants).

II.9.4 Le routeur

Il assure la commutation des paquets d'un réseau vers un autre réseau.

II.9.5 Le Switch

Il assure la distribution et commutation de dizaines de port Ethernet à 10/100 voire 1000 Mbits/s. Suivant les modèles, il peut intégrer la télé alimentation des ports Ethernet à la norme 802.3af pour l'alimentation des IP-phones ou des bornes WIFI en 48V.

II.9.6 Le Gatekeeper

Il effectue les translations d'adresses (identifiant H323 et @ IP du référencement du terminal) et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action.

II.9.7 Le MCU

Le MCU (multi conferences unit) est un élément optionnel et gère les conférences audio vidéo.

III.9.8 Le Soft phone

C'est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP [2].

II.10 Qualité de service de la voix sur IP

La qualité du transport de la voix est affectée par les paramètres suivants :

- La qualité du codage.
- Le délai d'acheminement (delay).
- La gigue (jitter).
- La perte de paquets (packetloss).
- L'écho.

Toutes ces contraintes déterminent la QoS (Quality of Service ou Qualité de service en français).

II.10.1 Qualité de codage

Généralement, plus le taux de compression est élevé par rapport à la référence de 64Kb/s (G711), moins la qualité de la voix est bonne. Toutefois, les algorithmes de compression récents permettent d'obtenir des taux de compression élevés, tout en maintenant une qualité de la voix acceptable. L'acceptabilité par l'oreille humaine des différents algorithmes est définie selon le critère MOS (Mean Operationnal Score), défini par l'organisme de normalisation internationale ITU (International Telecommunication Union / Union internationale des Télécommunications). Dans la pratique, les deux algorithmes les plus utilisés sont le G.729 et le G.723.1. Le tableau II.2 ci-après montre une liste des codecs avec leur débit correspondant :

Nom du codec	Débit
G.711	64 kbps
G.726 b	32 kbps
G.726 a	24 kbps
G.728	16 kbps
G.729	8 kbps
G.723.1	MPMLQ 6.3 kbps
G.723.1	ACELP 5.3 kbps

Tableau II.2 Liste des codecs avec leur débit correspondant.

II.10.2 Délai d'acheminement

Latence (Delay) Selon la norme ITU G114, le délai d'acheminement permet :

- Entre 0 et 150 ms, une conversation normale ;
- Entre 150 et 300 ms, une conversation de qualité acceptable ;
- Entre 300 et 700 ms, uniquement une diffusion de voix en half duplex (mode talkie-walkie) Au-delà, la communication n'est plus possible.

II.10.3 Gigue (jitter)

La gigue est la variance statistique du délai de transmission. En d'autres termes, elle mesure la variation temporelle entre le moment où deux paquets auraient dû arriver et le moment de leur arrivée effective. Cette irrégularité d'arrivée des paquets est due à de multiples raisons dont: l'encapsulation des paquets IP dans les protocoles supportés, la charge du réseau à un instant donné, la variation des chemins empruntés dans le réseau. Pour reconstruire le son exact à partir des paquets on doit supprimer la gigue. Maintenant, on utilise le tampon pour supprimer la gigue. Les paquets arrivés vont stocker dans le tampon avant être traité. Cette méthode peut augmenter le temps de délai.

II.10.4 Perte des paquets

Le réseau Internet n'assure pas que tous les paquets sont transportés à la destination. Les paquets peuvent être perdus à cause de la congestion, de la bande passante. Pour la VOIP, le

taux de la perte de paquet doit être inférieur à 10%. À cause de la limite de délai alors les protocoles de retransmission ne sont pas satisfaits pour résoudre ce problème. Il y a quelques techniques pour résoudre le problème de la perte de paquet. Par exemple on peut remplacer les paquets perdus par les signaux calmes ou diminuer la transmission des paquets par les techniques d'impression de signal. On trouve que le temps d'appel active est seulement de 30% à 40% du temps d'appel alors on peut utiliser un dispositif pour créer les sons agréables quand l'appel n'est pas actif.

II.10.5 Echo

L'écho est un phénomène lié principalement à des ruptures d'impédance lors du passage de 2 fils à 4 fils. Le phénomène d'écho est particulièrement sensible à un délai d'acheminement supérieur à 50 ms. Il est donc nécessaire d'incorporer un équipement ou un logiciel qui permet d'annuler l'écho [3].

II.11 Les protocoles de la VOIP

Un protocole est un ensemble de spécifications décrivant les conventions et les règles à suivre dans un échange de données. Jusqu'à présent, il existe trois standards ou protocoles qui permettent la mise en place d'un service VoIP. Le plus connu est le standard H.323 qui a été élaboré dans le milieu des télécommunications ensuite, plus ancien le MGCP (Media Gateway Control Protocol) et le plus récent SIP qui a été développé dans le milieu informatique (essentiellement le web).

Notre étude sera basée sur les protocoles les plus utilisés : H323 et SIP que nous allons développer dans cette section.

II.11.1 Le Protocole H.323

Introduction

H.323 est un protocole de signalisation défini par l'ITU-T en 1996 permettant l'établissement, la libération et la modification de sessions multimédia (voix, vidéo, données). Il hérite du protocole Q.931 du RNIS qu'il enrichit pour son fonctionnement dans des réseaux de transport en mode paquet. Le protocole H.323 supporte un ensemble de services complémentaires similaires à ceux mis en œuvre dans un réseau RNIS. D'abord H.323 est

pour la transmission de la voix sur réseau local(LAN) mais de plus en plus avec le développement des techniques, la norme H.323 est amélioré et appliqué sur les réseaux d'ordinateur plus grand (Internet, Intranet).

II.11.1.1 Architecture et composants de la norme H323

La norme H.323 définit quatre composants principaux: Terminal, Gatekeeper, Passerelle, MCU. La figure II.6 représente les composants de l'architecture H.323.

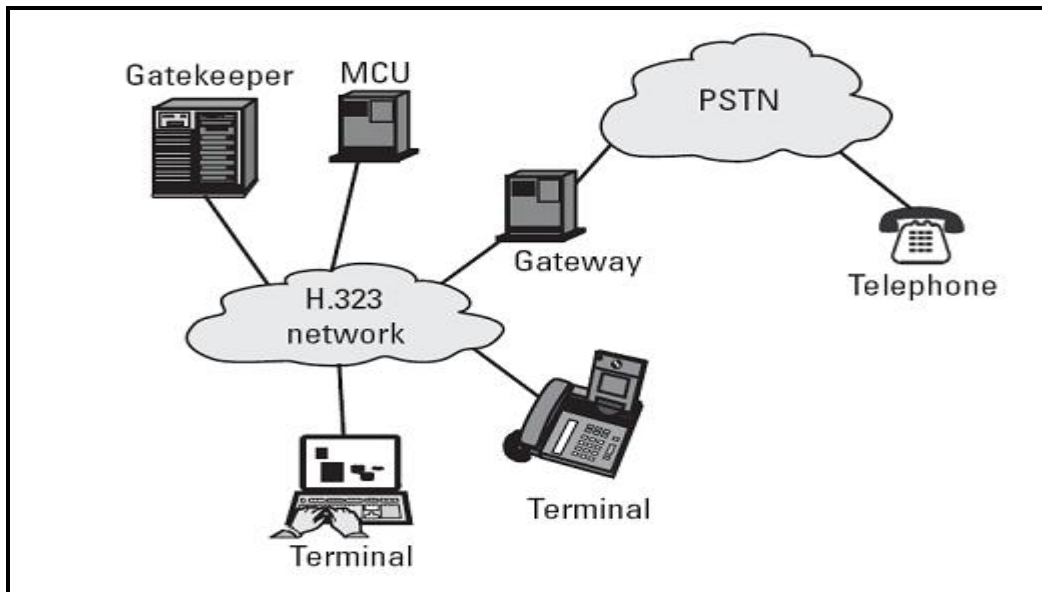


Figure II.6 Les composants de l'architecture H.323.

Terminal H.323: Il est nœud du réseau de la VOIP, il peut connecter sur le réseau pour :

- Faire un appel avec un autre terminal de la VOIP ou d'autre réseau.
- Accepter un appel de d'autre terminal.
- Terminer un appel.

Gatekeeper : Il est un composant de l'architecture de la VOIP qui gère la registration, L'admission et la statue des terminaux ou des passerelles. Il peut faire la gestion de zone, Traiter d'appel et signer d'appel.

- Traduire des adresses.
- Registrer les terminaux.
- Confirmer.
- Contrôler l'acceptation de canal d'information.

MCU: Il est nœud du réseau de la VOIP.

Le MCU est une station sur le réseau qui fournit les possibilités pour trois terminaux ou plus et passages pour participer à une conférence multipoints. Le MCU gère les ressources de la conférence, négocie avec les terminaux pour déterminer les codecs audio et vidéo à utiliser et gère les flux de données. Le MCU se compose d'un contrôleur multipoints obligatoire (MC) et des processeurs multipoints optionnels (MP). MC détermine les possibilités communes de terminaux en utilisant H.245 mais il n'exécute pas le multiplexage d'audio, de la vidéo et des données. Le multiplexage de médias est manipulé par le MP sous la commande de MC.

Passerelle (gateways) :

Les passerelles H.323 assurent l'interconnexion avec les autres réseaux, ex:((H.320/RNIS), les modems H.324, les téléphones classiques, etc...).

Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodage audio) [4].

II.11.1.2 Les avantages et inconvénients du protocole H.323

Avantages :

Les réseaux IP sont à commutation de paquets, les flux de données transitent en commun sur une même liaison. Les débits des réseaux IP doivent donc être adaptés en fonction du trafic afin d'éviter tout risque de coupure du son (et de la vidéo).

Tous les sites n'ont pas le même débit. Plus le débit sera élevé et plus le risque de coupure sera faible. Par ailleurs, tant que la qualité de service n'existera pas dans les réseaux IP, la fiabilité des visioconférences sur les lignes à faible débit sera basse.

Voici les principaux bénéfices qu'apporte la norme H.323 :

Codecs standards : H.323 établit des standards pour la compression et la décompression des flux audio et vidéo. Ceci assure que des équipements provenant de fabricants différents ont une base commune de dialogue.

Interopérabilité : Les utilisateurs peuvent dialoguer sans avoir à se soucier de la compatibilité du terminal destinataire. En plus d'assurer que le destinataire est en mesure de décompresser l'information, H.323 établit des méthodes communes d'établissement et de contrôle d'appel.

Indépendance vis à vis du réseau : H.323 est conçu pour fonctionner sur tout type d'architecture réseau. Comme les technologies évoluent et les techniques de gestion de la bande passante s'améliorent, les solutions basées sur H.323 seront capables de bénéficier de ces améliorations futures.

Indépendance vis à vis des plates-formes et des applications : H.323 n'est lié à aucun équipement ou système d'exploitation.

Support multipoint : H.323 supporte des conférences entre trois terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.

Gestion de la bande passante : Le trafic audio et vidéo est un grand consommateur de ressources réseau. Afin d'éviter que ces flux ne congestionnent le réseau, H.323 permet une gestion de la bande passante à disposition. En particulier, le gestionnaire du réseau peut limiter le nombre simultané de connexions H.323 sur son réseau ou limiter la largeur de bande à disposition de chaque connexion. De telles limites permettent de garantir que le trafic important ne soit pas interrompu.

Support multicast : H.323 supporte le multicast dans les conférences multipoint. Multicast, c'est le fait d'envoyer un paquet vers un sous ensemble de destinataires sans réplication, permet une utilisation optimale du réseau.

Indispensable pour permettre un minimum d'interopérabilité entre équipements de fournisseurs différents, ce standard présente toutefois les inconvénients suivants [3].

Inconvénients

H.323 est un protocole complexe, créé initialement pour les conférences multimédia et qui incorpore des mécanismes superflus dans un contexte purement téléphonique. Ceci a notamment des incidences au niveau des terminaux H.323 (téléphones IP, par exemple) qui

nécessitent de ce fait une capacité mémoire et de traitement non sans incidence au niveau de leur coût.

Il comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité ou de plus petit dénominateur commun (dans le choix du codec, par exemple) ; D'autre part, comme le seul codec obligatoire est le codec G.711 (64 Kbps) et que le support des autres codecs plus efficaces est optionnel, l'interopérabilité entre produits provenant de constructeurs différents ne signifie pas qu'ils feront un usage optimal de la bande passante. En effet, dans le cas où les codecs à bas débits sont différents, le transport de la voix se fera à 64 Kbps, ce qui, en termes de bande passante, ne présente guère d'avantages par rapport à un système téléphonique classique.

Le protocole H.323 est une des normes envisageables pour la voix sur IP à cause de son développement inspiré de la téléphonie. Cependant, il est pour l'instant employé par des programmes propriétaires (Microsoft, etc.). La documentation est difficile d'accès car l'ITU fait payer les droits d'accès aux derniers développements de cette technologie, en dehors des efforts faits par le projet Open H.323 pour rendre cette technologie accessible à tous. Ainsi son adaptation au réseau IP est assez lourde. C'est pourquoi au fil des recherches est né le protocole SIP [3].

II.11.2 Protocole SIP

II.11.2.1 Historique

SIP (Session Initiation Protocol) a été normalisé par le groupe de travail WG MMUSIC (Work Group Multiparty Multimedia Session Control) de l'IETF. La version 1 est sortie en 1997, et une seconde version majeure a été proposée en mars 1999 (RFC 2543). Cette dernière a elle-même été largement revue, complétée et corrigée en juin 2002 (RFC 3261). Des compléments au protocole ont été définis dans les RFC 3262 à 3265.

SIP est au sens propre un protocole de signalisation hors bande pour l'établissement, le maintien, la modification, la gestion et la fermeture de sessions interactives entre utilisateurs pour la téléphonie et la vidéoconférence, et plus généralement pour toutes les communications multimédias.

Le protocole n'assure pas le transport des données utiles, mais a pour fonction d'établir la liaison entre les interlocuteurs. Autrement dit, il ne véhicule pas la voix, ni la vidéo, mais assure simplement la signalisation. Il se situe au niveau de la couche applicative du modèle de référence OSI et fonctionne selon une architecture client-serveur, le client émettant des requêtes et le serveur exécutant en réponse les actions sollicitées par le client.

SIP fournit des fonctions annexes évoluées, comme la redirection d'appel, la modification des paramètres associés à la session en cours ou l'invocation de services. En fait, SIP ne fournit pas l'implémentation des services, mais propose des primitives génériques permettant de les utiliser. De cette manière, l'implémentation des services est laissée libre, et seul le moyen d'accéder aux services est fourni.

Compatibilité:

L'un des grands atouts de SIP est sa capacité à s'intégrer à d'autres protocoles standards du monde IP. En tant que standard ouvert, il offre un service modulaire, prévu pour fonctionner avec différentes applications, telles que la téléphonie, la messagerie instantanée, la vidéoconférence, la réalité virtuelle ou même le jeu vidéo.

En fait, plus qu'une simple compatibilité, c'est la possibilité de l'utiliser en conjonction avec d'autres protocoles qui caractérise SIP. Le protocole s'insère comme une partie d'un ensemble plus générique, intitulé Internet Multimedia Conferencing Suite. À l'image de H.323, SIP est peu à peu devenu un protocole dit parapluie, qui encadre et rassemble plusieurs autres protocoles. SIP peut notamment se déployer ou s'intégrer aux protocoles suivants :

- **RTP** (Real-time Transport Protocol), RFC 3550, qui se charge du transport des flux temps réel.
- **RTCP** (Real-time Transport Control Protocol), RFC 3550, qui fournit des informations dynamiques sur l'état du réseau.
- **RTSP** (Real-Time Streaming Protocol), RFC 2326, pour contrôler la diffusion de flux multimédias en temps réel.
- **SDP** (Session Description Protocol), RFC 2327, qui fournit la description d'une session, c'est-à-dire les paramètres utilisés dans une communication SIP.
- **SAP** (Session Advertisement Protocol), RFC 2974, pour les communications multi-cast, qui permet d'ajouter les spécifications d'une nouvelle session.

- **MIME** (Multipurpose Internet Mail Extension), RFC 2045, standard pour les descriptions de contenus, utilisé sur Internet.
- **RSVP** (Resource reservation Protocol), RFC 2205, pour obtenir des garanties de qualité de service et effectuer des réservations de ressources.
- **HTTP** (HyperText Transfer Protocol), RFC 2616, pour le traitement des pages Web sur Internet (on peut inclure des adresses SIP directement dans des pages Web).
- **MGCP** (Media Gateway Control Protocol), RFC 3435, pour le contrôle des passerelles assurant la connectivité entre un réseau IP et un réseau téléphonique.

Tous ces protocoles sont d'une nature différente de celle de SIP, et ils n'interfèrent pas avec la signalisation. Leur utilisation conjointe est possible, voire recommandée pour certains d'entre eux. Cela dit, aucun d'eux n'est indispensable au bon fonctionnement de SIP, qui reste totalement indépendant à leur égard et autorise a priori n'importe quel autre protocole. Dans la pratique, nous verrons cependant que SIP est classiquement utilisé avec les mêmes protocoles.

Modularité :

Le protocole SIP se veut modulaire. Son objectif est de constituer une brique de base pouvant se combiner avec le maximum d'autres protocoles.

C'est la raison pour laquelle il a été conçu d'une manière indépendante de la couche de transport.

Les protocoles TCP et UDP sont donc tous deux supportés pour l'envoi de messages SIP.

UDP est généralement préférable pour laisser à l'application le contrôle des retransmissions de messages, et donc l'enchaînement des messages. Pour sa part, TCP est préférable pour la traversée de pare-feu, dans la mesure où les ports utilisés avec SIP sont dynamiques et où la notion d'état de connexion n'existe pas avec UDP.

Simplicité:

SIP affiche une grande simplicité, comme l'atteste la taille de la spécification du protocole, qui ne dépasse pas 153 pages dans sa première version (RFC 2543) et 269 pages dans la seconde (RFC 3261), ce qui reste nettement inférieur aux 763 pages de la spécification H.323. SIP utilise un langage textuel très proche des protocoles HTTP et SMTP, ce qui facilite son intégration à Internet. Par comparaison, le protocole H.323 utilise ASN.1, qui est un langage compilé.

La simplicité de SIP en fait un protocole facile à embarquer et un candidat de choix pour les composants légers, dotés de capacités réduites, comme les téléphones mobiles. Son implémentation est peu gourmande en ressources de traitement [5].

II.11.2.2-Architecture de SIP

Contrairement à H.323, largement fondé sur une architecture physique, le protocole SIP s'appuie sur une architecture purement logicielle.

L'architecture de SIP s'articule principalement autour des cinq entités suivantes :

- terminal utilisateur.
- serveur d'enregistrement.
- serveur de localisation.
- serveur de redirection.
- serveur proxy.

La figure II.6 illustre de façon générique les communications entre ces éléments. Un seul terminal étant présent sur cette figure, aucune communication n'est possible. Nous nous intéressons en fait ici aux seuls échanges entre le terminal et les services que ce dernier est susceptible d'utiliser lors de ses communications.

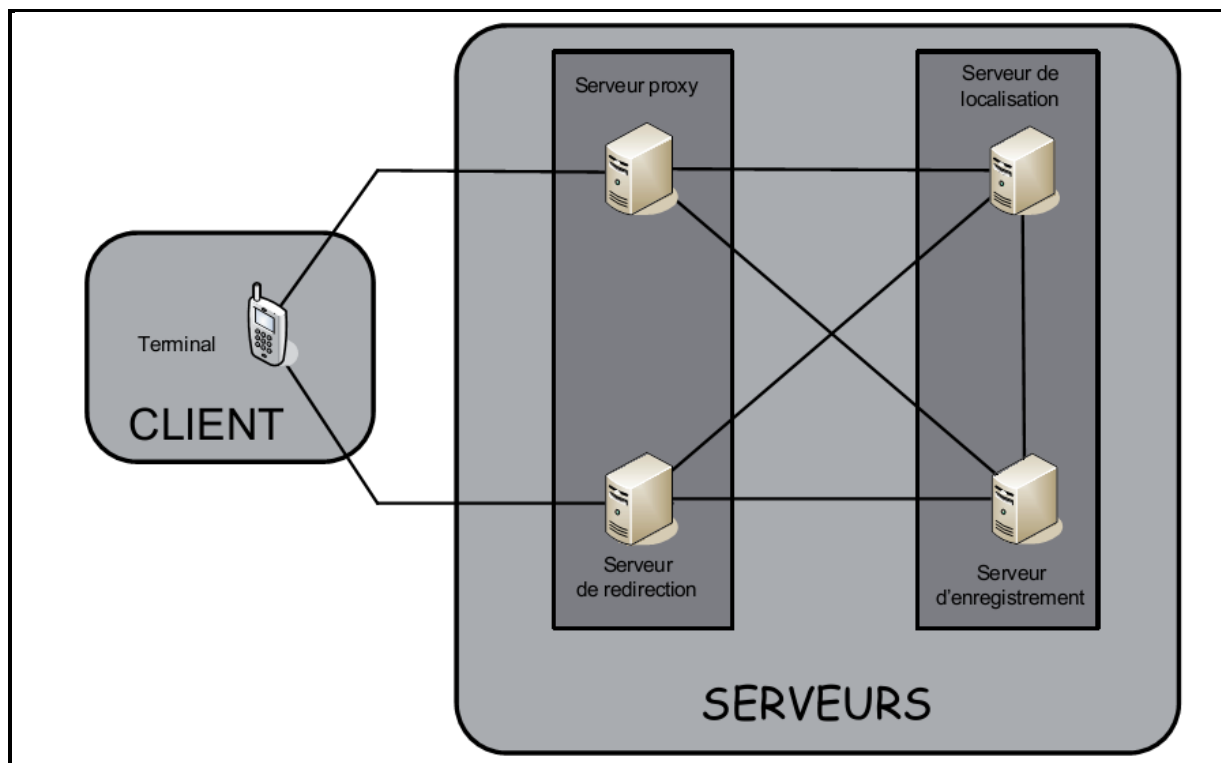


Figure II.7 : Architecture de SIP.

On peut schématiquement observer qu'il existe deux catégories de services : l'un fourni au niveau de l'utilisateur (par le terminal), l'autre fourni au niveau des serveurs du réseau. Ces derniers sont répartis en deux classes : les serveurs de redirection et proxy, qui facilitent le routage des messages de signalisation et jouent le rôle d'intermédiaires, et les serveurs de localisation et d'enregistrement, qui ont pour fonction d'enregistrer ou de déterminer la localisation des abonnés du réseau.

Terminal :

Le terminal est l'élément dont dispose l'utilisateur pour appeler et être appelé. Il doit donc permettre de composer des numéros de téléphone. Il peut se présenter sous la forme d'un composant matériel (un téléphone) ou d'un composant logiciel (un programme lancé à partir d'un ordinateur). Le terminal est appelé UA (User Agent). Il est constitué de deux sous-entités, comme illustré à la figure II.8 :

- Une partie cliente, appelée UAC (User Agent Client), chargée d'émettre les requêtes.

C'est l'UAC qui initie un appel.

- Une partie serveur, appelée UAS (User Agent Server), qui est en écoute, reçoit et traite les requêtes. C'est l'UAS qui répond à un appel. L'association des requêtes et des réponses entre deux entités de type UA constitue un dialogue.

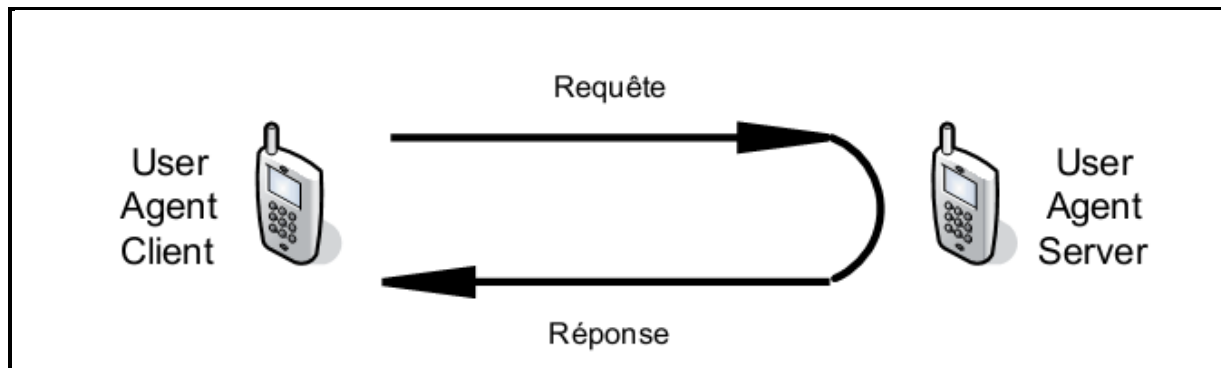


Figure II.8 UAC et UAS.

Par analogie, on peut remarquer que la même chose se produit avec le protocole http dans une application Web : un utilisateur exploite son navigateur comme client pour envoyer des requêtes et contacter une machine serveur, laquelle répond aux requêtes du client. La

différence essentielle par rapport aux applications standards utilisant HTTP est qu'en téléphonie un terminal doit être à la fois utilisé pour joindre un interlocuteur et pour appeler. Chaque terminal possède donc la double fonctionnalité de client et de serveur.

Lors de l'initialisation d'un appel, l'appelant exploite la fonctionnalité client de son terminal (UAC), tandis que celui qui reçoit la communication exploite sa fonctionnalité de serveur (UAS).

La communication peut être clôturée indifféremment par l'User Agent Client ou l'User Agent Server.

De nombreuses implémentations de clients SIP sont disponibles sur les plates-formes les plus courantes, Windows, Linux ou Mac. Elles sont le plus souvent gratuites, sous licence GPL.

Parmi les clients SIP les plus réputés, citons notamment les suivants :

- X-Lite Free
- Phone Gaim
- Wengo

Ces clients SIP disposent de diverses fonctionnalités améliorées. En choisir un est souvent affaire de goût, selon l'ergonomie du logiciel et les caractéristiques souhaitées (support d'un codec particulier, support de la messagerie instantanée, etc.).

Serveur d'enregistrement:

C'est un serveur qui accepte la requête REGISTRER. Il permet à un terminal de pouvoir s'enregistrer au serveur. Les positions actuelles sont stockées dans ce serveur ou transmises au serveur de localisation. Il peut offrir le service de localisation. L'enregistrement d'un utilisateur est constitué par l'association de son identifiant et de son adresse IP. Un utilisateur peut s'enregistrer sur plusieurs serveurs d'enregistrement en même temps. Dans ce cas, il est joignable simultanément sur l'ensemble des positions qu'il a renseignées.

Serveur de localisation:

Le serveur de localisation (Location Server) joue un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation de l'abonné.

Ce serveur contient la base de données de l'ensemble des abonnés qu'il gère. Cette base est renseignée par le serveur d'enregistrement. Chaque fois qu'un utilisateur s'enregistre auprès du serveur d'enregistrement, ce dernier en informe le serveur de localisation.

Presque toujours, le serveur de localisation et le serveur d'enregistrement sont implémentés au sein d'une même entité. On parle alors souvent non pas de serveur de localisation, mais de service de localisation d'un serveur d'enregistrement, tant ces fonctionnalités sont proches et dépendantes.

Les serveurs de localisation peuvent être collaboratifs. Le fonctionnement d'un serveur d'enregistrement est analogue à celui d'un serveur DNS dans le monde Internet : pour joindre un site Internet dont on ne connaît que le nom, il faut utiliser un serveur DNS, qui effectue la conversion (on parle de résolution) du nom en adresse IP. Ce serveur a connaissance d'une multitude d'adresses, qu'il peut résoudre parce qu'elles appartiennent à son domaine ou qu'il a la capacité d'apprendre dynamiquement en fonction des échanges qu'il voit passer. Dès qu'un nom lui est inconnu, il fait appel à un autre DNS, plus important ou dont le domaine est plus adéquat. De la même manière, les serveurs de localisation prennent en charge un ou plusieurs domaines et se complètent les uns les autres.

Serveur de redirection:

Le serveur de redirection (Redirect Server) agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur.

L'appelant envoie une requête de localisation d'un correspondant (il s'agit en réalité d'un message d'invitation, qui est interprété comme une requête de localisation) au serveur de redirection. Celui-ci joint le serveur de localisation afin d'effectuer la requête de localisation du correspondant à joindre. Le serveur de localisation répond au serveur de redirection, lequel informe l'appelant en lui fournissant la localisation trouvée. Ainsi, l'utilisateur n'a pas besoin de connaître l'adresse du serveur de localisation.

Serveur proxy:

Le serveur proxy (parfois appelé serveur mandataire) permet d'initier une communication à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux des interlocuteurs et agit pour le compte de ces derniers.

Le serveur proxy remplit les différentes fonctions suivantes :

- localiser un correspondant.
- réaliser éventuellement certains traitements sur les requêtes.

- initier, maintenir et terminer une session vers un correspondant.

Les serveurs proxy jouent aussi un rôle collaboratif, puisque les requêtes qu'ils véhiculent peuvent transiter d'un serveur proxy à un autre, jusqu'à atteindre le destinataire. Notons que le serveur proxy ne fait jamais transiter de données multimédias et qu'il ne traite que les messages SIP.

Le proxy est une entité très souvent utilisée dans la pratique. Par analogie avec l'architecture illustrée à la figure II.9, symbolisant l'organisation des communications, on parle souvent du trapèze SIP pour désigner l'ensemble formé par ces quatre entités.

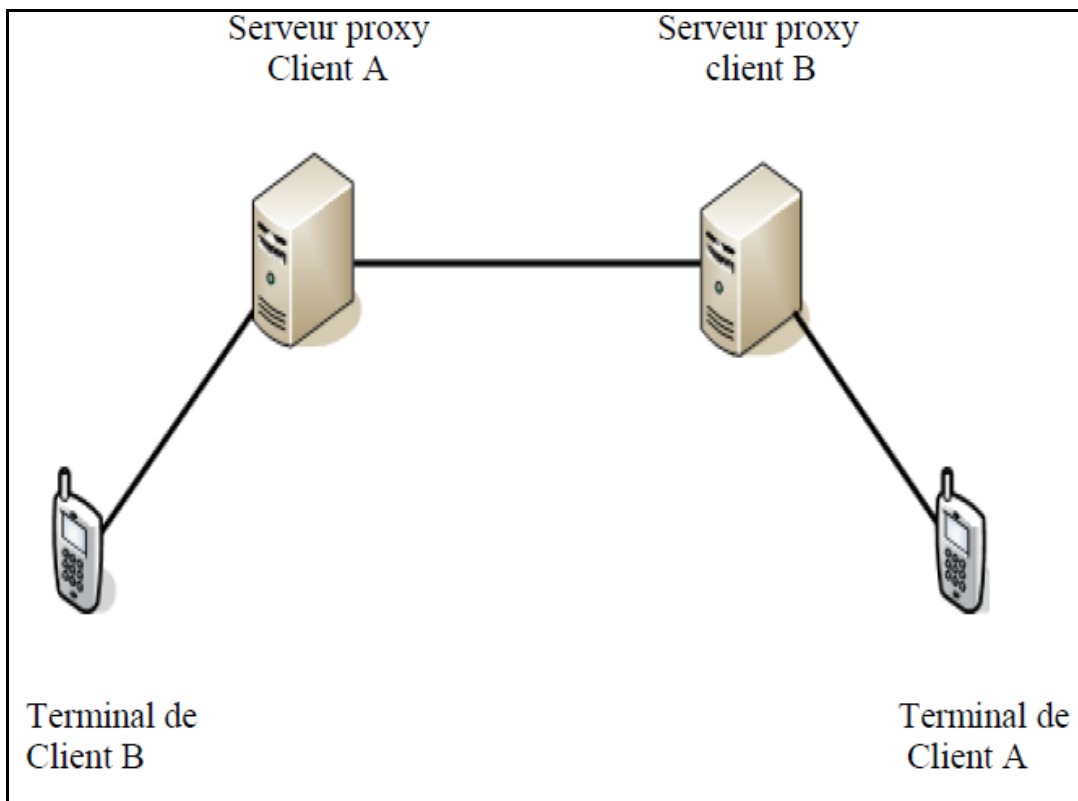


Figure II.9 Le trapèze SIP.

On distingue deux types de serveurs proxy :

- **Proxy statefull** qui maintient pendant toute la durée des sessions l'état des connexions.
- **Proxy stateless** qui achemine les messages indépendamment les uns des autres, sans sauvegarder l'état des connexions.

Les proxys stateless sont plus rapides et plus légers que les proxys statefull, mais ils ne disposent pas des mêmes capacités de traitement sur les sessions.

II.11.2.3 La connexion à des réseaux non-IP

SIP a été conçu initialement pour les réseaux à commutation de paquets de type IP, mais ses utilisateurs peuvent aussi joindre des terminaux connectés à des réseaux de nature différente. Pour cela, il est nécessaire de mettre en place des passerelles (Gateways), assurant la conversion des signaux d'un réseau à un autre. L'appel dans l'autre sens, c'est-à-dire d'un réseau non-IP vers un réseau à commutation de paquets, est tout aussi envisageable, à la seule condition que le terminal appelant dispose de la capacité d'entrer l'adresse de son correspondant SIP.

Cette adresse n'est généralement pas constituée uniquement de numéros, alors que la majorité des téléphones traditionnels actuels sont dépourvus de clavier. Plusieurs possibilités permettent de contourner cette difficulté, notamment la reconnaissance audio, la saisie d'une adresse à la manière d'un SMS ou l'attribution de numéros aux correspondants SIP [5].

II.11.2.4 L'adressage SIP

L'objectif de l'adressage est de localiser les utilisateurs dans un réseau. C'est une des étapes indispensables pour permettre à un utilisateur d'en joindre un autre.

Pour localiser les utilisateurs, il faut pouvoir les identifier de manière univoque. SIP propose des moyens très performants pour nommer les utilisateurs, grâce au concept d'URI, classique sur Internet, que nous allons détailler avant de voir son utilisation par SIP.

Un URI est formé d'une chaîne de caractères. Sa syntaxe a été définie au CERN (Centre Européen pour la Recherche Nucléaire) de Genève, par Tim Berners-Lee dès 1989, dans le cadre du système d'hyperliens (liens hypertextes) qu'il proposait la même année. Cette syntaxe a été normalisée par l'IETF en août 1998 dans la RFC 2396 puis révisée de nombreuses fois, notamment dans la RFC 2396bis, et reprise en janvier 2005 dans la RFC 3986.

Les URL (Uniform Resource Locator), que l'on manipule couramment dans l'adressage

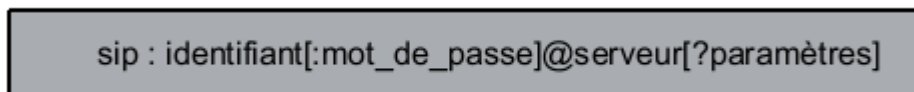
Web pour joindre un site Internet, constituent un sous-ensemble des URI. Elles ont pour fonction de spécifier une localisation relative à une ressource, ainsi que la méthode permettant d'y accéder (par exemple http, ftp, etc.).

À la différence d'un URI, une URL se contente d'apporter une localisation et non une définition de la ressource. Ainsi, un même document peut se trouver à deux emplacements différents, donc à deux URL différentes dans le réseau Internet, alors qu'il fait référence à une même ressource [5].

Format des adresses SIP:

Tout utilisateur SIP dispose d'un identifiant unique. Cet identifiant constitue l'adresse de l'utilisateur permettant de le localiser.

Le format d'une adresse SIP (ou URL SIP) respecte la RFC 3986 (nommée Uniform Resource Identifier: Generic Syntax) et se présente sous la forme illustrée à la figure II.10



```
sip : identifiant[:mot_de_passe]@serveur[?paramètres]
```

Figure II.10 Syntaxe d'une adresse SIP.

On distingue dans cette adresse plusieurs parties, telle que :

Le mot-clé sip : qui spécifie le protocole à utiliser pour la communication. Par analogie avec le Web, le mot-clé *sip* précise que ce qui va suivre est l'adresse d'un utilisateur ;

La partie identifiant : qui définit le nom ou le numéro de l'utilisateur. Cet identifiant est nécessairement unique pour désigner l'utilisateur de manière non ambiguë ;

La partie mot_ de_passe : qui est facultative. Le mot de passe peut être utile pour s'authentifier auprès du serveur, notamment à des fins de facturation. C'est aussi un moyen pour joindre un utilisateur qui a souhaité s'enregistrer sur l'équivalent d'une liste rouge : sans la connaissance de ce mot de passe, le correspondant n'est pas joignable.

De manière générale, cette possibilité offre le moyen de restreindre l'utilisation de certains services.

La partie serveur : qui spécifie le serveur chargé du compte SIP dont l'identifiant précède l'arobase. Le serveur est indiqué par son adresse IP ou par un nom qui sera résolu par DNS. Des paramètres URI peuvent être associés à ce nom. C'est ce serveur qui sera contacté pour joindre l'abonné correspondant. Un port peut être spécifié à la suite du serveur ;

La partie paramètres : est facultative. Les paramètres permettent soit de modifier le comportement par défaut (par exemple, en modifiant les protocoles de transport ou les ports, ou encore le TTL par défaut), soit de spécifier des informations complémentaires (par exemple, l'objet d'un appel qui sera envoyé à l'appelé en même temps que l'indication d'appel, à la manière d'un e-mail précisant l'objet du message).

On retiendra deux avantages de l'adressage SIP :

- L'adressage est indépendant de la localisation géographique des abonnés. SIP est conçu pour assurer la mobilité de ses utilisateurs, et donc permettre de joindre quelqu'un avec une adresse SIP unique, quels que soient sa localisation et son terminal. Le réseau peut toutefois adopter un plan de numérotation selon n'importe quel critère, comme la localisation géographique, sans que cela soit gênant.
- Un utilisateur peut avoir plusieurs adresses SIP aboutissant toutes au même terminal.

Par exemple, si quelqu'un souhaite différencier son adresse SIP professionnelle de son adresse SIP personnelle, il peut utiliser un même terminal référencé sur deux adresses distinctes. Il lui est alors possible d'activer la messagerie de son compte personnel pendant son travail et, le week-end, de rediriger les appels sur son adresse professionnelle vers un centre de permanence. Le tout en utilisant un terminal unique.

Ce mécanisme d'adressage particulièrement souple permet de supporter la mobilité des utilisateurs et le monde Internet [5].

II.11.2.5 Structure de message SIP

Les messages SIP sont codés en utilisant la syntaxe de message HTTP/1.1 (RFC2068). Il existe deux types de message, les requêtes et les réponses. La structure de message est présentée comme la figure suivante:

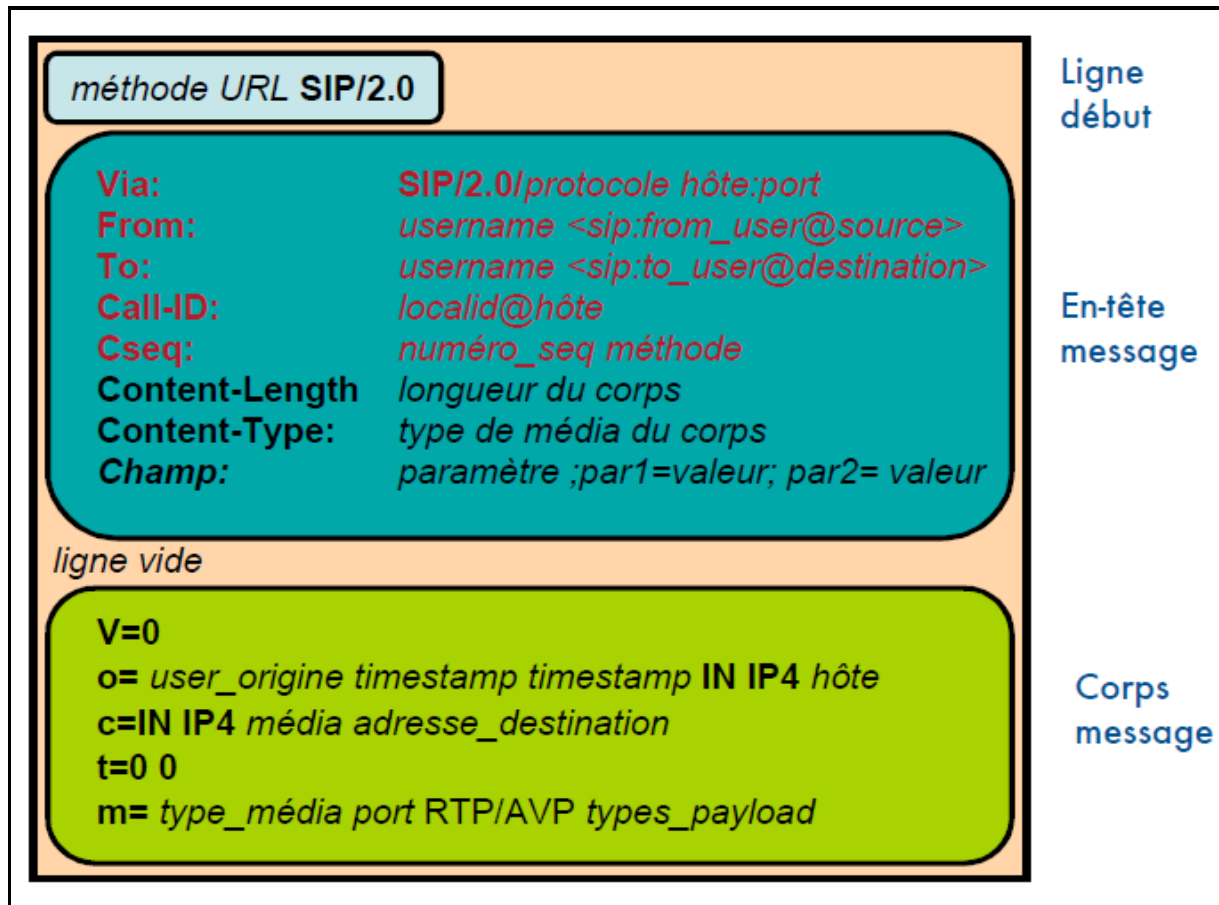


Figure II.11 Format générique d'un message SIP.

L'en-tête d'un message:

Il y a certains des champs d'en-têtes qui sont présents toujours dans les requêtes et les réponses, et forment l'en-tête (header) :

- **Call-ID**: Ce champ d'en-tête contient un identificateur globalement unique pour un appel.
- **Cseq**: il est un identificateur qui sert à rapprocher

- **From:** Il identifie l'appelant. Il doit présenter dans toutes les requêtes et les réponses.
- **To :** ce champ doit présenter dans toutes les requêtes et en indique la destination. Il est simplement copié dans les réponses.
- **Via :** Le champ Via est utilisé pour enregistrer la route d'une requête, de manière à permettre aux serveurs SIP intermédiaires de faire suivre aux réponses un chemin exactement inverse.
- **Content-Type:** Ce champ d'en-tête décrit le type de média contenu dans le corps message.
- **Content-Length :** il s'agit du nombre d'octets du corps du message, si le message ne comprend aucun corps la valeur 0 est utilisé.
- **Le champ Max-Forwards :** doit être utilisée pour toute requête pour limiter le nombre de serveurs SIP qui peut être traversé jusqu'à destination. Chaque serveur recevant une requête devra décrémenter la valeur du champ Max-Forwards. Si un serveur reçoit une requête avec un champ Max-Forwards égal à 0, il renvoie une réponse 483 Too Many Hops.
- **Champ Subject :** Le champ Subject fournit un résumé ou indique la nature de l'appel, autorisant ainsi le filtrage sans avoir à analyser la description de la session. La description de la session ne doit pas nécessairement utiliser le même sujet dans l'invitation [4].

Corps d'un message:

Le corps d'un message SIP contient le descriptif complet des paramètres de la session concernée. Typiquement, une description de la session à ouvrir comporte les informations suivantes :

- informations générales sur la session (nom de la session, date de la session, objet de la session, etc.).
- informations sur l'émetteur du message (nom, e-mail, numéro de téléphone, etc.) ;
- informations réseau (ressources nécessaires, protocole et port utilisés pour le transport des données multimédias, etc.).

- liste des flux multimédias utilisés (audio, vidéo, texte).
- liste des codages supportés (G.711, G.729, H.216, MPEG, etc.).
- informations de sécurité (type de cryptage utilisé) [5].

Champ SDP	Correspondance	Type d'information	Descriptif
V	PROTOCOL VERSION	Description de session	Version du protocole
O	OWNER/ CREATOR AND SESSION IDENTIFIER	Description de session	origine du message
S	SESSION NAME	Description de session	sujet du message
c	CONNECTION INFORMATION	Description de session et de média	Adresse réseau avec laquelle s'effectue la connexion.
t	TIME	Description temporelle	Date d'activité de la session
M	MEDIA NAME AND TRANSPORT ADDRESS	Description de média	Type de média utilisé et adresse de transport
a	SESSION	Description de	Attributs de média

	ATTRIBUTE	session et de média	
--	-----------	---------------------	--

Tableau II.3 Champs SDP les plus courants.

II.11.2.6 Les Requêtes SIP

La version actuelle de SIP prévoit 6 requêtes distinctes, permettant l'établissement d'un appel, la négociation des capacités (types de média, paramètres de la session, éléments de sécurité) ou la fermeture d'une session. Ces requêtes sont détaillées dans le tableau II.4. [3].

Requête	Définition
INVITE	Requête d'établissement d'une session, invitant un usager (humain ou non) à participer à une communication téléphonique ou multimédia ; l'émetteur de cette requête y indique les types de média qu'il souhaite et peut recevoir, en général au travers d'une description de session SDP (Session Description Protocol).
ACK	Requête d'acquiescement, émise pour confirmer que le client émetteur d'un INVITE précédent a reçu une réponse finale ; cette requête peut véhiculer une description de session qui clôt la négociation.
BYE	Requête de clôture d'un appel.
CANCEL	Requête d'annulation, signifiant au serveur de détruire le contexte d'un appel en cours d'établissement (cette requête n'a pas d'effet sur un appel en cours).
OPTIONS	Cette requête permet à un client d'obtenir de l'information sur les capacités d'un usager, sans pour autant provoquer l'établissement d'une session.
REGISTER	Requête à destination d'un serveur SIP et permettant de lui faire parvenir de l'information de localisation (machine sur laquelle se trouve l'utilisateur).

Tableau II.4 Les requêtes SIP.

II.11.2.7 Les réponses SIP

Après réception et traitement d'une requête, un agent ou un serveur SIP génère un message de réponse (succès ou échec du traitement). Ces réponses sont codées par une séquence de trois chiffres, où le premier est un code de classe. Le tableau II.5 donne quelques réponses SIP possibles [3].

Code	Définition de la famille de réponse	Principales réponses
1XX	Réponse intermédiaire d'information (traitement en cours)	100 Trying 180 Ringing 183 En progression
2XX	Succès	200 OK 202 Accepté
3XX	Redirection	300 Changement de localisation 302 Choix multiples 305 Utiliser un proxy
4XX	Erreur client	400 Bad Request 401 Non autorisé 403 Interdit 415 Type de média non supporté 486 Occupé 428 Utilise un en-tête d'identité
5XX	Erreur serveur	501 Non implémenté 503 Service non disponible
6XX	Echec global du traitement	600 Occupé 603 décline

Tableau II.5 Les réponses SIP.

II.11.2.8 Scénarios de communication

Nous allons illustrer la succession chronologique des messages de requêtes et de réponses dans les six scénarios classiques suivants :

1. Initialisation d'une communication directe.
2. Enregistrement d'un terminal.
3. Initialisation d'une communication avec un serveur proxy.
4. Localisation par un serveur de redirection et initialisation d'appel directe.
5. Modification dynamique d'une communication SIP.
6. Terminaison d'une communication [5].

II.11.2.9 Les modes de communication dans le protocole SIP

Deux modes de communication sont effectués dans le protocole SIP :

Mode Point à point :

Le mode point à point est donc une communication simple entre deux sans passer par une passerelle.

Pour ouvrir une session, un utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de s'accorder sur la comptabilité de leur média. L'appelant et l'appelé doivent être identifiés via son URL SIP. Pour le mode point à point on utilise donc l'adresse IP du poste à joindre dans le logiciel de communication. Pour ouvrir une session, l'appelant envoie une requête contenant l'URL SIP du destinataire. Lors de la mise en place de cette communication, plusieurs paquets sont échangés entre les deux postes :

Invite : Permet d'informer le destinataire qu'une communication veut être établie avec lui et l'appelant.

Trying : Essai d'établir la connexion,

Ringing : Emet une sonnerie en attendant le décrochage du combiné distant.

OK : Permet d'acquitter une fois le combiné distant décroché.

ACK : Cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête Invite.

BYE : Cette requête est utilisée par le terminal de l'appelé à fin de signaler qu'il souhaite mettre un terme à la session.

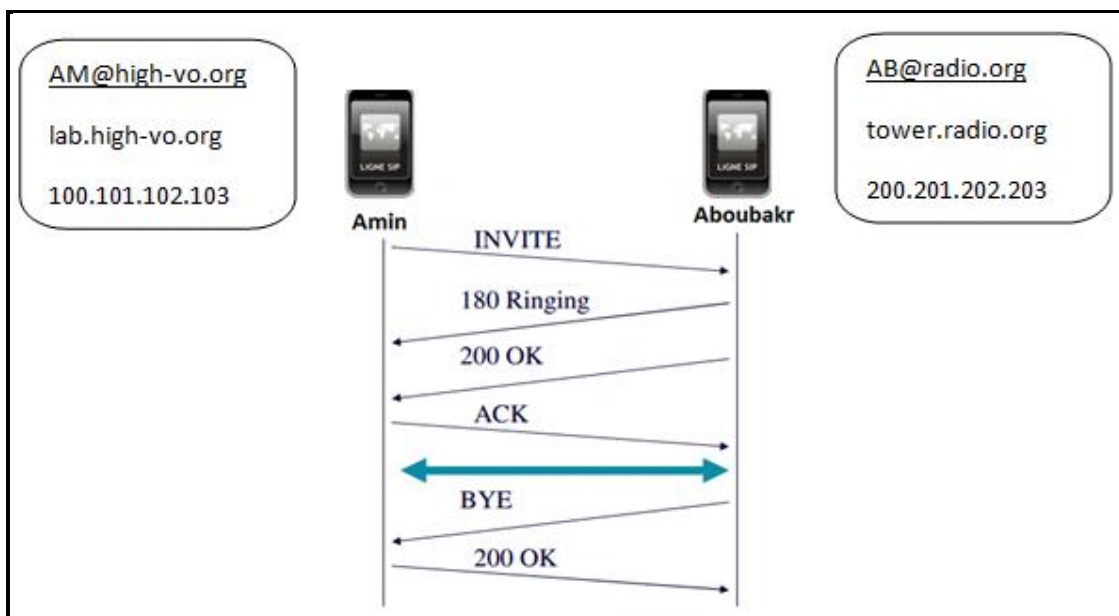


Figure II.12 Les paquets de Mode Point à Point.

Un exemple de message INVITE :

```
INVITE sip:AB@radio.org SIP/2.0
Via: SIP/2.0/UDP lab.high-vo.org:5060; branch=z9hG4bKfw19b
Max-Forwards: 70
To: B.AB <sip:AB@radio.org>
From: A.AM <sip:A.AM@high-vo.org>;tag=76341
Call-ID: 123456789@lab.high-vo.org
CSeq: 1 INVITE
Subject: About That Power Outage...
Contact: <sip:A.AM@lab.high-vo.org>
```

```

Content-Type: application/sdp
Content-Length: 158
v=0
o=AM 2890844526 2809844526 IN IP4 lab.high-vo.org
s=Phone Call
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000

```

Mode diffusif :

Le mode diffusif, contrairement au mode point à point, utilise une passerelle pour réaliser une communication entre deux éléments. Les clients sont enregistrés sur un serveur qui va les identifier par rapport à un numéro. Lorsqu'un client veut appeler quelqu'un, il ne va donc plus utiliser l'adresse IP mais son identifiant.

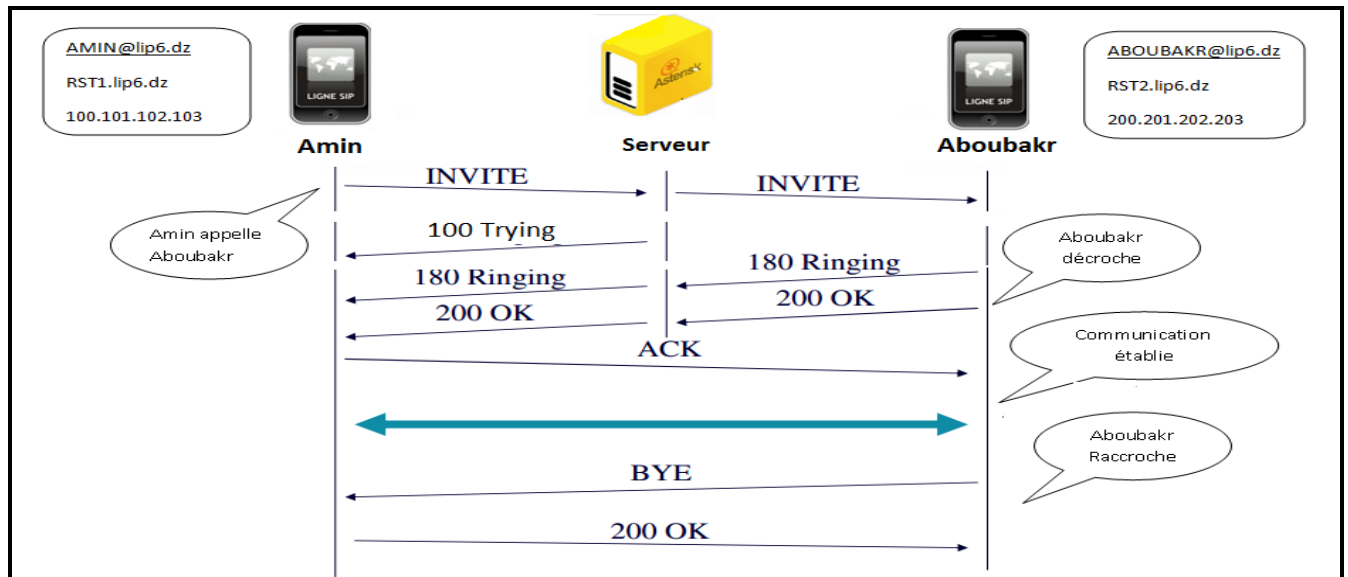


Figure I. 13 Les paquets de Mode diffusif

Un exemple de message INVITE AMIN → Proxy :

```

INVITE sip: ABOUBAKR@lip6.dz SIP/2.0
Via: SIP/2.0/UDP 100.101.102.103:5060; branch=z9hG4bKmp17a
Max-Forwards: 70
To: ABOUBAKR <sip: ABOUBAKR@lip6.dz>

```

From: AMINE <sip: AMIN@lip6.dz>; tag=42
Call-ID: 10@100.101.102.103
CSeq: 1 INVITE
Subject: Where are you?
Contact: <sip:AMIN@RST1.lip6.dz>
Content-Type: application/sdp
Content-Length: 159
v=0
o=AMINE 2890844526 2890844526 IN IP4 100.101.102.103
s=Phone Call
t=0 0
c=IN IP4 100.101.102.103
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000

Un exemple de message INVITE Proxy → ABOUBAKR :

INVITE sip: ABOUBAKR @100.101.202.203 SIP/2.0
Via: SIP/2.0.UDP proxy.lip6.dz:5060; branch=z9hG4bK83842.1
Via: SIP/2.0/UDP 100.101.102.103:5060; branch=z9hG4bKmp17a
Max-Forwards: 69
To: ABOUBAKR <sip:ABOUBAKR@lip6.dz>
From: AMINE <sip:AMIN@lip6.dz>;tag=42
Call-ID: 10@100.101.102.103
CSeq: 1 INVITE
Subject: Where are you?
Contact: <sip:AMIN@RST1.lip6.dz>
Content-Type: application/sdp
Content-Length: 159
v=0
o=AMINE 2890844526 2890844526 IN IP4 100.101.102.103
s=Phone Call
t=0 0
c=IN IP4 100.101.102.103
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000

Pourquoi un serveur proxy SIP? :

- Adresse IP n'est pas fixe comme un numéro de téléphone.
- Adresse IP est souvent attribuée dynamiquement à une machine via DHCP.

- SIP UA de l'appelant ne connaît pas toujours l'adresse IP de l'appelé pour envoyer le message INVITE.
- Serveur proxy SIP est une entité intermédiaire pour orienter les requêtes SIP vers le destinataire dans ce cas là.
- Serveur proxy n'initie ni termine une session mais seulement retransmet les messages SIP.
- Il est possible d'avoir plusieurs serveurs proxy dans un chemin de signalisation.

II.11.2.10 Avantage et inconvénients du protocole SIP

Avantages :

L'implémentation de la VoIP avec le protocole de signalisation SIP (Session Initiation Protocol) fournit un service efficace, rapide et simple d'utilisation. SIP est un protocole rapide et léger. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau.

Les utilisateurs s'adressent à ces serveurs Proxy pour s'enregistrer ou demander l'établissement de communications. Toute la puissance et la simplicité du système viennent de là. On peut s'enregistrer sur le Proxy de son choix indépendamment de sa situation géographique. L'utilisateur n'est plus "attaché" à son autocommutateur.

Une entreprise avec plusieurs centaines d'implantations physique différente n'a besoin que d'un serveur Proxy quelque part sur l'Internet pour établir son réseau de téléphonie gratuit sur l'Internet un peu à la manière de l'email. Les dizaines de milliers d'autocommutateurs peuvent être remplacés par quelques serveurs proxy.

On imagine bien la révolution. Mais comme d'habitude rien n'empêchera de remplacer un autocommutateur par un serveur Proxy réduisant ainsi l'intérêt du système. SIP est un

protocole indépendant de la couche transport. Il peut aussi bien s'utiliser avec TCP que le protocole UDP.

Inconvénients :

L'une des conséquences de cette convergence est que le trafic de voix et ses systèmes associés sont devenus aussi vulnérables aux menaces de sécurité que n'importe quelle autre donnée véhiculée par le réseau.

En effet, SIP est un protocole d'échange de messages basé sur HTTP. C'est pourquoi, il est très vulnérable face à des attaques de types DoS (Dénis de Service), détournement d'appel, trafic de taxation, etc. De plus, le protocole de transport audio associé RTP (Real Time Protocol) est lui aussi très peu sécurisé face à l'écoute indiscreète ou des DoS.

Le SIP est une norme pour la communication multimédia, il devient de plus en plus utilisé pour la mise en place de la téléphonie sur IP, la compréhension de ce protocole aidera le professionnel à l'épreuve de la sécurité sur le réseau .Ce protocole est un concurrent direct à H.323 [3].

II.12 Comparaison entre le protocole SIP et H.323

Les deux protocoles SIP et H323 représentent les standards définis jusqu'à présent pour la signalisation à propos de la téléphonie sur Internet .Ils présentent tous les deux des approches différentes pour résoudre un même problème. H323 est basé sur une approche traditionnelle du réseau à commutation de circuits. Quant à SIP, il est plus léger car basé sur une approche similaire au protocole http.

Tous les deux utilisent le protocole RTP comme protocole de transfert des données multimédia.

Au départ, H323 fut conçu pour la téléphonie sur les réseaux sans QoS, mais on l'adopta pour qu'il prenne en considération l'évolution complexe de la téléphonie sur internet.

Pour donner une idée de la complexité du protocole H323 par rapport à SIP, H323 est défini en un peu plus de 700 pages et SIP quand à lui en moins de 200 pages. La complexité de

H323 provient encore du fait de la nécessité de faire appel à plusieurs protocoles simultanément pour établir un service, par contre SIP n'a pas ce problème.

SIP ne requiert pas de comptabilité descendante, c'est un protocole horizontal qui est le contraire de H323 : Les nouvelles versions de H323 doivent tenir compte des anciennes versions pour continuer à fonctionner. Ceci entraîne pour H323 de traîner un peu plus de codes pour chaque version.

H323 ne reconnaît que les Codecs standardisés pour la transmission des données multimédias proprement dit alors que SIP, au contraire, peu très bien en reconnaître d'autres. Ainsi, on peut dire que SIP est plus évolutif que H323. Le tableau II.6 nous donne l'approche comparative du protocole SIP et du protocole H.323 [4].

	H.323	SIP
Architecture	Pile de protocoles Point à Point	Eléments Client/ Serveur
Origine	ITU	IETF
Protocole de transport	TCP (Version 1,2) UDP (Version 3...)	Utiliser n'importe quel protocole de transport
Codage de message	Binaire ASN.1	Texte
Dérivé de	Téléphonie	Multimédia/internet
Serveur	Gatekeeper	Serveur de localisation Serveur d'enregistrement Serveur de redirection Proxy
Etablir un appel	Q.931/RAS	SIP

Etablir flux média	H.245 Code connue Négocié pour choisir le codeur pertinent Canal logic	SDP n'importe quel code
Délai d'appels	V1 6 - 7 RT V2 3 - 4 RT V3 2 - 3 RT	2 - 3 RT
Terminal	Terminal H.323	Agent d'utilisateur

Tableau II.6 Tableau de comparaison entre le protocole SIP et H.323

Conclusion

La VoIP est une technologie émergente et qui tente plusieurs entreprises de l'exploiter vu les avantages qu'elle présente. En Algérie, cette technologie n'est pas encore très bien développée vu l'absence des fournisseurs de VoIP. Cependant, il est possible de déployer quelques applications de cette technologie au sein des entreprises multi-sites ce qui nous permettra de migrer les communications du réseau RTC vers le réseau IP.

Dans le chapitre suivant, on va entamer la partie environnement matériel et logiciel de ce travail.

Chapitre III

Environnement matériel et logiciel

Introduction

Il existe plusieurs logiciels qui permettent d'implémenter une solution VoIP dans une entreprise, que ça soit dans le monde libre, ou dans le monde des logiciels propriétaires.

Dans ce chapitre, une brève présentation sur un PABX, un logiciel Asterisk qu'il suffit d'installer sur un ordinateur, librement et gratuitement, avant de s'intéresser au Java Media Framework et à la configuration d'un client X-lite.

III-1 Principes de base d'un PABX

Un PABX est un autocommutateur téléphonique privé (définition anglaise : Private Automatic Branch eXchange) destiné à alimenter et à mettre en relation une certaine quantité de postes téléphoniques internes dans une entreprise ou dans une administration. Un PABX, travaille aussi bien en numérique qu'en analogique.

Les raccordements opérateurs les plus courants sont le RTC (ligne analogique) et le RNIS (NUMERIS en T0 ou T2).

Le PABX est un commutateur spécialisé de voix et/ou de DATA. Il existe plusieurs types de générations:

- Commutation spatiale, électronique ou électromécanique (première génération).
- Commutation de données ou temporelle (deuxième génération).
- Commutation temporelle avec multiplexage de la voix et de la donnée (troisième génération) autorisant des liaisons MICS opérateurs à 2Mbits/s, avec l'apparition des premiers CODEC.
- Commutation numérique (fonctionne par tri et commutation des paquets 64 Kbits/s et X25 entre les différentes interfaces).

Un autocommutateur privé possède sa propre intelligence pour faciliter la commutation des appels voix.

➤ Il existe deux sortes de PABX :

- Les PABX traditionnels ceux que l'on appelle de génération TDM (Time Division Mltiplexing), qui peuvent éventuellement migrer partiellement ou totalement en IP (sur certaines gammes seulement),

- les PABX-IP ou IPBX ou PBXIP (qui nativement offrent une connectivité IP Ethernet afin d'offrir des services de téléphonie sur IP).
- Les IPBX peuvent actuellement se présenter sous la forme d'un PC traditionnel équipé d'un logiciel Asterisk par exemple (Open Source), et de cartes d'entrées/sorties RNIS et/ou analogiques.

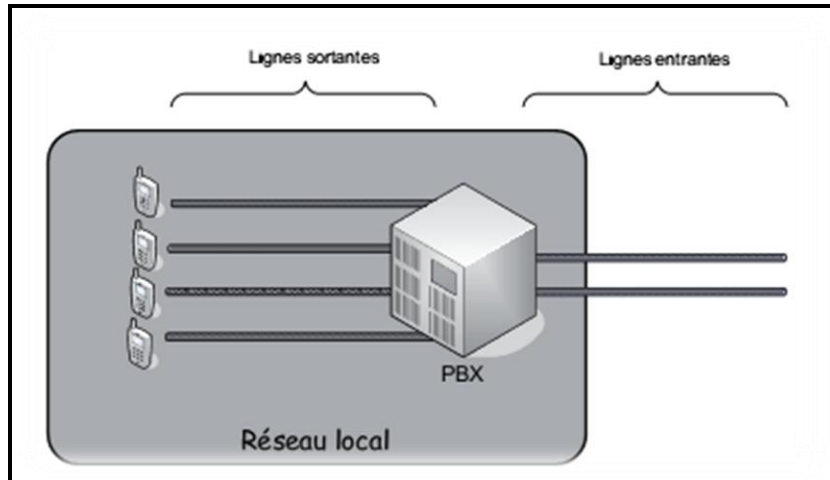


Figure III.1 PBX pour la gestion des appels.

III 2 Quelles sont les gammes ?

Il existe quatre gammes principales de PABX ou d'autocommutateur privé :

- 1) Les microcommutateurs (en général, jusqu'à 5 ou 10 postes internes).
- 2) Les autocomms de petite capacité (de 10 à 50 postes environ).
- 3) Les autocomms de moyenne capacité (50 à 350 postes environ).
- 4) Les autocomms de grande capacité (de 350 jusqu'à plusieurs milliers de postes).

Plusieurs gammes sont disponibles dans tous les pays et dans toutes les langues (versions export).

III-3 Les Principes De Bases

- Simplifier le flux de vos communications.
- Attribuer une ligne directe à chaque poste.
- Permettre les appels d'un poste à l'autre.
- assurant automatiquement les connexions téléphoniques entre appelé et appelant (à l'intérieur de l'entreprise comme vers l'extérieur).

Remarque : les fonctionnalités attendues d'un autocommutateur privé dépendent :

- du budget.
- du choix du constructeur (et donc du modèle),

- et surtout du besoin initial du demandeur (dans certains cas, une étude s'impose avant tout achat et/ou rédaction d'un AO).

C'est un peu comme l'achat d'une voiture, il faut ou non acquérir des options (suivant le choix du constructeur) [6].

III.4 Asterisk

III.4.1 Historique

Asterisk C'est un logiciel "Open Source", développé en langage C sous Linux par Mark Spencer de la société américaine Digium Inc (devenu le sponsor d'Asterisk), Il est apparu dans l'année 2002.

Avec l'effort employé par des utilisateurs, Asterisk a atteint une maturité et a gagné la confiance des utilisateurs. Cette réussite est due à l'amélioration du code source, la rédaction des documentations, l'existence de l'aide en ligne, la correction de certains bugs.

III.4.2 Définition

Asterisk est un commutateur téléphonique privé à part entière mais d'implémentation logicielle, compatible Linux, qui s'interconnecte avec quasiment tous les équipements de téléphonie de base standard et peu coûteux, a été développé par Mark Spencer à l'origine, de l'entreprise Digium, (anciennement Linux Support Services Inc.) et qui continue, grâce à de nombreux contributeurs, à évoluer régulièrement. Ce logiciel a été conçu pour une flexibilité maximale et reste un système ouvert à de nouvelles applications.

III.4.3 Rôle

Asterisk est IP-PBX qui transforme un ordinateur en "central téléphonique" ou "PABX" (Private Automatic Branch eXchange), autocommutateur téléphonique privé .Ce PABX est un commutateur qui relie dans une entreprise les appels d'un poste quelconque vers un autre (appels internes) ou avec un réseau téléphonique public (appels externes).

Asterisk a le rôle d'un middleware entre les technologies de téléphonie VOIP (TDM, SIP ...) et les applications (conférence, messagerie vocale, ...). Ce PBX est basé sur le protocole IP. Donc les communications et les paquets échangés sont transportés sous forme plusieurs protocoles de la voix qu'on veut (SIP, H.323, ADSI, MGCP) [6].

III.4.4 Les principes de fonctionnement d'Asterisk

Asterisk offre toutes les fonctions d'un PBX et ses services associés :

- **Les principes de fonctionnement:**

- Appels en mode conférence (et visioconférence)
- Messagerie SMS
- Insertion et Redirection des messages vocaux par courriel
- Interface Web pour la gestion des messages
- Listes noires
- Identification de l'appelant sur appel en attente
- les répondeurs interactifs.
- la mise en attente d'appels.
- la distribution des appels.
- la musique d'attente.
- la génération d'enregistrement d'appels pour l'intégration avec des systèmes de facturation.
- Asterisk fonctionne sur les principaux systèmes d'exploitation (Linux, BSD, Windows, Mac OS X).

Ces protocoles gèrent la communication et le transport entre les correspondants :

H.323: il est assez complexe, présente des failles et il est rarement utilisé car il est remplacé par SIP.

SIP (Session Initiation Protocol) : il est beaucoup utilisé pour la voix sur IP, il est apprécié pour sa simplicité, il ressemble à http, FTP.

IAX (Inter Asterisk eXchange): il est développé par Digium pour permettre le dialogue entre serveurs Asterisk. Il est plus simple et rapide que SIP. Donc c'est un protocole propre à Asterisk.

MGCP (Media Gateway Control Protocol).

SCCP (Skinny Client Control Protocol): protocole propriétaire de Cisco.

Asterisk peut également jouer le rôle de registre et passerelle avec les réseaux publics (RTC, GSM, etc.). « Il peut être utilisé dans la téléphonie d'entreprise en interne comme en externe. Ainsi, une entreprise multi site pourra utiliser Asterisk pour ses communications entre sites et ainsi économiser tous les frais de télécommunication ».

III.4.5 Protocole IAX/IAX2

Inter-Asterisk EXchange protocol est un protocole utilisé par les serveurs PBX open source Asterisk et les clients qui leurs sont associés.

Grâce à ce protocole, Asterisk permet de déployer des passerelles d'interconnexion vers la téléphonie classique ainsi que vers d'autres protocoles de téléphonie sur IP.

Le protocole IAX2 est une alternative au protocole SIP. Il s'agit du protocole sur lequel s'appuie Asterisk. Il utilise un port UDP unique qui est le port 4569 (IAX1 utilisait le port 5036) et ceci marque l'une des grandes différences avec le protocole SIP. En effet, le protocole SIP, est célèbre pour sa principale limite qui est la difficulté à l'implémenter derrière un NAT. IAX2 ne rencontre nullement ce problème de NAT d'où son principal succès [7].

III.4.6 Architecture d'asterisk

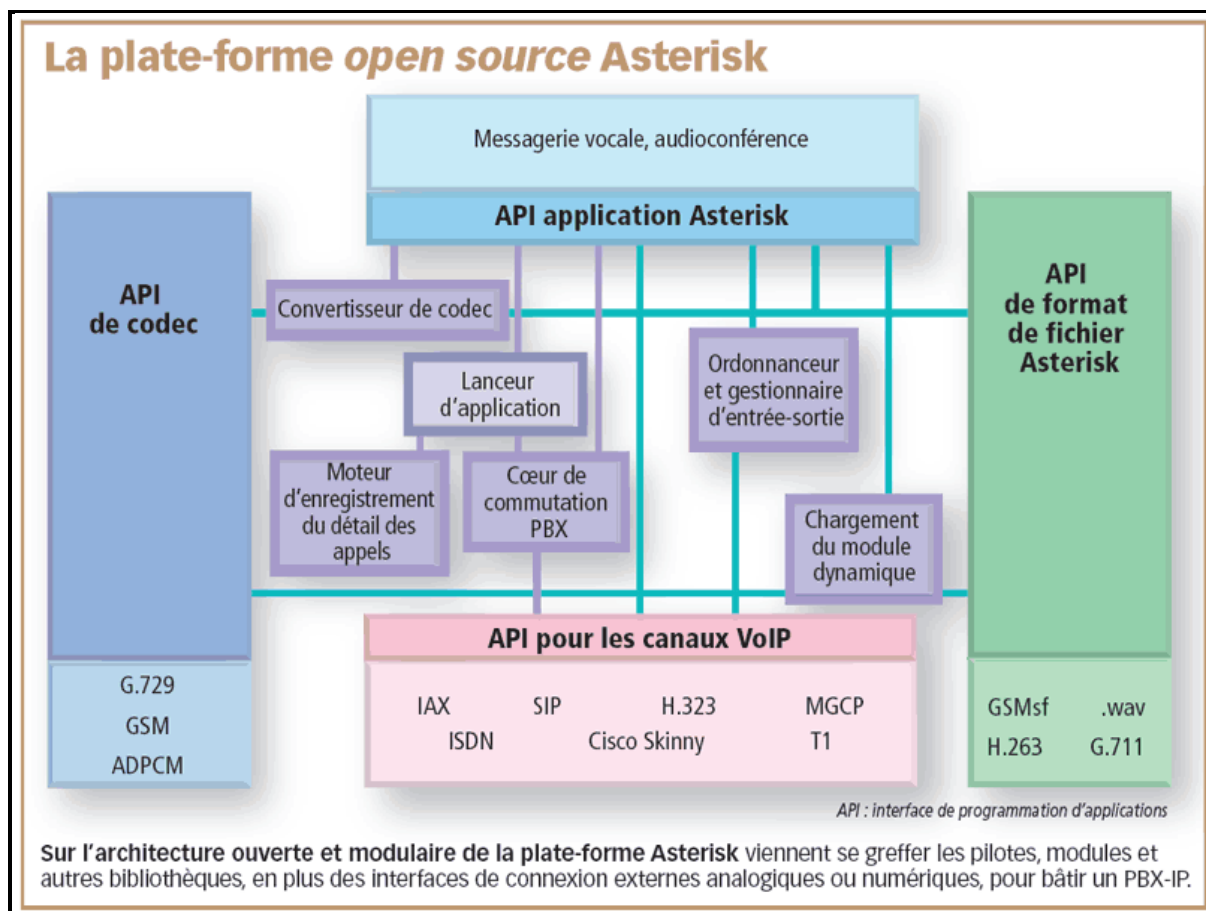


Figure III.2 Architecture interne d' Asterisk.

Asterisk est composé d'un noyau central de commutation, de quatre API (Interface de programmation d'applications) de chargement modulaire des applications téléphoniques, des interfaces matérielles, de traitement des formats de fichier, et des codecs. Il assure la commutation transparente entre toutes les interfaces supportées, permettant à cette

commutation de relier entre eux une diversité de systèmes téléphoniques en un unique réseau commuté.

III.4.7 Les Composants d'asterisk

III.4.7.1 Le noyau

Le noyau central contient 5 moteurs ayant chacun un rôle essentiel et critique dans les opérations :

Cœur de commutation PBX (PBX Switching Core) :

Système de commutation de central téléphonique privé, reliant ensemble les appels entre divers utilisateurs et des tâches automatisées. Le noyau de commutation relie d'une manière transparente des appels arrivant sur divers interfaces de matériel et de logiciel.

Lanceur d'applications (Application Launcher) :

Lance les applications qui assurent des services pour des usagers, tels que la messagerie vocale, la lecture de messages et le listage de répertoires (annuaires).

Traducteur de codec (Codec Translator) :

Utilise des modules de codec pour le codage et le décodage de divers formats de compression audio utilisés dans l'industrie de la téléphonie. Un certain nombre de codecs sont disponibles pour palier aux divers besoins et pour arriver au meilleur équilibre entre la qualité audio et l'utilisation de la bande passante.

Ordonnanceur et gestionnaire d'entrée/sortie (Scheduler & I/O Manager) :

Ils traitent la planification des tâches de bas niveau et la gestion du système pour une performance optimale dans toutes les conditions de charge.

Dynamic Module Loader (chargement de module dynamique) :

Charge les pilotes (lors de la 1ère exécution d'Asterisk, il initialise les pilotes et fait le lien avec les APIs appropriés).

Enregistrement des détails d'appel (Call Data Record) : application pour enregistrer les détails d'appel.

III.4.7.2 Les APIs

L'API application (Asterisk Application API) :

Elle autorise différents modules de tâches à être lancé pour exécuter diverses fonctions.

Communication, audioconférence, pagination, liste d'annuaire, messagerie vocale, transmission de données intégrée, et n'importe quelle autre tâche qu'un système PBX standard exécute actuellement ou exécuterait dans l'avenir, sont mises en œuvre par ces modules distincts.

L'API traducteur de Codec (Codec Translator API) :

Charge les modules de codec pour supporter divers formats de codage et de décodage audio tels que le GSM, la μ -Law, l'A-Law, et même le MP3.

L' API Canal (Asterisk Channel API):

Cette API gère le type de raccordement sur lequel arrive un appelant, que ce soit une connexion VoIP, un RNIS, un PRI, une signalisation de bit dérobé, ou une autre technologie. Des modules dynamiques sont chargés pour gérer les détails de la couche basse de ces connexions.

L'API de format de fichier (Asterisk File Format API) :

Elle permet la lecture et l'écriture de divers formats de fichiers pour le stockage de données dans le fichier système.

Sa particularité modulaire permet à Asterisk d'intégrer de façon continue le matériel de commutation téléphonique actuellement mise en œuvre, et les technologies de Voix par paquet en constante augmentation, émergeant aujourd'hui [7].

III.5 Java Media Framework :

Java Media Framework(JMF) est une API extension à la JDK, fournie par Sun Microsystems, Silicon Graphics, Intel, IBM et RealNetworks .Elle permet d'incorporer des données de type audio ou vidéo dans des applications Java et des applets. En effet, JMF fournit un support pour la capture et le stockage de données audio et vidéo.

Elle a été conçue pour répondre aux attentes suivantes :

- Permettre la présentation et la capture de données multimédias.
- Permettre le développement d'application java utilisant le streaming ou les conférences vidéos.
- Permettre l'accès à un large type de données.
- Offrir un support pour le protocole RTP (Real-Time Transport Protocol).

III.5.1 Les formats supportés par l'API

JMF prend en charge différents types de médias, y compris :

- **les protocoles** : FILE, HTTP, FTP, RTP ;
- **les formats audio** : AIFF, AU, AVI, GSM, MIDI, MP2, MP3, QT, RMF, WAV ;
- **les formats vidéo** : AVI, MPEG-1, QT, H.261, H.263 ;
- **autres** : Flash 2, HotMedia.

Décomposition :

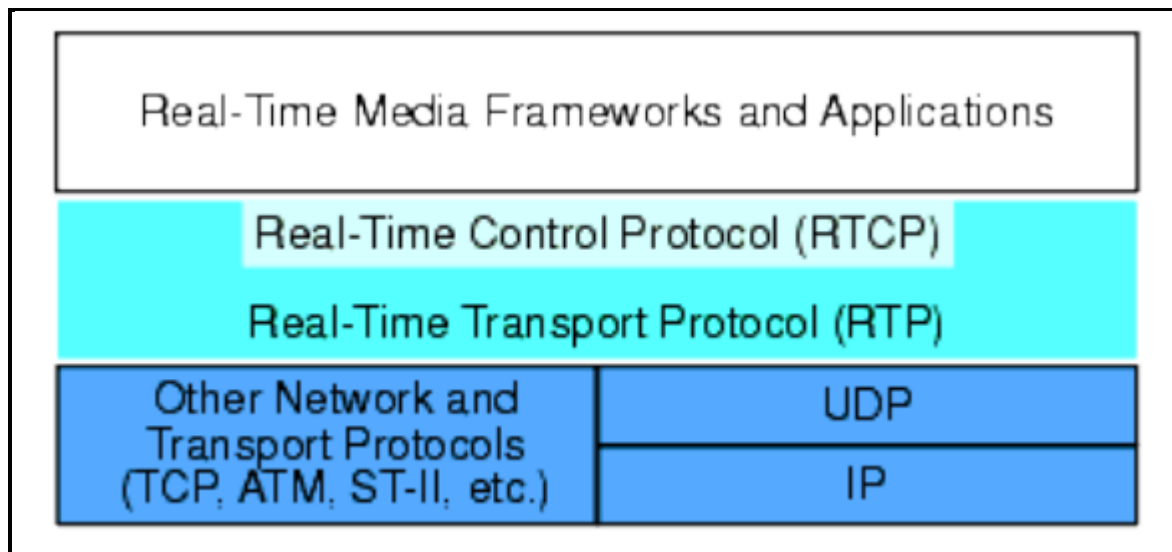


Figure III.3 la décomposition de JMF.

JMF se décompose en deux modules distincts :

- **L'API de base** : Elle fournit toute une architecture permettant de gérer l'acquisition, le traitement et l'affichage de données multimédias. On peut alors facilement à l'aide de JMF, créer un applet ou une application qui présente capture, manipule ou enregistre des flux multimédia. On trouve alors différents outils comme les Players qui vont permettre la visualisation et le traitement des données. On pourra alors grâce à eux traiter le flux vidéo et permettre les options que l'on souhaite sur le lecteur media.
- **L'API RTP** : Jusque là, JMF ne permettait que de lire, traiter et présenter un flux arrivant à un utilisateur. Grâce à l'API RTP on va maintenant pouvoir transmettre un flux et ainsi créer son propre serveur de streaming. On peut maintenant capturer un flux à partir d'une caméra ou un micro et le transmettre à différents utilisateurs ou encore centraliser un ensemble vidéo et sons et les transmettre sur demande.

Enfin JMF est prévue pour être étendue. En effet elle permet de développer ses propres plugins afin d'effectuer des traitements particuliers de fichiers audio ou vidéo ou encore de traiter certains formats non supportés pour des besoins particuliers [8].

III.6 le logiciel X-Lite

X-Lite est un « logiciel téléphone » ou « softphone », permettant l'utilisation d'un téléphone virtuel sur un ordinateur. Ce logiciel est un des plus abouti en termes de fonctionnalités, de fiabilités et de simplicité. Il permet la gestion de contacts et de groupes et fait également la messagerie instantané ainsi que le support de la vidéo [7].

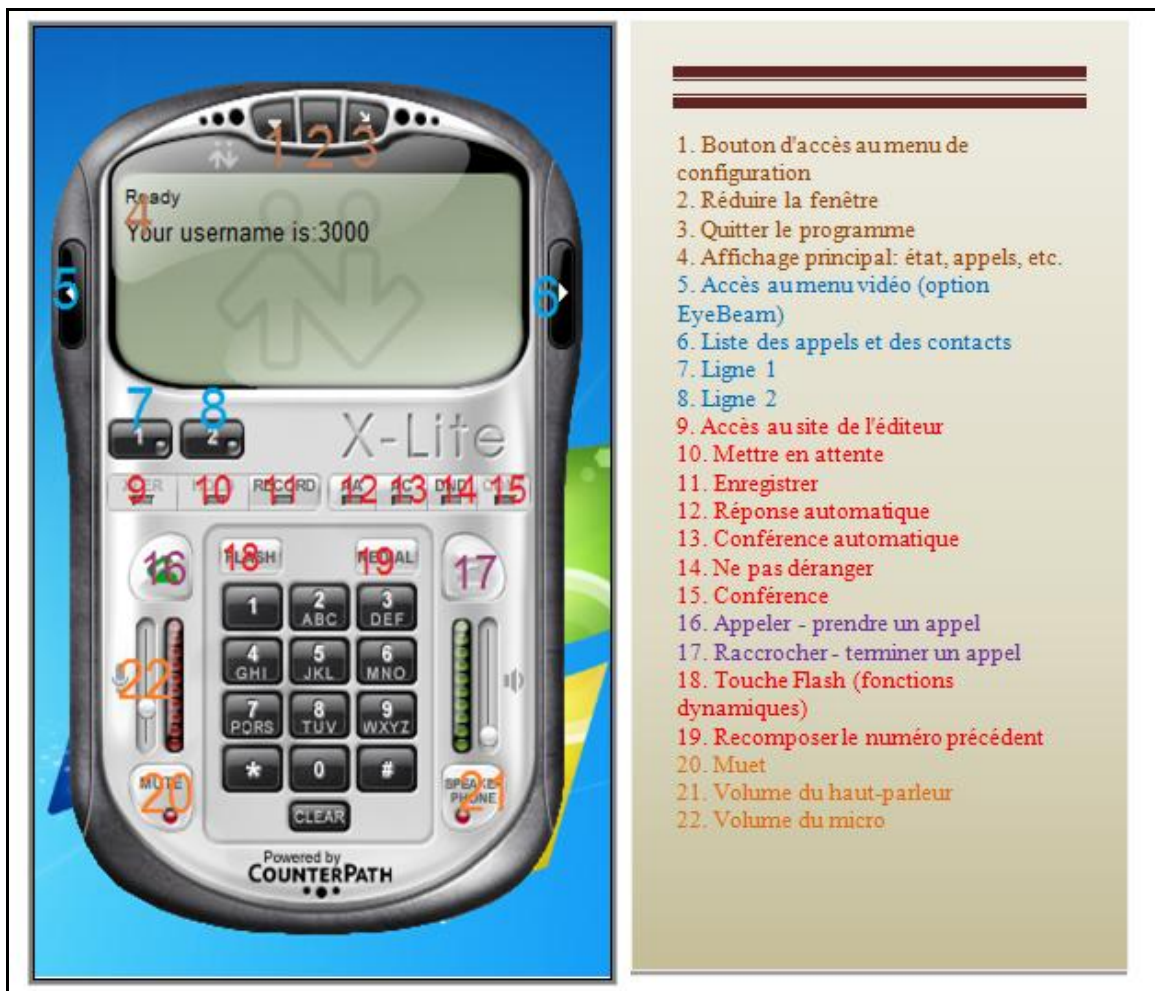


Figure III.4 Principales fonctionnalités.

- **Communication** : à condition d'être connecté au web et de disposer d'un micro-casque, cet opus est conçu pour permettre les conversations entre utilisateurs. On a la possibilité de faire des conférences audio ou vidéo quel que soit l'endroit où se trouvent les interlocuteurs.

- **Messagerie** : si le contact ciblé est en ligne et qu'il ne peut accepter un appel téléphonique, on lui envoie des messages instantanés. Ce qui singularise **X-Lite**, c'est qu'il prend en charge les messageries vocales.
- **Téléphonie** : tous les contacts peuvent être ajoutés dans le carnet d'adresses et on a accès à l'historique des appels. L'outil intègre la plupart des fonctions d'un vrai téléphone telles que la mise en attente ou le renvoi automatique. On peut appeler un autre softphone, un mobile ou un fixe.

III.6.2 Configuration du logiciel X-Lite

Pour la procédure d'installation, suivez les instructions comme n'importe quel logiciel . L'exemple de cette installation est faite sur une plateforme « Windows 7 sp1».

Une fois le logiciel installé, la fenêtre de configuration va automatiquement s'ouvrir afin de créer un nouveau compte. Si ce n'est pas le cas, positionnez le curseur de votre souris dans l'écran du logiciel et cliquez avec le bouton de droite pour faire apparaître l'écran de configuration et cliquez sur « SIP Account Settings... » [9].



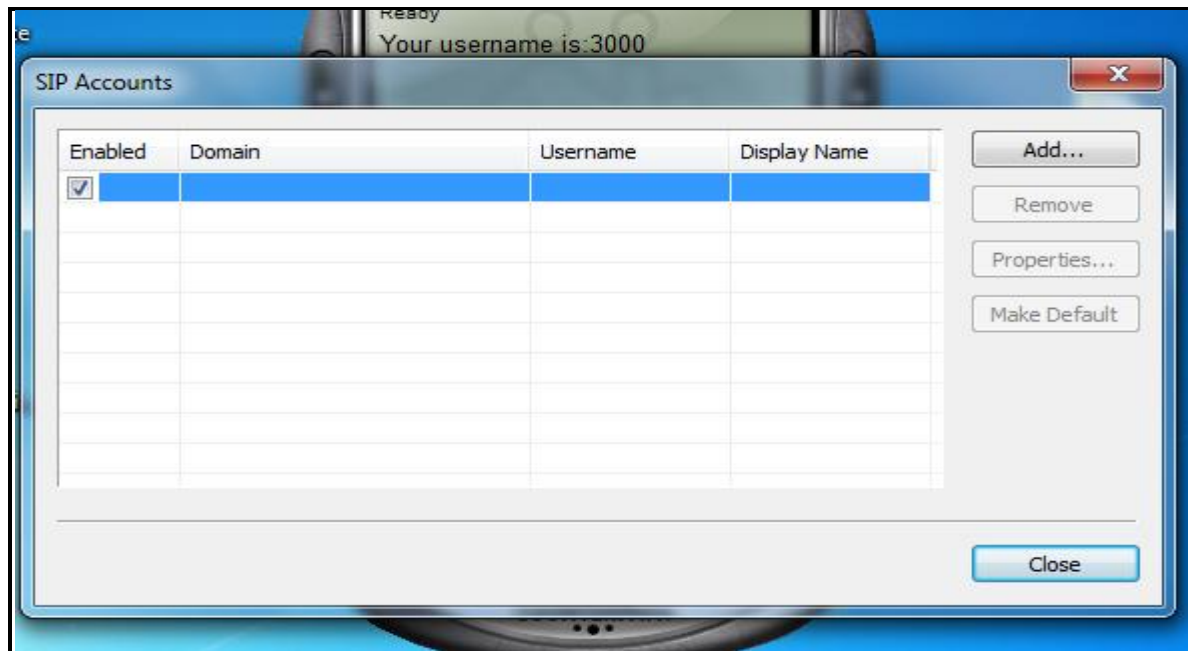


Figure III.5 Affichage des comptes SIP de X-Lite.

La fenêtre de configuration des comptes SIP s'ouvre, cliquez sur "Add..." pour ajouter vos paramètres personnels.

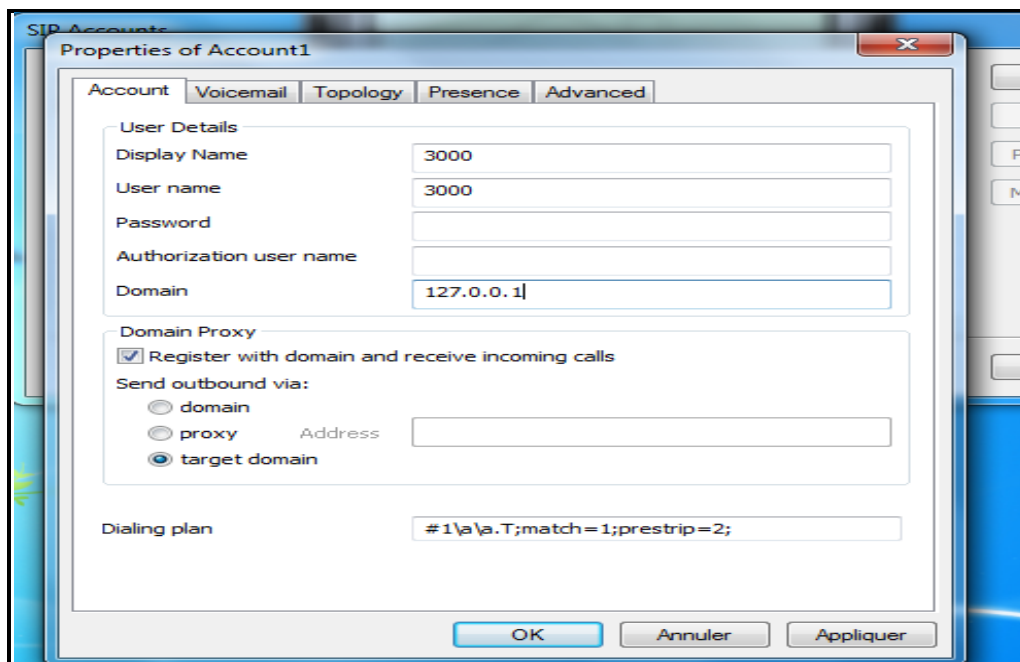


Figure III.6 Menu de configuration SIP.

Il vous suffira ensuite de remplir les champs vides par les informations du compte à connecter sur le système téléphonique.

Supposons que votre administrateur vous donne au minimum les 3 informations suivantes pour votre numéro de poste afin de vous connecter au système téléphonique :

1. Numéro de poste :

2. Mot de passe du compte SIP :

3. Adresse du serveur :

Note : l'adresse du serveur peut être un adresse à numéro («127.0.0.1») ou un nom (exemple : «abc.pb.poin.com»).

Les informations qui devront être saisies, le seront de la façon suivante :

- « Display name»:est le nom du poste téléphonique (votre prénom et nom par exemple).
- « Password» : Le mot de passe que vous aura donné l'administrateur. Attention à bien respecter les MAJUSCULES et les minuscules si il y a lieu.
- « Domain» : est l'adresse du serveur (« 127.0.0.1 » dans cet exemple)

Une fois toutes les informations saisies, appuyez sur « OK » et « Close ».

Une fois toutes ces opérations effectuées, le logiciel X-Lite devrait fonctionner.

Le logiciel devrait ressembler à ceci :



Figure III.7 Interface de Logiciel X-lite.

Conclusion

Dans ce chapitre nous avons présenté une étude de l'ensemble des outils choisis pour la réalisation de notre application. On s'est intéressé à mettre en place les principes de base d'un PABX, a effectué une petite présentation sur logiciel AstérisK. A fin de parler sur Java Media Framework et le softphone X-lite.

Dans le chapitre suivant, on va entamer la partie réalisation de notre application qui constitue le dernier volet de ce rapport.

Chapitre IV

Application

Introduction

On va entamer dans ce chapitre la partie réalisation qui constitue le dernier volet de ce rapport et qui a pour objectif d'exposer le travail réalisé. Pour ce faire, on va commencer tout d'abord par préciser l'environnement matériel et logiciel de ce travail. Ensuite, on va présenter le travail accompli tout au long de ce projet.

L'objectif est de réaliser une application mobile qui implémente la voix IP, et de la tester sur un réseau WIFI.

IV.1 Environnement de développement

Dans cette partie on présentera l'environnement matériel et logiciel, ainsi que les outils de développement.

a) Environnement matériel :

Pour la réalisation de ce projet on a disposé de :

- Au moins deux ordinateurs (serveur + client).
- Pour créer un réseau local, il faut déjà des ordinateurs équipés chacun d'une **carte réseau wifi**.

b) Environnement logiciel :

Les logiciels utilisés sont :

- Windows (**XP, Win 7, ou Vista**).
- Un autocommutateur téléphonique **PABX (serveur Asterisk)**.
- Un logiciel de Programmation mobile J2ME (Java 2 Micro Edition), utilisant **Netbeans mobile** dans notre cas.
- Equipment mobile: soft phone X-lite.

IV.2 Description du travail réalisé

Cette partie est consacrée à la description de phase de réalisation et d'implémentation de ce projet, on va présenter quelques interfaces afin d'illustrer plus clairement les diverses utilisation de l'application.

IV.3 Méthode et application

L'analyse des besoins, qui donne une compréhension détaillée des besoins, impose une structure du système qu'on doit préserver tout au long de son développement. Ainsi, il nous permet de cerner et clarifier les besoins des différents acteurs agissant avec le système. Dans cette partie, on va présenter la réalisation de l'application et enfin la conception.

IV.3.1 Pourquoi Java comme langage de programmation ?

Le développement d'une application mobile basé sur une plate forme java, Micro Edition (Java 2 ME) qui fournit un environnement robuste et flexible pour les applications qui s'exécutent sur des périphériques intégrés et mobiles : téléphones mobiles, décodeurs, lecteurs Blu-ray, appareils multimédia numériques, modules M2M, imprimantes, etc. De plus, notre groupe de projet possède une base en Java et beaucoup d'éléments vus au cours de la 1^{ère} année de Master seront réutilisables dans cette application. Nous avons aussi choisi Java pour la puissance de la Javadoc native ainsi que celle de SIP API for J2ME (JSR180).

IV.3.2 L'architecture

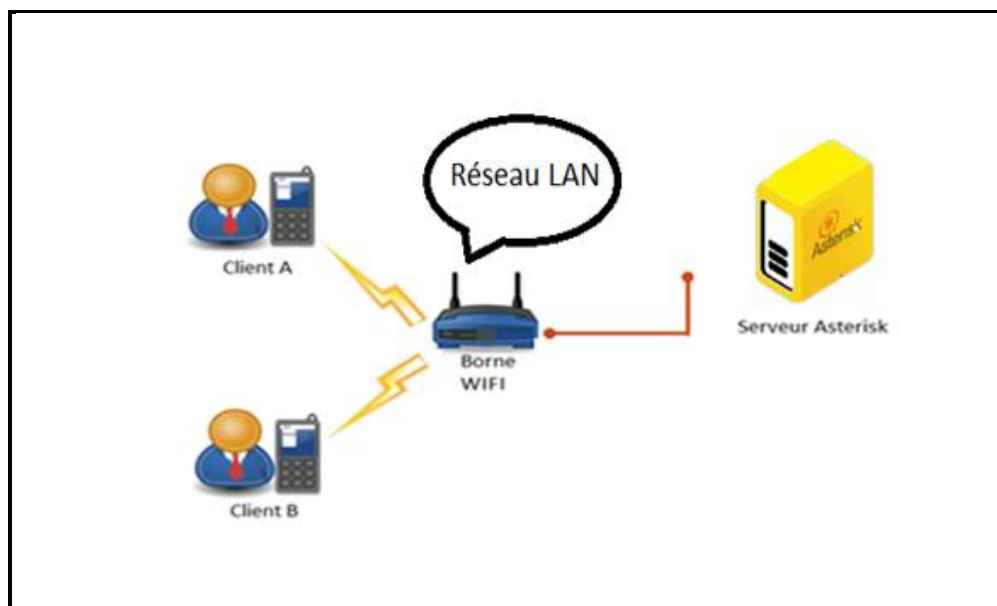


Figure IV.1 Architecture de notre application

IV.3.3 Description du prototype de test

Un client A veut établir un appel téléphonique IP vers un client B à travers un serveur Asterisk utilisant le protocole SIP qu'il a un rôle d'établissement, la modification et la terminaison de sessions multimédias.

Le protocole SIP est la norme du secteur des télécoms pour les communications multimédia. Les appels d'une adresse SIP vers une autre adresse SIP sont gratuits, peu importe l'opérateur SIP utilisé tant que son réseau SIP est ouvert.

Notre programme sert à établir cette connexion, utilisons des adresses SIP et des noms utilisateurs (User Name) grâce au protocole de signalisation SIP via un serveur Asterisk.

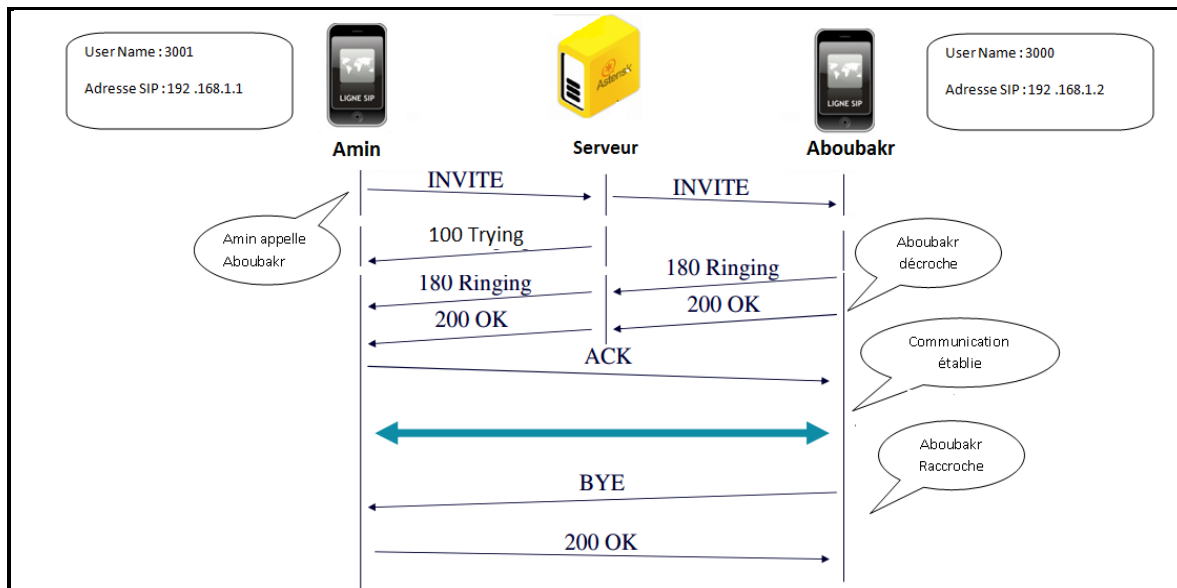


Figure IV.2 Schéma descriptif d'une communication mobile en mode diffusif

IV.3.3.1 Scénarios de communication

- 1- Amin compose sur son terminal l'adresse SIP et le nom utilisateur d'Aboubakr. Un message d'invitation (requête INVITE) est envoyé de l'UAC d'Amin vers le serveur Asterisk, À la réception de ce message, le serveur utilise la partie adresse SIP d' Aboubakr pour localiser l'UAC de son terminal. En parallèle, le serveur informe Amin qu'il prend en charge la requête et tente de la mettre en relation. La réponse temporaire **100 TRYING** indique à cette dernière que le message a été reçu et qu'il est en cours de traitement.

- 2- Le terminal d'Aboubakr sonne. il reçoit l'invitation. En parallèle, il indique au serveur (par un message 180 RINGING) que l'appel est en train d'être notifié à Aboubakr et que la communication est en attente de son acceptation. Ce message informatif est relayé jusqu'à l'émetteur Amin, qui reçoit généralement un retour audio ou visuel (une tonalité de sonnerie particulière le plus souvent).
- 3- On suppose le cas où Aboubakr a choisi de répondre à l'appel. À l'instant où il décroche, l'UAS retourne à l'UAC un message **200 OK** pour l'informer que l'appel est accepté. À ce stade, la communication n'a pas encore débuté, et aucun son n'est transmis.
- 4- Le terminal d'Amin confirme les paramètres d'appel. Il envoie un message d'acquiescement **ACK** qui spécifie les paramètres définitifs à utiliser lors de cette session. Notons que le message d'acquiescement peut passer directement d'un interlocuteur à l'autre, sans transiter par le serveur. À ce stade, chacun des utilisateurs a pu apprendre la localisation exacte de son interlocuteur, et il n'est donc plus nécessaire de recourir au serveur. Toutes les transactions qui suivent sont effectuées directement, de poste utilisateur à poste utilisateur. À réception de ce message, la communication entre les interlocuteurs peut débuter.
- 5- On suppose qu'Aboubakr veut terminer cette communication, Un message (requête BYE) est envoyé pour indiquer au correspondant que la session va être clôturée. Amin répond à cette requête en validant la prise en compte de cette demande par une réponse **200 OK**.

IV.3.4 Réalisation

Après avoir achevé l'étape de conception de l'application, on va entamer dans cette partie l'étape de réalisation.

Les coordonnées des clients :

<i>Les coordonnées de client A</i>	{	<i>User Name:3001</i> <i>Domain : 192.168.1.1</i> <i>N° de port : 9090</i>
<i>Les coordonnées de client B</i>	{	<i>User Name:3000</i> <i>Domain : 192.168.1.2</i> <i>N° de port : 47396</i>

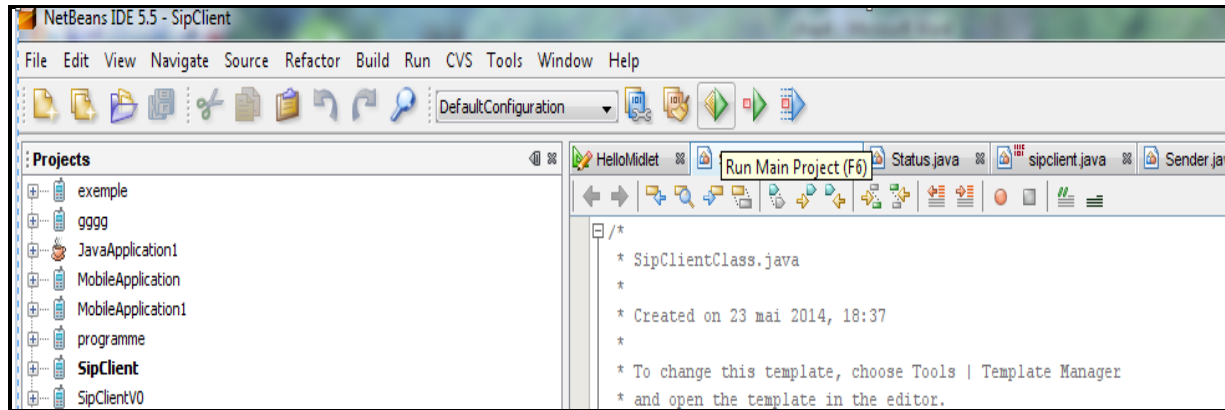


Figure IV.3 Interface d'exécution le programme client A (Amin)

Après l'exécution de programme avec la commande Run, un terminal Java s'affiche. Pour l'enregistrement de client A au serveur Asterisk, on doit entrer les coordonnées de ce client (user name : 3001 ; N° de port : 9090).

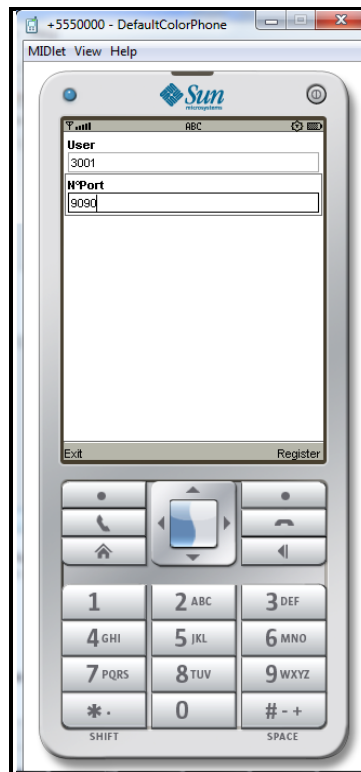


Figure IV.4 Interface d'un terminal Java.

Remarque 1 : Lorsque l'enregistrement de client A est établi, le serveur Asterisk affiche ces coordonnées dans l'autocommutateur PBX manager, utilisant la commande « **sip show peers** ».

```

WillVoice PBX MANAGER Free Edition
Main Commands Tools Admin Help
Connecting to Asterisk...
=====
Connected to Asterisk 1.2.26.1 currently running on client-PC (pid = 4112)
Verbosity is at least 1
CLI> sip show peers
Name/username      Host              Dyn Nat ACL Port    Status
3002/3002          (Unspecified)    D         0      Unmonitored
3001/3001          192.168.1.1     D         9090   Unmonitored
3000/3000          (Unspecified)    D         0      Unmonitored
3 sip peers [3 online , 0 offline]

```

Figure IV.5 L'affichage des coordonnées de client A.

Pour le client B, on applique les mêmes étapes (exécution de programme client B, enregistrement).

Remarque 2 : Lorsque l'enregistrement de deux client est établi, le serveur Asterisk affiche les coordonnées dans l'autocommutateur PBX manager.

```

WillVoice PBX MANAGER Free Edition
Main Commands Tools Admin Help
Connecting to Asterisk...
=====
Connected to Asterisk 1.2.26.1 currently running on client-PC (pid = 4112)
Verbosity is at least 1
CLI> sip show peers
Name/username      Host              Dyn Nat ACL Port    Status
3002/3002          (Unspecified)    D         0      Unmonitored
3001/3001          192.168.1.1     D         9090   Unmonitored
3000/3000          192.168.1.2     D         47396  Unmonitored
3 sip peers [3 online , 0 offline]

```

Figure IV.6 L'affichage des coordonnées des clients A et B.

Après la partie **REGISTRING** des deux clients, Amin compose sur son terminal le numéro de port et le nom utilisateur d'Aboubakr, comme représente la figure suivante :

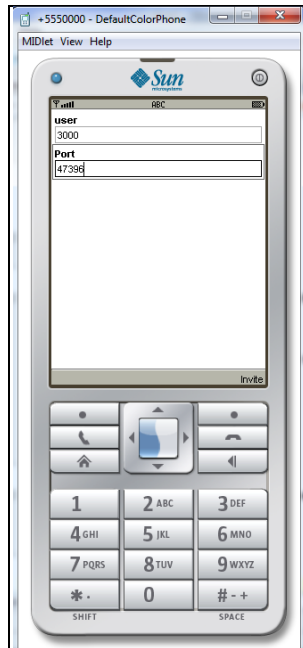


Figure IV.7 Interface de l'appelant (client A).

Après avoir cliquer sur la commande INVITE, Un message d'invitation (requête INVITE) est envoyé vers l'UAC de client B (Aboubakr). En suite, le terminal d'Aboubakr sonne. Il reçoit l'invitation.

Remarque 3 : la réalisation de notre application peut être s'effectuer a travers différents équipements mobile, on prend par exemple le soft phone X-lite, le terminale JAVA, ou le téléphone IP(SIP).

On veut établir un appel entre deux client, tel que :

1. Le client A : terminal JAVA, et le client B : le soft phone X-lite.



Figure IV.8 Etablissement un appel (T.java, X-lite).

2. Le client A : terminal JAVA, et le client B : terminal JAVA

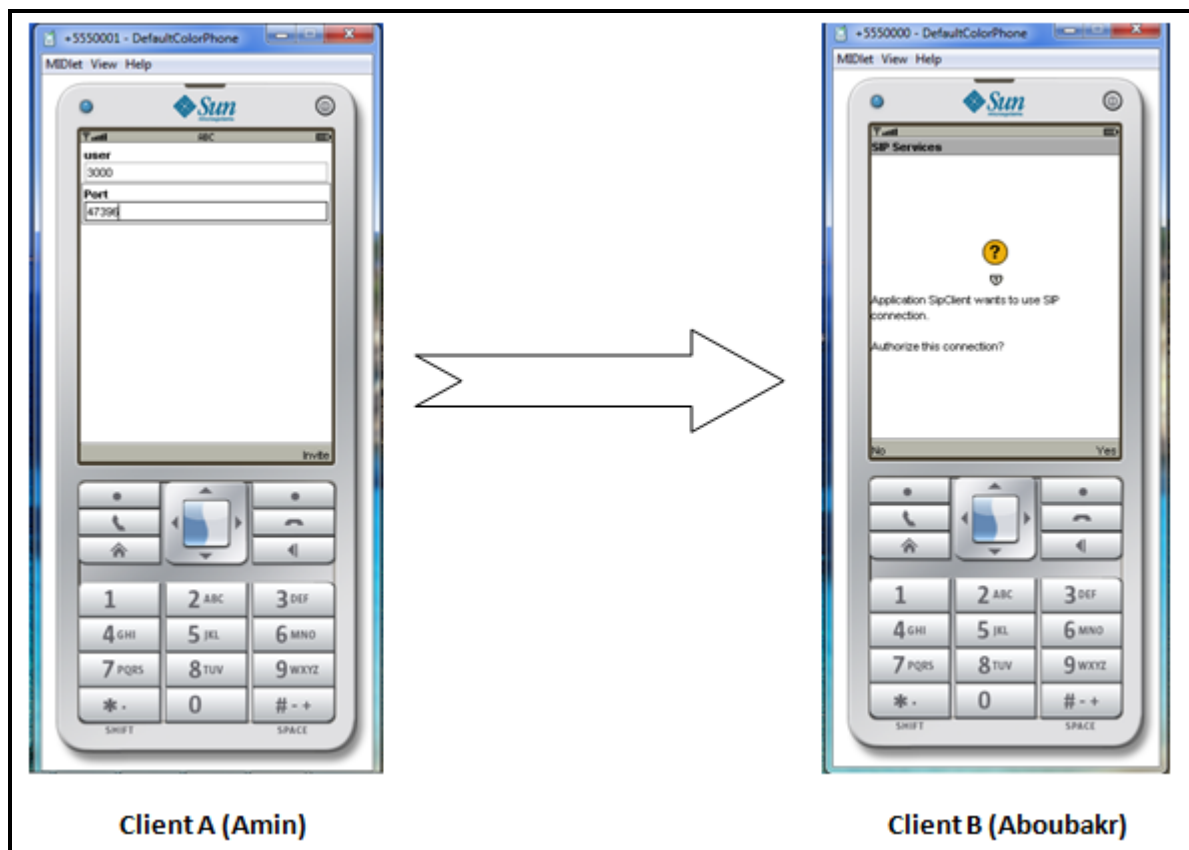


Figure IV.9 Etablissement un appel (T.java, T.java).

On suppose que le client B termine cette communication, Un message (requête BYE) est envoyé pour indiquer au correspondant que la session va être clôturée.

Conclusion

Dans ce chapitre, nous avons décrit brièvement le processus de réalisation de notre application, l'environnement de développement, l'implémentation des étapes et la démarche suivie pour la réalisation. En effet, nous avons achevé l'implémentation et les tests de tous les cas d'utilisation, tout en respectant la conception élaborée.

Conclusion générale

Ce mémoire s'inscrit dans le cadre d'un projet de fin d'étude. Il aboutit à la réalisation d'une application mobile de la VoIP sur un réseau Wifi.

De ce fait, un travail important de recherche sur Internet et une étude minutieuse sur les outils de travail ont été faits afin de dégager les différents besoins et de choisir l'architecture informatique la mieux adaptée au système. Ce travail nous a été bénéfique du fait qu'il nous a permis d'élargir nos connaissances des nouvelles outils tel les PABX , le serveur Asterisk , ainsi que la programmation mobile J2ME. Ce projet nous a aussi permis d'étudier les normes et les concepts de VoIP utilisés pour le développement des applications de VoIP .surtout la norme SIP.

A la fin de la réalisation de ce mémoire, nous avons accumulé une masse importante de connaissances aussi bien sur le plan théorique que sur le plan pratique, et nous estimons qu'elle nous sera très utile à l'avenir, en tant que futur Ingénieur .

Perspective

Quelques aspects peuvent être développés dans les projets à venir:

- Développement de l'application(ANDROID).
- Prise en charge la visioconférence.
- Transfère de l'application en mode pratique.

Bibliographie

[1]: Maiga Malik et Faye Modou (juin 2004) : Téléphonie sur IP. Mémoire d'ingénieur. Institut des télécommunications Abdelhafid boussouf-Oran

[2]: Mr Abed Amine et Mr Guenouna Abdelwahab. (juin 2004) : La voix sur IP. Mémoire d'ingénieur. Institut des télécommunications Abdelhafid boussouf-Oran

[3] : Tshimanga Kapampi Denis (2013). Etude d'implémentation d'une solution VoIP Sécurisée dans un réseau informatique d'entreprise. Mémoire d'ingénieur. Institut supérieur de techniques appliquées « I.S.T.A / KINSHASA ».

[4] : DANG Quang Vu (juillet 2005) : Comparaison de la technologie de la norme H.323 et la technologie de SIP pour l'application au service de la voix sur IP (VOIP). Rapport final. Institut de la Francophonie pour l'Informatique.

[5]: Laurent Ouakil, Guy Pujolle (2007). Téléphonie sur IP, 2nd edition.

[6]: Hafid Adem et Douara Messaoud (2011): VoIP avec Asterisk (Mise en place des Travaux Pratiques). Mémoire d'ingénieur. Institut national des télécommunications et des technologies de l'information et de la communication. Alger.

[7] : Benseyoub Mohamed Nadir et Rerbal Smail (juin 2008), PABX video avec Asterisk, Mémoire d'ingénieur. Institut des télécommunications Abdelhafid boussouf-Oran.

[8] : Mohamed Slim .(juin 2010). Traitement vidéo en java.

[9] : Cahiers du support techniques Programmer X-Lite. (Point CA Télécom) (www.pointCA.com).

Résumé

Voix sur IP ou VoIP est un terme utilisé dans la téléphonie IP pour un ensemble d'installations qui utilisent le internet protocole (IP) pour transmettre la voix. En générale, cela signifie l'envoi de la voix sous forme numérique dans des paquets discrets plutôt que dans les protocoles de commutation de circuits traditionnels du réseau téléphonique commuté(RTC).

Le but de ce projet est d'établir une communication des appels simples entre deux clients. Cette communication sera établie à partir d'un téléphone mobile de l'utilisateur à travers un serveur dans un réseau sans fil ou un réseau locale, et par conséquent sans passer par le réseau GSM/3G d'un opérateur.

Mots clés : VOIP, H.323, SIP, Application mobile, Wifi.

Abstract

Voice over IP or VoIP is a term used in IP telephony for a set of facilities that use Internet Protocol (IP) to transmit voice In general, this means sending voice in digital form in discrete packets rather protocols in traditional circuit-switched public switched telephone network (PSTN).

The purpose of this project is to establish a simple communication calls between two clients. This communication is established from a mobile phone user through a server in a wireless network or a local network, and therefore without going through the GSM/3G network operator.

Keywords : VOIP, H.323, SIP, Application mobil, Wifi.

ملخص

الصوت عبر بروتوكول الإنترنت هو مصطلح يستخدم في الاتصال الهاتفي عبر الإنترنت من اجل مجموعة من المرافق و المنشآت التي تستخدم هذا البروتوكول لنقل الصوت بشكل عام ، وهذا يعني إرسال الصوت في شكل رقمي بواسطة حزم منفصلة بدلا من البروتوكولات التقليدية المستخدمة في شبكة الهاتف العام RTC.

الغرض من هذا المشروع هو إنشاء مكالمات هاتفية بين عميلين تنشئ هذه المكالمات بواسطة مستخدم هاتف نقال عبر المرور بنظام الخادم في شبكة لا سلكية او شبكة محلية و بالتالي دون المرور عبر مشغل شبكة الهاتف النقال GSM/3G. الكلمات الدلالية : الصوت عبر بروتوكول الإنترنت، بروتوكول SIP، بروتوكول H.323، تطبيقات الموبايل، شبكة لا سلكية.