

République Algérienne Démocratique Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université d'Ibn Khaldoun – Tiaret

Faculté des Sciences, Technologies et Sciences de la Matière

Département Informatique

Thème

Conception d'une application pour l'administration du serveur Asterisk

Pour l'obtention du grade de Master

Spécialité : Master Réseaux et Télécom

Réalisé par :

CISSÉ FANTA

BOKO EDGAR CORRINTHE

Dirigé par :

Mr. Mostefaoui Sid A

Année universitaire 2012-2013

Dédicaces

Je dédie ce modeste travail à ceux qui me sont les plus chers :

*A mes parents, pour leur aide, encouragement et soutien qu'ils ont porté
à mon égard.*

A ma fiancée Yapi Shaully Audrey, qui m'a apporté un soutien indéfectible et inconditionnel tout au long de mon cycle.

*A mes frères sangs : Ablo, Exo, Trésor, Géro, Dorgelès, Zapa, Moussé,
Camso, Nasco.*

*A mes môgôtines : Noëlle, Aïcha, Armandine, Jessica, Doui, Flotché,
Imène.*

A toute la communauté chrétienne de Tiaret en particulier : le Père Hubert, Frère Dominique, Père René

A ma binôme : Cissé Fanta

A toute ma famille et amis.

A toute la promotion 2008

Boko Edgar Corrinthe

Dédicaces

Je dédie ce travail :

A ma famille plus particulièrement à mes parents pour leurs conseils et leurs soutiens.

A tous mes amis (es) qui m'ont aidé à réaliser ce projet.

A Tous ceux qui vont admirer notre travail.

Enfin à toutes les personnes ayant contribué, matériellement ou moralement, de près ou de loin, à la réussite de ce projet.

Avec toute la chaleur de notre affection et notre sincérité.

Cissé Fanta

Remerciements

Nous tenons à remercier en premier lieu « Dieu » le tout puissant, pour tous ses bienfaits dans notre vie de tous les jours et surtout en ce jour particulier.

Ensuite, notre encadreur Monsieur Mostefaoui Sid Ahmed, Monsieur Saim Mohamed notre maître de stage, ainsi que Monsieur Yacine, pour leurs conseils pertinents et leur disponibilité tout au long de la réalisation de ce travail.

Nous remercions également les membres du jury, pour avoir accepté de juger ce modeste travail.

Enfin, nos remerciements vont également à tous nos enseignants du département informatique.

Résumé

Asterisk est un PABX open source pour systèmes UNIX originellement créé en 1999 par Mark Spencer fondateur de la société Digium.

Notre projet consiste à son administration complète par la programmation d'un logiciel sous Java, prenant en compte les fichiers de configuration du serveur AstérisK, qui lui-même sera interconnecté à un serveur de base de données dénommé MySQL.

Afin que toute personne ayant ou pas des notions en informatique et sur le serveur Asterisk puisse l'utiliser sans problème.

Mots-clés : Asterisk, MySQL, Administration, PABX

Lexiques

ToIP:	Telephony over Internet Protocol/ Téléphone par internet
IP:	Internet Protocol
VoIP:	Voice over IP
TCP:	Transmission Control Protocol
DHCP:	Dynamic Host Configuration Domain
Gatekeeper:	Grande Barrière
SIP:	Session Initiation Protocol
HTTP:	Hyper Text Transfer Protocol
RTP:	Real-time Transport Protocol
FAI:	Fournisseur d'Accès Internet
UDP:	User Datagram Protocol
DSP:	Digital Signal Processor
SPIT:	Spam over IP Telephony
PCM:	Pulse Code Modulation
RNIS:	Réseaux Numériques à Intégration de Services
PABX :	Private Automatic Branch eXange
Qos :	Qualite off Services
UIT :	Union Internationale des Télécommunications
RTCP:	Real-time Control Protocol
VCoDSL:	Voice Channelization on DSL
ADSL:	Assymetric Digital subscriber Line/ Services d'Accès Internet utilisant des lignes téléphoniques
PC:	Personal Computer
MSN:	Microsoft Network
GSM:	Global System for Mobile/ Téléphone Portable
Wi-Fi:	Wireless Fidelity

LAN: Local Area Network

IETF: Internet Engineering Task Force

RFC: Request For Comment

MGCP: Média Gestion Control Protocol

SCCP: Skinny Client Control Protocol

MCU: Multipoint Control Unit

ATM: Asynchronous Transfer Mode/ method de communication asyn-
chrone

MMUSIC: Multiparty Multimedia Session Control

OSI: Open System Interconnexion/ Modèle normalise pour
l'interconnexion de Systems ouverts.

UAC: User Agent Client

UAS: User Agent Server

GPL: Généric Public Licence

ENUM: tElephone NUmber Mapping

DNS: Domain Name System

NAT: Network Address Translation

ALC: Adaptative Light Control

STUN: Simple Traversal of UDP through NAT/ Traversée Simple UDP à
Travers les NATs

DoS: Denis off Services

API: Interface de Programmation d'applications

IAX: Inter Central Asterisk

URL: Uniform Ressource Locator

ARA: Asterisk Real-time Architecture

MCD : Modèle conceptuel de Données

SOMMAIRE

Introduction Générale	01
Chapitre I: VoIP	02
Introduction	03
Définition	03
I-Principe de Fonctionnement	03
1-Mise en place de la communication	04
2-Etablissement de la communication	04
3-Transport de l'information téléphonique	04
4-Changeement de réseau	04
5-Arrivée au destinataire	05
II-Les Concepts de la VoIP	05
III-Inconvénients de la voix sur IP	07
1-Sécurité de VoIP	07
2-Qualité Sonore	07
3-La QoS de la VoIP	08
a-Le temps de latence	08
b-La perte de paquets	08
c-La gigue	09
IV-Enjeux	09
1-Réduction des coûts d'appel	09
2-Mutualisation des réseaux, simplification de l'architecture	10
3-Prépondérance de la téléphonie et convergence voix-données	10
V-Perspectives	10
1-Le challenge de la VoIP	10
2-Les difficultés de VoIP	11
Conclusion	13
Chapitre II : La ToIP	14
Introduction	15
Définition	15
I- Les Contraintes de la ToIP	16
1-Contraintes temporelles	16
2-Le processus de resynchronisation de la parole téléphonique	16
3-Qualité de service de la ToIP	16

II-Les Solutions de la ToIP	17
1-Solution 1	17
2-Solution 2	18
3-Solution 3	18
4-Solution 4	19
5-Solution 5	19
6-Solution 6	20
7-Solution 7	20
III-Les avantages de la ToIP	21
Conclusion	22
Chapitre III : Protocoles liés à la ToIP	23
Définition	24
I-Les protocoles de signalisation	24
1-Le protocole H.323	25
a-Les terminaux (au minimum deux)	25
b-Le MCU (Multipoint Control Unit)	25
c-Le Gatekeeper	25
d-La passerelle	25
2-Le protocole SIP	26
a-Architecture protocolaire	26
b-Architecture d'une plate-forme SIP	27
3-Structure des messages SIP	30
4-Le corps du message	31
5-Requêtes et Réponses SIP	31
6-Fonctionnement	32
7-Transport	33
8-Comparaison SIP et H.323	33
a-Avantages du protocole H.323	33
b-Avantages du protocole Sip	34
II-Standard ENUM	35
III-Problématique ToIP avec les NAT et les pare-feux	36
1-Problème de NAT	36
2-Problème de pare-feux	37
IV-Solutions de traversées des NAT et des pare-feux	39
V-ToIP et la sécurité des communications voix	40
1-Vulnérabilités de la ToIP	40

2-Solutions de sécurité de la ToIP	41
3-La ToIP et IPv6	41
VI-Asterisk	42
Définition	42
1-Historique	42
2-Fonctionnalités	43
3-De la téléphonie à moindre coût	43
4-Une particularité modulaire	43
5-Principales fonctions	44
a-PBX Switching Core	44
b-Application Launcher	44
c-Codec Translator	44
d-Scheduler & I/O Manager	44
6-Les APIs	44
a-Asterisk Application API	44
b-Asterisk Translator API	44
c-Asterisk Channel API	44
d-Asterisk File Format API	44
7-Fonctionnement évolué	45
8-Choix d'Asterisk pour notre projet	45
Conclusion	46
Chapitre IV : Implémentation	47
I-Installation et configuration du serveur Asterisk	48
1-Installation du système d'exploitation	48
2-Installation du serveur Asterisk	48
3-Configuration du serveur Asterisk	49
4-Configuration basique du serveur Asterisk	50
5-Configuration avancée du serveur Asterisk	52
6-Asterisk en temps réel avec MySQL	53
a-La base de données Realtime	54
b-Création et configuration de Realtime avec une base de données MySQL	54

7-Création d'une interface graphique pour l'administration du serveur Asterisk	56
8-Test de fonctionnalités avec le client X-Lite	61
Définition	61
a-Installation et configuration d'un client X-Lite	61
Conclusion	63
Conclusion Générale	64
Bibliographie	65

Liste des figures et des tableaux

- Figure 1 : Processus de numérisation de la voix
- Figure 2 : Architecture détaillé d'un réseau VoIP
- Figure 3 : Le traitement de la voix
- Figure 4 : Principe pour transformer la voix en IP
- Figure 5: Architecture de la ToIP
- Figure 6 : La première génération de Téléphonie sur IP
- Figure 7 : La téléphonie au travers de l'ordinateur personnel
- Figure 8: Téléphonie IP utilisant l'ordinateur personnel comme intermédiaire
- Figure 9: Apparition du modem ADSL dans la chaîne de transmission de la téléphonie
- Figure 10 : Téléphonie IP de bout en bout
- Figure 11 : Le triple-Play
- Figure 12: quadruple-Play
- Figure 13: penta-Play
- Figure 14 : Différence entre la ToIP et la VoIP
- Figure 15 : Composantes de l'Architecture H.323
- Figure 16 : Architecture protocolaire
- Figure 17 : Echange entre terminal et services associés
- Figure 18 : Dialogue entre deux entités
- Figure 19 : illustration des requêtes et des réponses
- Figure 20 : scénario d'une communication SIP
- Figure 21 : principe de fonctionnement d'ENUM
- Figure 22 : utilisation d'ENUM
- Figure 23 : problème de NAT avec la ToIP
- Figure 24 : scénario d'établissement de session avec blocage de contenu multimédia par firewall
- Figure 25 : Fonctionnement du firewall
- Figure 26 : Mode de fonctionnement d'un PABX
- Figure 27 : Architecture détaillée d'Asterisk
- Figure 28 : sélection de logiciels a installer
- Figure 29: Console du serveur Asterisk
- Figure 30: MCD de la base de données
- Figure 31: Ajout et configuration des droits d'accès d'un administrateur de base de données
- Figure 32: Identification Administrateur
- Figure 33: accueil de l'outil d'administration de notre serveur
- Figure 34: Ajout d'un utilisateur
- Figure 35: Ajout de la messagerie vocale
- Figure 36: Rapport CDR (Call Detail Report)
- Figure 37: Recherche d'utilisateurs (numéro)

Figure 38: Recherche d'utilisateurs (Compte)

Figure 39: suppression d'un compte

Figure 40: Ajout et configuration d'un client x-lite

Figure 41: Utilisateur connecté

Tableau 1 : liste des codecs utilisés dans Asterisk

Tableau 2 : Limite entre Service téléphoniques et transport de la voix

Tableau 3 : Comparaison de SIP et H.323

Tableau 4 : Récapitulatif des avantages et inconvénients des solutions

Introduction Générale

Introduction Générale

La téléphonie sur IP (ToIP) connaît un essor considérable depuis une dizaine d'années. Aussi bien pour les besoins de l'entreprise que du particulier, cette technologie à bouleversé notre usage du téléphone. Les nouvelles fonctionnalités apportées ainsi que l'impact sur le coût des communications font que la ToIP s'implante massivement créant ainsi des emplois et des entreprises spécialisées dans le domaine. [1]

Elle marque un tournant dans le monde de la communication en permettant de transmettre de la voix sur un réseau numérique et sur internet. L'objectif de la ToIP est d'appliquer à la voix le même traitement que les autres types de données circulant sur internet. Grâce au protocole IP, des paquets de données, constitués de la voix numérisées, y sont transportés.

Il peut être du ressort de l'administrateur système et réseau de prendre en charge tout ou partie du système de ToIP de son entreprise. Des solutions opensource de logiciels ToIP sont largement utilisées et ont acquis une notoriété telle qu'il est très intéressant de les étudier. [1]

Après avoir bien détaillé et compris les caractéristiques de la VoIP et la ToIP dans le premier et deuxième chapitre, nous présenterons dans le troisième, les Protocoles liés à la ToIP. Nous essaierons dans le dernier chapitre, d'exploiter l'un de ses outils pour la mise en place de notre propre solution VoIP.

Ce projet va permettre, à travers l'étude du logiciel opensource Asterisk, de faire un tour d'horizon de cette technologie, de connaître les possibilités offertes par cet outil.

Aussi de créer un interface graphique facilement maniable, par toutes personnes ayant des connaissances ou pas en informatique, en vue de gérer de façons simple et efficace ce dit projet, qui est l'administration d'Asterisk.

Par ailleurs cela nous aura appris les notions de ToIP et d'utilisation d'Asterisk qui pourront être mise en avant lors de notre future recherche d'emploi.

Chapitre I : VoIP

Introduction

Dans ce chapitre, nous présenterons les bases fondamentales sur lesquelles repose la téléphonie sur IP. Ensuite évoquerons-nous, l'intérêt et les difficultés soulevés par la VoIP, expliquerons quels sont les enjeux posés par la voix sur IP, ce à quoi elle peut se substituer et quels bénéfices il est possibles d'en tirer. Aussi détaillerons-nous les contraintes imposées par la VoIP et l'architecture à respecter pour être pleinement fonctionnelle. Enfin montrerons-nous la différence entre la ToIP et la VoIP.

Définition

VoIP est l'abréviation anglaise de Voice over Internet Protocol.

Le protocole de Voix sur IP (VoIP) qui offre la possibilité de transmettre des appels vocaux via Internet et des réseaux de données basés sur IP, est devenu une technologie éprouvée. Une technique qui permet d'intégrer la voix aux données transmises par paquets sur un réseau utilisant le protocole IP.

La voix sur IP permet le transport de la voix comme n'importe quel genre de données sur l'ensemble du réseau qui accepte le protocole IP, tels que l'Internet publique, le réseau d'entreprise/privé ou bien une combinaison des deux. [6]

I-Principe de Fonctionnement

La voix sur IP (Voice over IP) caractérise l'encapsulation d'un signal audio numérique (La voix) au sein du protocole IP. Cette encapsulation permet de transporter la voix sur tout réseau compatible TCP/IP.

Le transport de la voix sur un réseau IP nécessite au préalable sa numérisation. Il convient alors de récapituler les étapes nécessaires à la numérisation de la voix avant d'entrer dans les détails de la VoIP. [5]

Le processus de la numérisation de la voix est schématisé par la figure suivante :

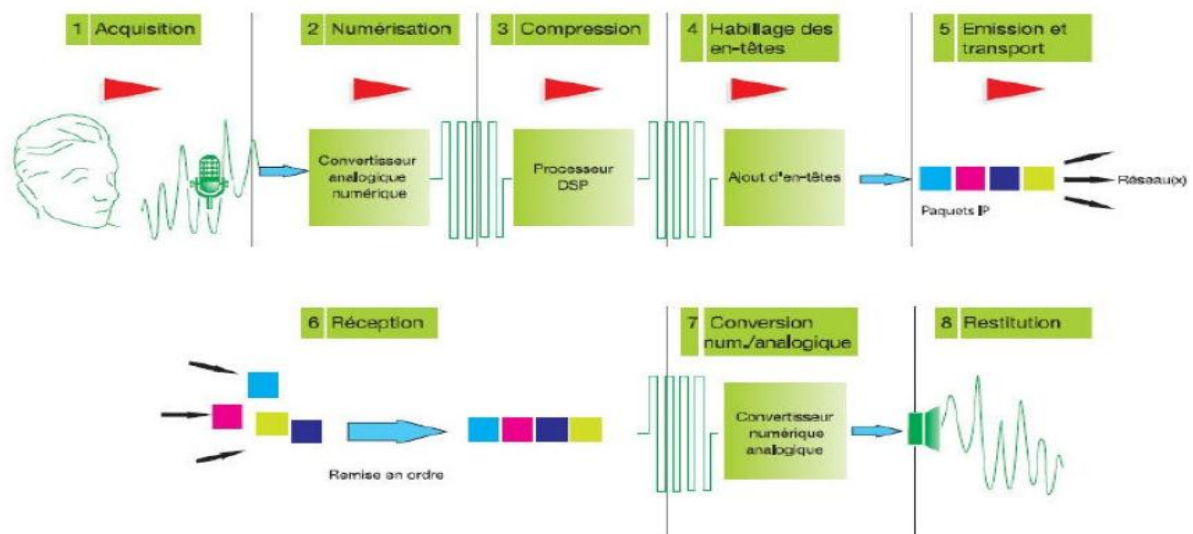


Figure 1 : *Processus de numérisation de la voix*

Enfin la voix sur IP permet de combiner le téléphone et l'ordinateur, grâce à une infrastructure intégrée basée sur le protocole Internet (IP).

Le déroulement d'une communication vocale sur IP se résume en cinq grandes étapes. [8]

1-Mise en place de la communication

Une signalisation démarre la session. Le premier élément à considérer est la localisation du récepteur (*User Location*). Elle s'effectue par une conversion de l'adresse du destinataire (adresse IP ou adresse téléphonique classique) en une adresse IP d'une machine qui puisse joindre le destinataire (qui peut être le destinataire lui-même). Le récepteur peut être un combiné téléphonique classique sur un réseau d'opérateur télécoms ou une station de travail (lorsque la communication s'effectue d'un combiné téléphonique vers un PC). Le protocole DHCP (Dynamic Host Configuration Protocol) et les passerelles spécialisées (*gatekeeper*) sont employés à cette fin.

2-Etablissement de la communication

Cela passe par une acceptation du terminal destinataire, que ce dernier soit un téléphone, une boîte vocale ou un serveur Web. Plusieurs protocoles de signalisation sont utilisés pour cela, en particulier le protocole SIP (Session Initiation Protocol) de l'IETF. Comme son nom l'indique, SIP est utilisé pour initialiser la session. Une requête SIP contient un ensemble d'en-têtes, qui décrivent l'appel, suivis du corps du message, qui contient la description de la demande de session. SIP est un protocole client-serveur, qui utilise la syntaxe et la sémantique de HTTP. Le serveur gère la demande et fournit une réponse au client.

Trois types de serveurs gèrent différents éléments : un serveur d'enregistrement (Registration Server), un serveur relais (Proxy Server) et un serveur de redirection (Redirect Server). Ces serveurs travaillent à trouver la route : le serveur proxy détermine le prochain serveur (Next-Hop Server), qui, à son tour, trouve le suivant, et ainsi de suite. Des champs supplémentaires de l'en-tête gèrent des options, comme le transfert d'appel ou la gestion des conférences téléphoniques.

3-Transport de l'information téléphonique

Le protocole RTP (Real-time Transport Protocol) prend le relais pour transporter l'information téléphonique proprement dite. Son rôle est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie de façon à reformer le flot avec ses caractéristiques de départ (vérification du synchronisme, des pertes, etc.). C'est un protocole de niveau transport, qui essaye de corriger les défauts apportés par le réseau.

4-Changement de réseau

Un autre lieu de transit important de la ToIP est constitué par les passerelles, qui permettent de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, en prenant en charge les problèmes d'adressage, de signalisation et de transcodage que cela pose. Ces passerelles ne cessent de se multiplier entre FAI et opérateurs télécoms.

5-Arrivée au destinataire

De nouveau, le protocole SIP envoie une requête à la passerelle pour déterminer si elle est capable de réaliser la liaison circuit de façon à atteindre le destinataire. En théorie, chaque passerelle peut appeler n'importe quel numéro de téléphone. Cependant, pour réduire les coûts, mieux vaut choisir une passerelle locale, qui garantit que la partie du transport sur le réseau téléphonique classique est le moins cher possible.

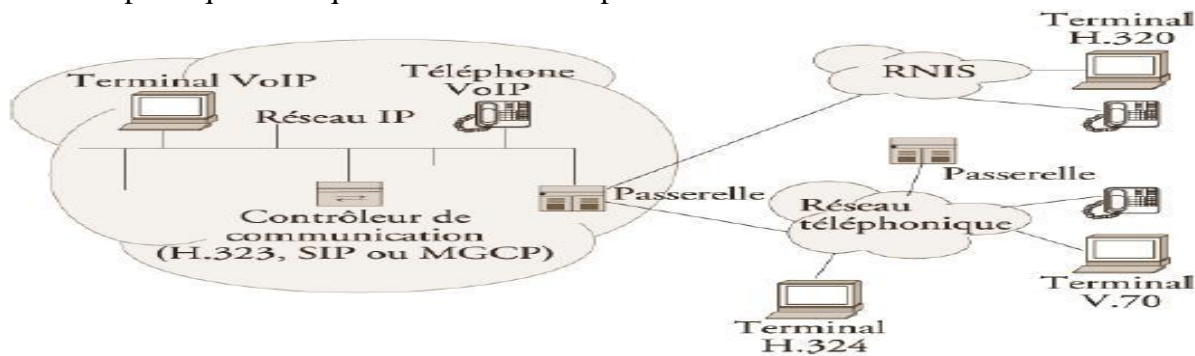


Figure 2 : Architecture détaillée d'un réseau VoIP

II-Les Concepts de la VoIP

La téléphonie sur IP est un service de transport de la voix afin d'effectuer des appels sur réseaux IP au lieu d'utiliser une ligne téléphonique traditionnelle. Ainsi la voix circule sur un réseau unique (voix, données, vidéos) permettant de réduire considérablement les coûts d'investissement.

La téléphonie sur IP est une transmission de la voix en mode paquets au format TCP/UDP.

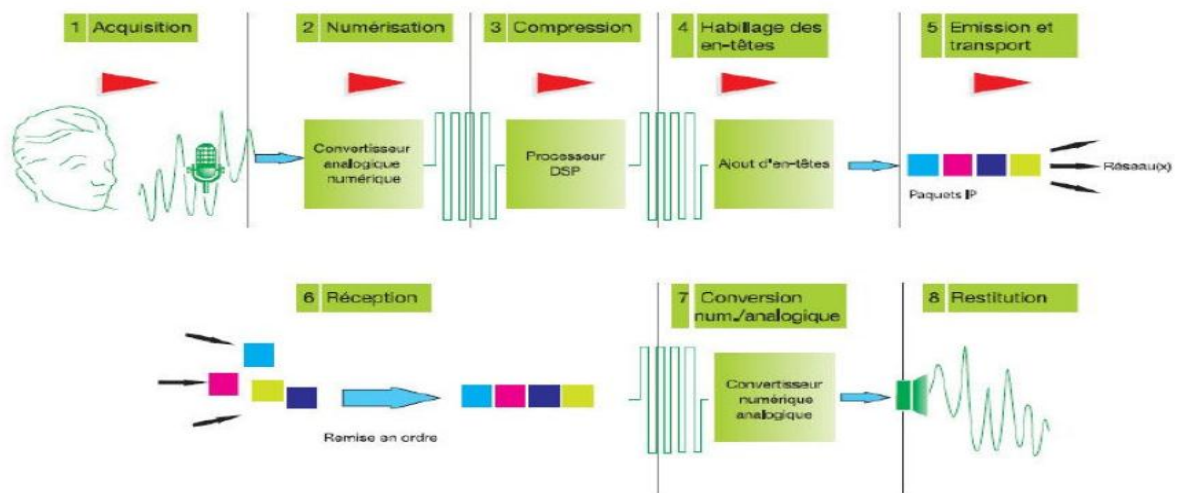


Figure 3 : Le traitement de la voix

Lorsqu'un utilisateur veut entrer en communication avec un autre, une connexion est alors établie entre les deux terminaux. L'utilisateur peut alors émettre un son par le biais d'un micro (signal analogique) qui est ensuite numérisé et compressé par la machine (signal par synthèse). Une fois les données encapsulées dans un paquet, il est envoyé au destinataire qui procédera aux opérations inverses assurant ainsi la mise en forme d'un message audible. [9]

Les différentes étapes sont: [10]

➤ Acquisition du signal:

La première étape consiste naturellement à capter la voix à l'aide d'un micro, qu'il s'agisse de celui d'un téléphone ou d'un micro casque.

➤ Numérisation

La voix passe alors dans un convertisseur analogique numérique qui réalise deux tâches distinctes

- échantillonnage du signal sonore: un prélèvement périodique de ce signal, il s'agit d'enregistrer à des intervalles très rapprochés la valeur d'un signal afin de pouvoir disposer d'un enregistrement proche de la valeur réelle de ce signal.
- quantification, qui consiste à affecter une valeur numérique (en binaire) à chaque échantillon.
- Plus les échantillons sont codés sur un nombre de bits important, meilleure sera la qualité.

➤ Compression

- Le signal une fois numérisé peut être traité par un DSP (Digital Signal Processor) qui va le compresser, c'est-à-dire réduire la quantité d'informations nécessaire pour l'exprimer.
- L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal

➤ Habillage des en-têtes

Les données doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau

Exemple: type de trafic

Synchronisation: s'assurer du réassemblage des paquets dans l'ordre

➤ Emission et transport

Les paquets sont acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réservé pour leur transport.

➤ Réception

Lorsque les paquets arrivent à destination, il est essentiel de les replacer dans le bon ordre et assez rapidement. Faute de quoi une dégradation de la voix se fera sentir.

➤ Conversion numérique analogique:

La conversion numérique analogique est l'étape réciproque de l'étape 2.

➤ Restitution

Dès lors, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur.

III-Inconvénients de la voix sur IP

1-Sécurité de VoIP

L'entreprise a toutes les chances de se retrouver avec un réseau de VoIP qui, certes, fonctionne correctement, mais est ouvert à tous et à tout Les risques.

À commencer par le spit (spam over IP telephony), pratique visant à encombrer les boîtes vocales de messages publicitaires. Il s'agit, avec les attaques par déni de service (interruption du trafic ou saturation de la capacité de stockage des boîtes vocales) de l'attaque la plus évidente.

L'interception des appels et le détournement du service (n'importe qui pouvant alors téléphoner via l'infrastructure de l'entreprise).

Ou encore l'usurpation de l'identité de l'appelant (se faire passer pour le patron d'un grand groupe auprès de quelques employés importants peu s'avérer particulièrement tentant).

2-Qualité Sonore

Le transport de la voix sur un réseau IP nécessite, au préalable, tout ou une partie des étapes suivantes: **[2]**

-Numérisation : dans le cas où les signaux téléphoniques à transmettre sont sous forme analogique, ces derniers doivent d'abord être convertis sous forme numérique suivant le format PCM (Pulse Code Modulation) à 64 Kbps. Si l'interface téléphonique est numérique (accès RNIS, par exemple), cette fonction est omise.

-Compression : le signal numérique PCM à 64 Kbps est compressé selon l'un des formats de codec (compression / décompression) puis inséré dans des paquets IP. La fonction de codec est le plus souvent réalisée par un DSP (Digital Signal Processor). Selon la bande passante à disposition, le signal voix peut également être transporté dans son format originel à 64 Kbps.

-Décompression : côté réception, les informations reçues sont décompressées. Il est nécessaire pour cela d'utiliser le même codec que pour la compression. L'objectif d'un codec est d'obtenir une bonne qualité de voix avec un débit et un délai de compression les plus faibles possibles. Le facteur de la gigue est primordial pour une bonne écoute de la Voip (gigue = délai entre l'émission et l'écoute de la voix).

Le tableau ci-dessous présente les caractéristiques des principaux codecs et standards implémentés dans la solution Asterisk. Les codecs les plus souvent mis en œuvre dans les solutions VoIP sont G.711, G.729 et G.723.1

Codecs VoIP	Débit (Kbps)
G711	64
G726	32
G723	6,4 (très bonne qualité)
G729	8 (très bonne qualité)
GSM	13
ILBC	15
LPC10	2.4 (voix métallique)
SPEEX	2 à 44 (peu utilisé)

Tableau1 : liste des codecs utilisés dans Asterisk

La qualité de la voix obtenue par les codecs G.729 et G.723.1 est de loin la meilleure et est très proche de celle du service téléphonique actuel. Ces deux codecs présentent une meilleure qualité que celle des réseaux téléphoniques cellulaires qui reste de bonne qualité (codec : gsm).

Le cumul, dans une même communication, d'opérations de compression/décompression conduit à une rapide dégradation de la qualité. La solution Asterisk doit éviter des configurations en tandem dans lesquelles l'IPBX reçoit un appel d'un poste distant avec un codec et doit le rediriger vers un autre poste avec un codec différent. [2]

3-La QoS de la VoIP

La qualité de service (QoS) est une notion importante à prendre en compte lors de l'implémentation de la VoIP. L'objectif est de garantir le transfert des trames IP sur le réseau sans retarder ou rejeter les trames transportant la voix. Il faut prendre en compte 3 principaux éléments pour caractériser la QoS. [2]

a-Le temps de latence :

La maîtrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho. La durée de traversée d'un réseau IP dépend du nombre d'éléments réseaux traversés (et du débit sur chaque lien), du temps de traversée de chaque élément et du délai de propagation de l'information (une transmission par fibre optique, à l'opposé de la terre, dure environ 70 ms). L'UIT a défini 4 classes qui permettent de caractériser, à titre indicatif, la qualité de transmission en fonction du retard de transmission dans une conversation téléphonique. Ces chiffres concernent le délai total de traitement, et pas uniquement le temps de transmission de l'information sur le réseau. La limite supérieure «acceptable» pour une communication téléphonique, se situe entre 150 et 200 ms par sens de transmission (en considérant à la fois le traitement de la voix et le délai d'acheminement).

b-La perte de paquets :

En cas de congestion du réseau, le protocole TCP prévoit de supprimer les trames IP entrant dans un élément saturé (buffers pleins). Les paquets de voix étant véhiculés au dessus d'UDP ce qui ne permet aucun mécanisme de contrôle de flux ou de retransmission sur cette couche au niveau du transport. D'où l'importance des protocoles RTP et RTCP qui permettent de déterminer le taux de perte de paquet et d'agir en conséquence au niveau applicatif.

Si aucun mécanisme performant de récupération des paquets perdus n'est mis en place (cas le plus fréquent dans les équipements actuels) alors la perte de paquets IP se traduit par des ruptures au niveau de la conversation et une impression de hachure de la parole. Plus un paquet de voix contient une longue durée de parole plus cet effet est accentué d'où la nécessité de choisir un bon codec audio (de faible débit).

c-La gigue :

La gigue mesure la variation temporelle entre le moment où deux paquets auraient dû arriver et le moment de leurs arrivées effectives. Les origines de la gigue sont multiples:

- ❖ encapsulation des paquets IP dans les protocoles supportés,
- ❖ charge du réseau à un instant donné,
- ❖ variation des chemins empruntés dans le réseau.

Pour compenser la gigue, on utilise des tampons (mémoire: buffer) qui permettent de lisser l'irrégularité des paquets. Le fait d'insérer des buffers augmente le temps de latence, leur taille doit donc être soigneusement définie, et si possible adaptée de manière dynamique aux conditions du réseau. La dégradation de la qualité de service due à la présence de gigue se traduit par une combinaison des deux facteurs cités précédemment:

Le délai et La perte de paquets.

Pour pallier à ces paramètres, il existe deux principales approches :

- ✓ Réserver une bande passante exclusivement au transfert de la voix :

Cette solution est possible dans le cas des réseaux locaux (type Intranet) mais il n'est pas possible de l'appliquer lorsque le réseau TCP/IP Internet intervient dans la communication.

- ✓ Prioriser les flux :

Chaque routeur traversé décide s'il prend en compte ou pas le champ de priorisation (champ TOS) propre à chaque type de données.

IV-Enjeux

La convergence voix/données/images pousse les entreprises à faire fonctionner ensemble les services en charge de la téléphonie et ceux en charge du système informatique. L'objectif est de rationaliser les dépenses télécoms et réseau de l'entreprise. Ceci permet de modéliser les architectures mais aussi de réduire les coûts de possession des équipements en maximisant le retour sur investissement des applications basées sur les réseaux.

Avec tant de problèmes technologiques, pourquoi donc s'escrimer à vouloir à tout prix utiliser le protocole IP afin de transporter la voix. Alors que les réseaux téléphoniques le font très bien et pour des coûts en constante diminution ? [11]

1-Réduction des coûts d'appel

Dans le cas d'une communication via IP, il n'est facturé en terme de téléphonie que la transition sur les réseaux téléphoniques classiques. Ainsi que vous appelez votre voisin ou bien un client à l'autre bout du monde, il ne vous en coûtera que le prix d'une communication locale. Ces solutions s'avèrent donc beaucoup plus avantageuses si vos appels téléphoniques se font sur longue distance. [11]

2-Mutualisation des réseaux, simplification de l'architecture

Le réseau téléphonique d'une entreprise qui a choisi la Voix sur IP est dorénavant géré comme un réseau informatique. Il n'existe plus un réseau téléphonique et un réseau informatique mais belle et bien, un système d'information dans sa globalité qui s'avère bien plus facile à gérer. Il n'y a plus besoin que d'une équipe informatique qui gère l'ensemble. Cela permet également d'alléger les coûts d'infrastructure en terme de réseau capillaire (le câblage). [11]

3-Prépondérance de la téléphonie et convergence voix-données

Quelques soient les époques, le dialogue de vive voix a toujours été le mode de communication préféré des Hommes. Lorsque vous essayer de résoudre un problème à distance avec votre interlocuteur via des solutions de messagerie instantanée par exemple, vous avez toujours plus ou moins envie de prendre le téléphone et d'appeler votre correspondant, meilleur interactivité, meilleur moyen de s'exprimer, rapidité également. Les téléphones peuvent maintenant appeler les Ordinateur et les ordinateurs appeler des téléphones. La communication s'en trouve ainsi encore facilitée. De plus, le nouveau cap à franchir est la convergence globale voix données. Beaucoup d'application son basée autour de la communication téléphonique. Votre messagerie ne comportera plus que des emails, mais également des messages enregistrés. La vidéo conférence se généralisera également. [11]

V-Perspectives

1-Le challenge de la VoIP :

L'application "voix sur IP" peut s'intégrer aux offres de réseaux privés virtuels des entreprises, ou bien elle peut être ouverte à tout utilisateur de poste téléphonique ordinaire, ou d'ordinateur connecté à un réseau public. Cette multiplicité de choix explique la confusion des jugements de valeur qui sont émis aujourd'hui encore en faveur ou contre l'usage de la téléphonie sur Internet.

Il est certain que l'évolution des réseaux conduit à un changement des usages. Nous passons très progressivement du règne des classiques réseaux publics en commutation de circuits à l'émergence de la technologie des réseaux en mode paquets, dont l'évolution est encore loin d'être achevée et dont les performances devraient progressivement s'améliorer. La téléphonie sur Internet ouvre donc des applications nouvelles qui vont conduire l'évolution des réseaux IP.

De plus, la communication de type vocal étant l'une des applications de communications les plus exigeantes en qualité de service, les réseaux de paquets en IP doivent évoluer (techniquement et économiquement) pour rendre cette application acceptable en toute circonstance et en tout lieu, quel que soit le réseau et la chaîne de connexion utilisés. Des classes de service de VoIP sont en cours d'étude, offrant des délais de transmission variés. L'Union In-

ternationale des Télécommunications (UIT-T G114) a fixé la limite entre service téléphonique et transport de la voix à 150ms. [11]

Nom	Latence	Utilisation recommandée
Class 1	0 à 150 ms	Communications normales
Class 2	150 à 300 ms	Bidirectionnel peu interactif
Class 3	300 à 700 ms	Half Duplex
Class 4	700 à + ms	Radio Amateur et militaires.

Tableau 2 : Limite entre Service téléphoniques et transport de la voix

Aujourd'hui, vu sous l'aspect global, le marché semble s'orienter vers l'interconnexion permanente de tous les systèmes possibles au coût le plus faible, de façon à faciliter le transfert d'informations en tout lieu vers toute personne qui le souhaite, ouvrant ainsi les possibilités d'achats et de ventes de marchandises ou de biens au meilleur prix. La connectivité permanente à haut débit (supérieur à 200 ou 400 kbit/s selon les auteurs) devrait permettre des applications voix, données et images propices au télétravail, à la télémédecine (e-health), au téléenseignement (e-education), à l'aide de la gestion des collectivités (e-gouvernement), etc.

La première étape qui précède ces projets grandioses concerne l'adaptation de chacun des réseaux d'accès régionaux aux techniques de haut débit les plus appropriées, compte tenu de la densité d'usage en hauts débits (Gbit/s / km²) et de la répartition des populations visées.

Ensuite, vient le choix des protocoles de communications adaptés aux applications sélectionnées, opération qui s'effectuera progressivement dans le temps, après plusieurs évolutions, probablement.

2-Les difficultés de VoIP :

Plusieurs problèmes subsistent pour le développement de VoIP. La VoIP demande l'emploi de terminaux spéciaux qui sont encore coûteux. La numérotation des terminaux VoIP doit être gérée par un bureau unique et en général, un préfixe commun (le 050, au Japon par exemple) leur est alloué, encore à titre provisoire.

Dernier inconvénient majeur connu, les services d'urgence demeurent seulement joignables par le réseau classique. Les abonnés sont astreints à conserver le terminal classique pour la réception des appels non-VoIP. Le statut d'exploitant de service vocal sur IP ne peut donc pas couvrir un service qui est attaché à des obligations de service public. Pas question également de parler de "service universel" ! VoIP demeure encore considéré juridiquement comme un service d'information de données sur liaison à haut débit. La question aujourd'hui est de savoir si VoIP doit recevoir un statut particulier, avec des contraintes inhérentes, ou bien, s'il est préférable de ne pas imposer de réglementation sur cette application. La réglementation pourrait simplement accepter que le paiement ne se fasse plus à la durée, mais sur la base d'une contribution fixe mensuelle attachée à la valeur d'un débit permanent délivré.

Comment doit-on considérer un fournisseur d'accès à Internet qui proposerait des accès de téléphonie en VoIP ? Aux Etats-Unis, cette réglementation se décide au niveau de cha-

cun des Etats, de sorte que des opinions contradictoires sur VoIP ont été émises. Ce désordre n'est pas favorable à l'extension internationale de VoIP, car il tend à soutenir la position des exploitants historiques qualifiés de "dinosaures" par les partisans de VoIP. Pourtant, parmi cela, ils y en a qui offrent déjà des applications VoIP car ils ont compris que l'objectif d'un exploitant dynamique est de créer de la valeur ajoutée !

L'Europe semble avoir une attitude plus souple à cet égard que les Etats-Unis. Bruxelles se montre plus sévère pour les exploitants qui ont pris une position dominante (les exploitants dits "puissants") que pour ceux qui s'essaient au développement de nouveaux services. VoIP devrait logiquement trouver un terrain favorable en Europe, poussé par l'essor des réseaux d'accès numériques.

Malheureusement, il y a loin de la théorie à la pratique et pendant que certains traitent de l'évolution possible des notions juridiques du service universel au XXIème siècle, considéré comme un obstacle majeur, les spécialistes en normalisation ont abandonné leurs études sur le VCoDSL (Voice Channelization on DSL), jugées commercialement "lourdes et inopportunes " ! [11]

Conclusion

Beaucoup de développements techniques se sont produits dans un passé récent et il a toujours été difficile de formuler des prévisions sur ce qu'il est susceptible de se produire dans le domaine des communications. **Mais VoIP est sans doute l'un des fleurons des applications de la technologie numérique qui devrait engendrer, dès 2004, de nombreux développements dans les réseaux et dans notre société.**

Il y a deux types de statistiques à rapprocher. D'abord, on estime que le nombre d'utilisateurs de VoIP sur des connexions à haut débit devrait atteindre les 200 000 dans le monde et 20 000 en Europe. Le Japon est plus optimiste et estime que son parc actuel de 2,3 millions de terminaux IP en usage à la fin de 2002 parviendra au chiffre de 23 millions dès 2007.

Malgré l'incohérence du rapprochement de ces chiffres, on remarque que la croissance de l'usage de VoIP semble être corrélée à la croissance du parc d'ordinateurs et des terminaux mobiles de troisième génération. Ceci ne fait pas encore de VoIP un outil réellement efficace pour réduire la fracture numérique ou pour élargir l'audience d'Internet.

Il y a donc (et fort heureusement !) encore de nombreux problèmes à résoudre ! Au travail !

Chapitre II : La ToIP

Introduction

Dans ce chapitre, nous présenterons les contraintes liées à la ToIP. Ensuite donnerons-nous une liste de solutions existantes et futures ainsi que les avantages pour ce type de téléphonie. Puis montrerons-nous brièvement la différence entre la VoIP et la ToIP. Et enfin, nous parlerons de manière superficielle d'Asterisk, afin d'avoir une idée sur son fonctionnement dans le dernier chapitre qui est la phase la plus importante.

Définition

La téléphonie sur IP (ToIP) est un ensemble de technologies visant à utiliser un réseau sous protocole TCP/IP pour y faire circuler des conversations téléphoniques.

Cette technologie permet de communiquer de façon très simple sur un réseau IP, mais elle permet également d'établir des ponts avec le réseau téléphonique historique (nommé RTC pour réseau téléphonique commuté).

Il devient ainsi possible d'établir des communications entre des personnes téléphonant depuis des réseaux différents. Pour cela, il faut installer des cartes chargées de transformer les trames IP en signal pouvant transiter sur le réseau classique. [1]

Ces cartes sont nommées carte PABX (Private Automatic Branch eXchange).

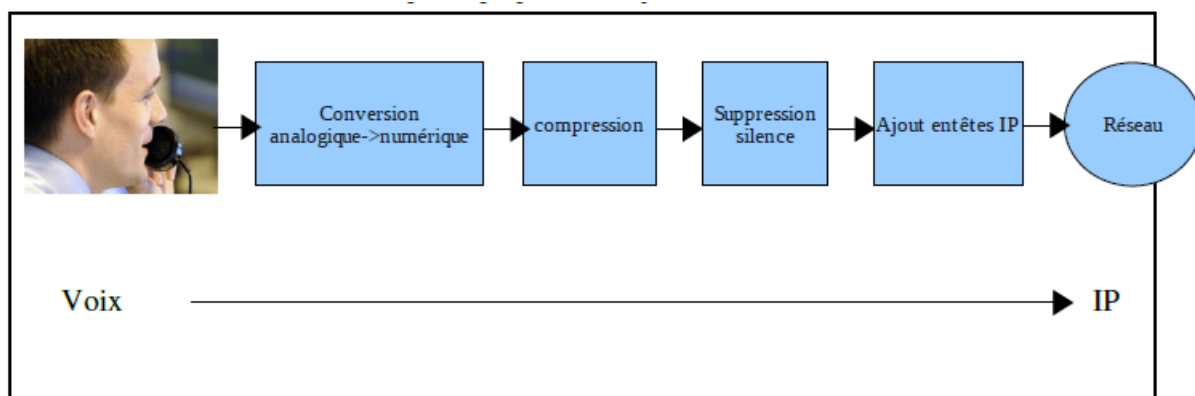


Figure 4 : Principe pour transformer la voix en IP

Explications:

La bande voix (qui est un signal électrique analogique) est d'abord échantillonnée numériquement par un convertisseur puis compressée selon une certaine norme de compression variable selon les codecs utilisés, puis ensuite on peut éventuellement supprimer les pauses de silences observées lors d'une conversation, pour être ensuite habillée RTP,UDP et enfin en IP. Une fois que la voix est transformée en paquets IP, ces paquets IP identifiés et numérotés peuvent transiter sur n'importe quel réseau IP (ADSL, Ethernet, Satellite, routeurs, switches, PC, Wifi, etc...) [1]

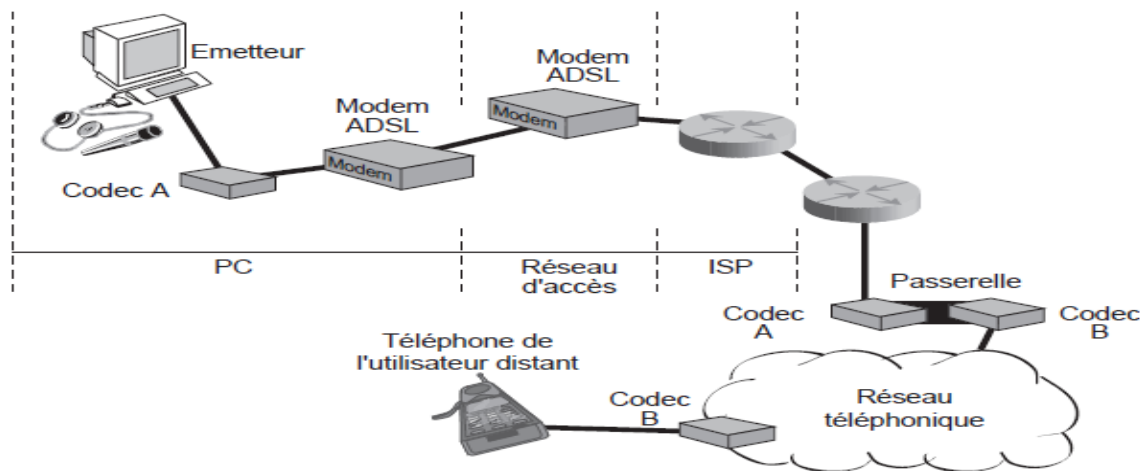


Figure 5: Architecture de la ToIP

I- Les Contraintes de la ToIP

Elles sont nombreuses alors nous parlerons de quelques un. [8]

1-Contraintes temporelles

La principale difficulté pour réaliser de la téléphonie par paquet provient de la contrainte temporelle très forte due à l'interaction entre individus. Le temps de latence, c'est-à-dire le temps qui s'écoule entre l'entrée d'un paquet dans le réseau et son temps de sortie du réseau doit être inférieur à 300 ms si l'on veut garder une interaction humaine acceptable.

Si l'on souhaite une bonne qualité de la conversation, il ne faut pas que la latence soit supérieure à 150 ms.

2-Le processus de resynchronisation de la parole téléphonique

Du fait de l'interactivité entre deux interlocuteurs, la téléphonie IP implique une contrainte temporelle de 600 ms (300 ms dans chaque sens). Il faut donc, après le transport des échantillons dans le réseau, les resynchroniser au récepteur de sorte qu'un flot régulier soit remis au codec. La difficulté provient du temps de transport asynchrone, assez aléatoire, du réseau, qui implique que les paquets sont remis au récepteur à des instants quelconques.

3-Qualité de service de la ToIP

D'une manière générale, on retient trois facteurs pour déterminer la qualité de service d'une application de téléphonie :

- **Qualité de la transmission de la voix :** C'est la partie technique qui prend en compte le signal de départ et qui essaie de le retranscrire au mieux au niveau du récepteur.
- **Efficacité de la conversation :** C'est l'interactivité plus ou moins grande entre les deux individus en train de converser.
- **Intelligibilité de la communication :** C'est la façon dont s'expriment les individus en communication.

Ce dernier facteur ne dépend que des individus qui parlent, mais l'impact des deux premiers facteurs est important sur le troisième. Si l'intelligibilité est faible et qu'en plus la qualité de la transmission et l'efficacité de la conversation sont mauvaises, il y a de fortes chances que les paroles ne soient pas comprises.

II-Les Solutions de la ToIP

Le développement de la ToIP a vu se succéder sur plusieurs années différentes générations de services et de configurations.

1-Solution 1

La première génération de téléphonie IP grand public a été proposée par des opérateurs alternatifs afin d'offrir des communications internationales à tarif local. Ce service consiste à rassembler un grand nombre de voies téléphoniques classiques sur le commutateur local et à les encapsuler dans un même paquet IP. Ce paquet IP peut devenir assez important suivant le nombre de voix multiplexées et le nombre d'octets de chaque voix.

L'utilisateur se connecte en local sur le commutateur de l'opérateur historique. L'opérateur alternatif récupère les différentes voix et les multiplexe sur Internet ou sur une même liaison IP, transatlantique par exemple. À la sortie du réseau IP, les voies de parole retrouvent leur composition normale sur le commutateur local et sont envoyées de façon classique aux destinataires au travers de la boucle locale de l'opérateur de télécommunications.

Si la téléphonie locale est gratuite, comme aux États-Unis, le coût total est approximativement égal à la tarification locale de départ. Les opérateurs de téléphonie classique suivent plus ou moins les mêmes principes, tout en tentant de préserver une marge bénéficiaire importante. D'où une chute des prix beaucoup plus lente.

Cette solution est illustrée à la figure 6 [7]

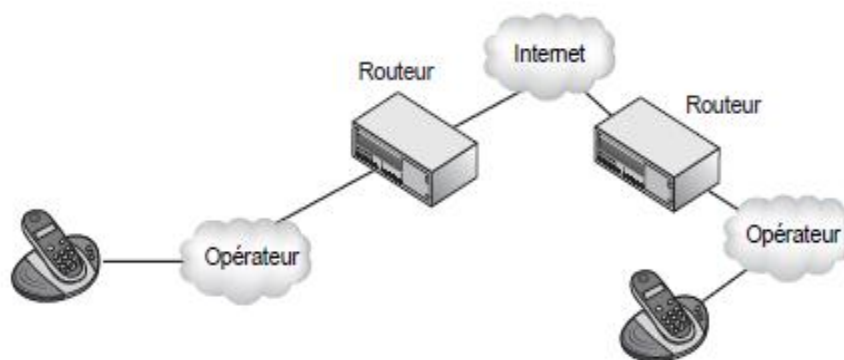


Figure 6 : *La première génération de Téléphonie sur IP*

2-Solution 2

La deuxième génération a vu les opérateurs de télécommunications offrir des accès Internet au travers de la boucle locale *via* des modems standards permettant des débits de l'ordre de 50 Kbit/s.

Sur cet accès Internet peuvent être raccordés des ordinateurs personnels. Si l'ordinateur est équipé d'un micro et d'un haut-parleur, il est possible d'utiliser l'ordinateur personnel comme téléphone et de faire transiter les paquets de téléphonie sur Internet après les avoir acheminés sur la boucle locale de l'opérateur. [7]

Cette amélioration est illustrée à la figure 7

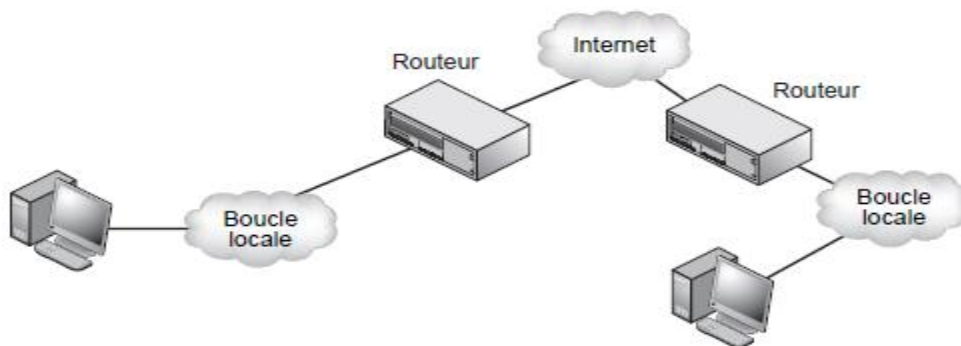


Figure 7 : La téléphonie au travers de l'ordinateur personnel

3-Solution 3

Dans la troisième génération, au lieu d'utiliser l'ordinateur comme téléphone, un combiné analogique est connecté au PC, équipé d'une carte d'acquisition de la parole téléphonique.

L'ordinateur personnel joue ici le rôle d'une passerelle, transformant le signal analogique du combiné en un flux d'octets de téléphonie numérisés par un codec intégré à l'ordinateur. Les octets sont envoyés par un modem vers le routeur de l'opérateur, auquel revient la charge de la paquetsation et de l'envoi des paquets IP. [7]

Cette étape est illustrée à la figure 8

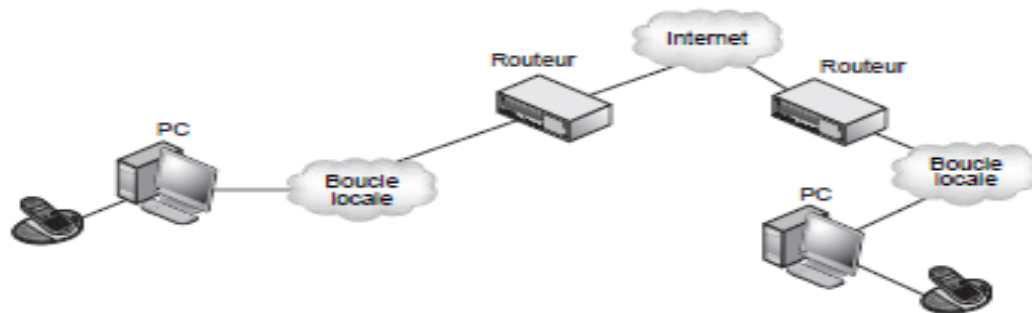


Figure 8: Téléphonie IP utilisant l'ordinateur personnel comme intermédiaire

4-Solution 4

La quatrième génération est caractérisée par l'arrivée de modems ADSL munis de plusieurs prises, chacune prenant en charge un média particulier et un protocole associé.

Le modem ADSL permet de connecter des téléphones standards. Les conversions nécessaires sont effectuées dans le modem, qui devient de ce fait une véritable *Internet Box*, le travail spécifique de la partie modem devenant mineur par rapport à l'ensemble des fonctionnalités réseau réalisées.

La boucle locale de l'opérateur transporte les paquets IP. Pour sa part, le téléphone demeure analogique. [7]

Cette solution est illustrée à la figure 9

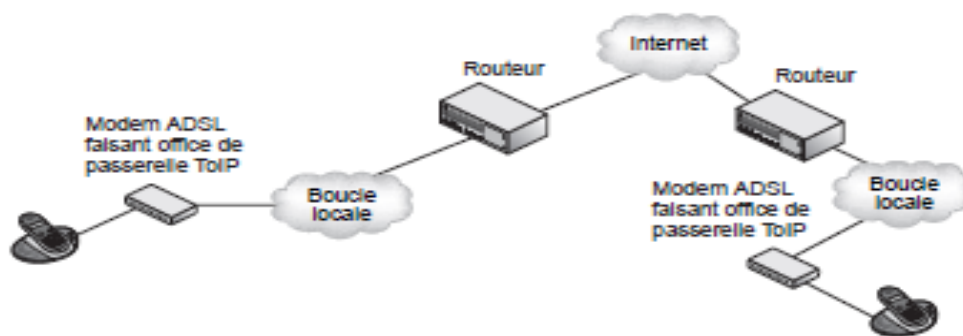


Figure 9: Apparition du modem ADSL dans la chaîne de transmission de la téléphonie

5-Solution 5

La cinquième génération du processus aboutit à de la téléphonie IP de bout en bout. La paquetsation est repoussée dans l'équipement terminal de l'utilisateur. Le téléphone devient un téléphone IP.

La figure 10 illustre cette solution. Le téléphone IP n'est pas connecté directement sur la boucle locale de l'opérateur mais sur le réseau d'entreprise, lui-même connecté à l'opérateur. Le téléphone IP fait en réalité office de routeur. Il intègre en outre un codec et assure la paquetsation IP et l'encapsulation des paquets IP dans une trame Ethernet. La trame Ethernet est ensuite transmise sur le réseau d'entreprise. [7]

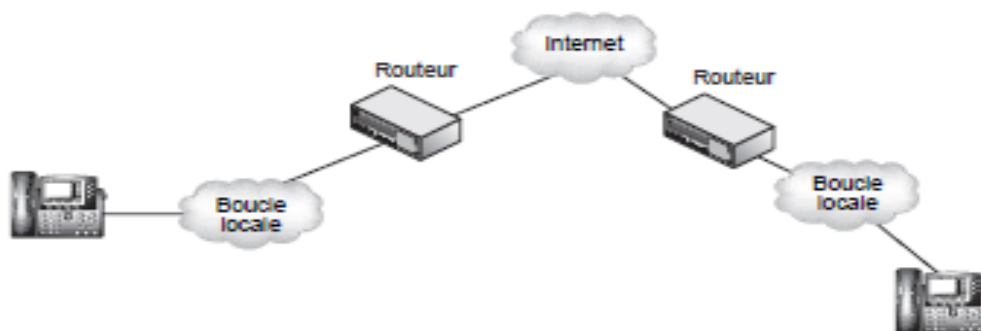


Figure 10 : Téléphonie IP de bout en bout

6-Solution 6

Avec l'arrivée massive d'ordinateurs personnels suffisamment puissants pour émuler un téléphone IP, la ToIP est devenue une téléphonie de bout en bout gratuite, puisque la téléphonie devient une application comme une autre transitant par l'intermédiaire du modem ADSL.

Du fait de cette configuration, de nouvelles applications ont fait leur apparition pour proposer des services grand public. Parmi celles-ci, Skype ou MSN (Microsoft Network) proposent de la téléphonie sur IP de bout en bout.

En cas d'utilisation d'un logiciel de téléphonie sur l'ordinateur portable, le flux de téléphonie est multiplexé avec l'ensemble des données et n'est pas traité de façon spécifique.

On appelle cette solution, le Double-Play lorsqu'il y a un canal de données et un canal téléphonique et Triple-Play lorsqu'un canal de télévision est ajouté voir figure 11 [7]

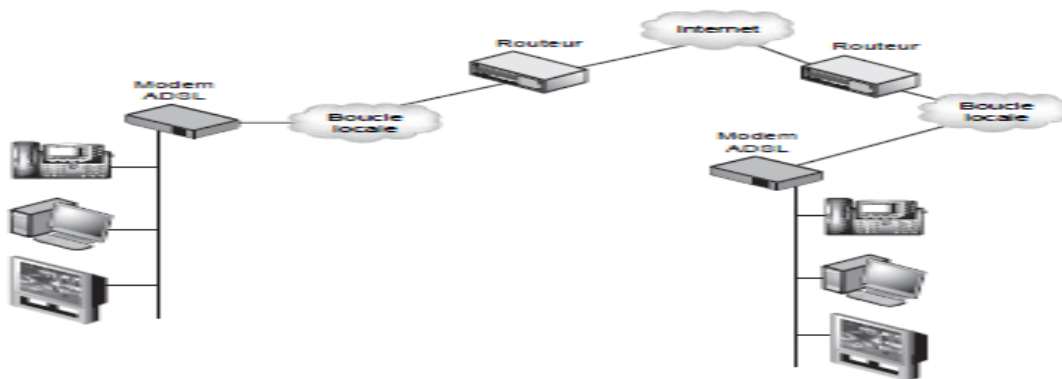


Figure 11 : Le triple-Play

7-Solution 7

Si l'on ajoute un canal supplémentaire, comme le canal de mobilité provenant d'un terminal mobile de type GSM/Wi-Fi, on parle de Quadruple-Play. Lorsque ce téléphone est situé près d'un modem incorporant un réseau Wi-Fi, le mobile se connecte en Wi-Fi.

S'il n'est pas situé dans une zone Wi-Fi, le téléphone utilise le mode GSM. Il est possible de commencer à téléphoner en Wi-Fi et de continuer en GSM lorsqu'on sort de la zone Wi-Fi. En sens inverse, le téléphone peut éventuellement repasser en Wi-Fi. [7]

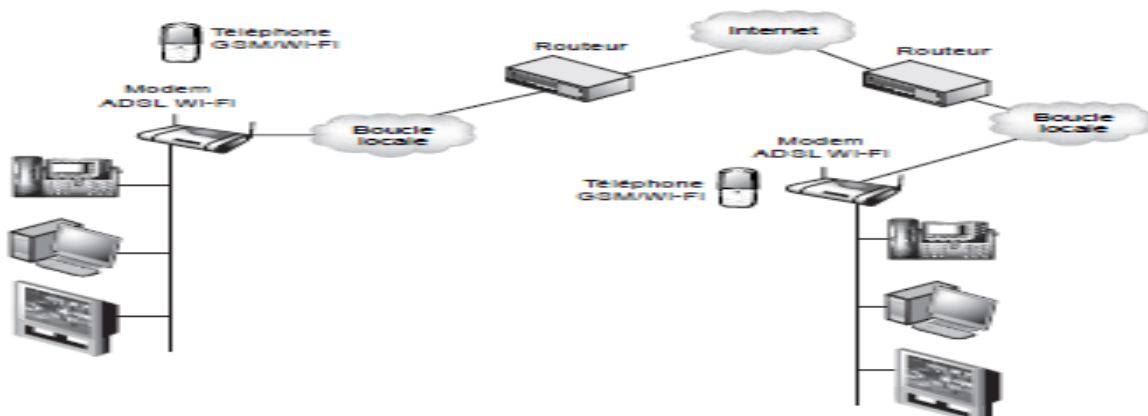


Figure 12: quadruple-Play

III- Avantage de la ToIP

Le principal argument en faveur des systèmes de téléphonie sur IP est la garantie d'un retour sur investissement en quelques années. En effet, elle permet la réduction de nombreux coûts tels que les coûts de communication, de câblage, de maintenance, de supervision du système... [2]

Aussi, certaines fonctionnalités reposant sur la nature même de la téléphonie IP seront aussi disponibles avec une qualité et une facilité d'utilisation bien supérieure à la téléphonie classique. Il s'agit de la transmission parallèle de données (vidéo,...) et de la conférence multi-point.

Remarque :

La voix sur IP concerne la partie du cœur de réseau, c'est à dire tous les équipements d'interconnexion permettant à un poste d'en appeler un autre.

La ToIP repose sur le réseau local privé LAN de l'entreprise (utilisation du câblage réseau informatique existant) et la gestion du central de communication est réalisée depuis n'importe quel site de l'entreprise. Les entreprises multi-sites allègent leurs coûts en liaison d'interconnexion entre les établissements et en coût de communication car les communications inter-sites sont gratuites. [2]

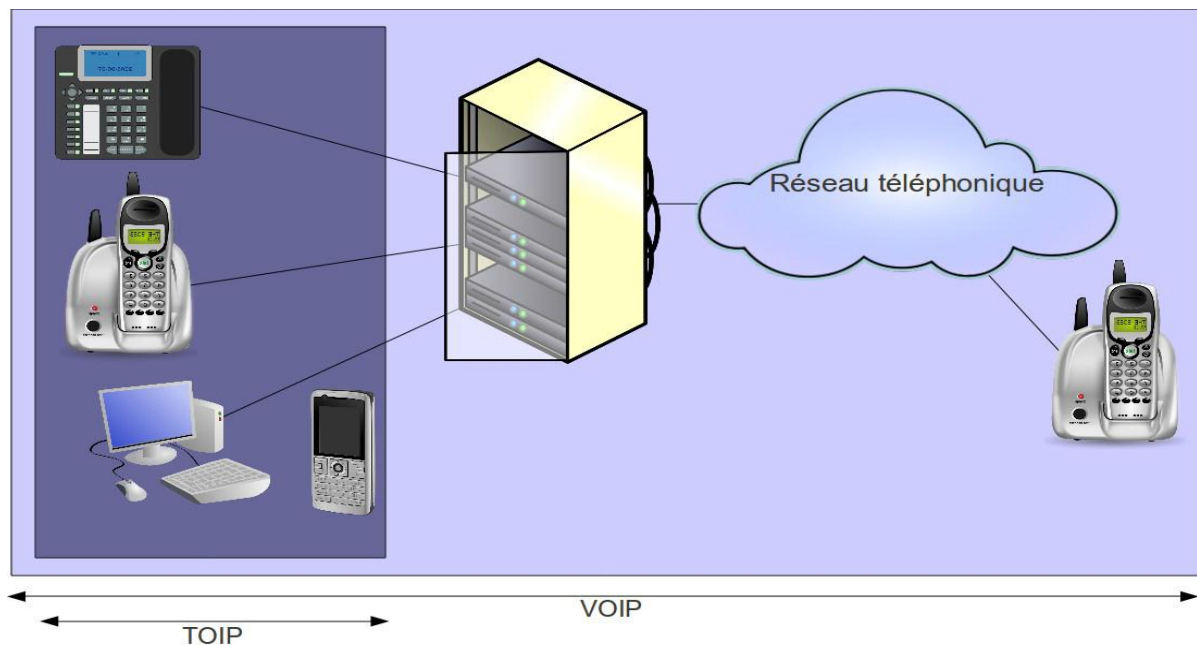


Figure 14 : *Différence entre la ToIP et la VoIP*

Conclusion

En regard des explications précédentes, on perçoit que la qualité du service n'est pas équivalente à celle qui est offerte par les opérateurs habituels, et cela pour plusieurs raisons. Tout d'abord, en termes de fiabilité, la téléphonie sur Internet ne peut prétendre rivaliser avec les télécommunications classiques. Bien sûr, lorsque le trafic sur le réseau et l'heure s'y prêtent, qu'il s'agit d'appels entre particuliers, cette technologie remplit parfaitement son office.

Mais dans son état actuel de développement, les entreprises ne peuvent pas encore lui faire confiance (ce procédé ne peut donc pas intéresser les entreprises qui basent leur activité sur une utilisation intensive du téléphone) et les particuliers se fatiguent vite des contraintes d'utilisation et des variations de qualité sonore. Néanmoins, cet aspect des choses va avoir tendance à s'estomper en conséquence des améliorations technologiques que l'on projette d'apporter.

Chapitre III : Protocoles liés à la ToIP

Définition

La téléphonie sur IP ou ToIP (Telephony over IP) est un service de téléphonie qui transporte les flux voix des communications téléphoniques sur un réseau IP. A la différence de la VoIP ou l'on ne fait qu'établir une communication «voix», la ToIP intègre l'ensemble des services associés à la téléphonie : double appel, messagerie, renvoi d'appel, FAX, etc.

Afin de rendre possibles les communications ToIP, les solutions proposées dopent la couche IP par des mécanismes supplémentaires nécessaires pour apporter la QOS nécessaire au flux voix de types temps réel, en plus de l'intelligence nécessaire à l'exécution de services.

A cet effet, il existe deux types de protocoles principaux utilisés dans la ToIP :

Protocoles de signalisation

Protocoles de transport

I- Les protocoles de signalisation:

La signalisation désigne la transmission d'un ensemble de signaux et l'information de contrôle échangés entre les intervenants d'une communication. Ces intervenants peuvent être des entités en bout de liaison (terminaux) ou des entités intermédiaires de contrôle et de gestion des communications. Leurs échanges permettent l'initiation, la négociation, l'établissement, le maintien et la fermeture de la connexion.

Il convient de distinguer deux types de transferts pour comprendre à quoi correspond la signalisation :

- le transfert de données brutes ;
- le transfert d'informations de contrôle.

Plusieurs normes et protocoles ont été développés pour la signalisation ToIP, quelques-uns sont propriétaires et d'autres sont des standards. Ainsi, les principales propositions disponibles pour l'établissement de connexions en ToIP sont :

- SIP (Session Initiation Protocol) qui est un standard IETF (Internet Engineering Task Force) décrit dans le RFC 3261.
- H323 englobe un ensemble de protocoles de communication développés par l'UIT-T (Union Internationale des Télécommunications – secteur de la normalisation des Télécommunications).
- MGCP (Media Gateway Control Protocol) standardisé par l'IETF (RFC 3435).
- SCCP (Skinny Client Control Protocol) est un protocole propriétaire CISCO.

1-Le protocole H.323 :

Développé par le groupement ITU-T, le protocole H.323 s'articule autour d'une architecture particulière. Cette dernière concentre les fonctionnalités autour d'entités, ce qui explique pourquoi le protocole H.323 est considéré comme fortement centralisé.

Les quatre entités d'une architecture H.323 :

a-Les terminaux (au minimum deux):

Un terminal ou client est le point de départ ou d'arrivée d'un flux de données H.323. On distingue deux catégories de terminaux : les terminaux matériels (les combinés téléphoniques IP) et les terminaux logiciels (les softphones). Deux terminaux doivent au minimum être présents pour qu'une communication ait lieu.

b-Le MCU (Multipoint Control Unit):

La conférence entre plusieurs terminaux est assurée par le MCU ou unité de contrôle multipoint, parfois appelée pont multipoint. C'est l'équipement permettant la gestion des conférences, c'est-à-dire les communications multimédias mettant en jeu plus de deux interlocuteurs.

Ces derniers doivent préalablement se connecter à la MCU, sur laquelle s'établissent les demandes et négociations des paramètres à utiliser lors de la conférence.

c-Le Gatekeeper :

Gatekeeper ou garde-barrière, est l'équipement qui assure la localisation des utilisateurs. Ces derniers peuvent s'identifier entre eux par des noms, auxquels il faut attribuer l'adresse IP correspondante dans le réseau ou, si l'appelé n'est pas situé dans un réseau IP, la localisation de l'entité intermédiaire à joindre pour l'appel.

Outre cette fonction primordiale, un gatekeeper remplit tout un ensemble de fonctions complémentaires de gestion et de contrôle des communications, certaines étant indispensables et d'autres facultatives.

d-La passerelle :

Passerelle, ou gateway, permet de faire l'interface entre plusieurs réseaux. Permettant ainsi à des utilisateurs du réseau IP de joindre les utilisateurs qui sont actifs sur d'autres types de réseaux téléphoniques, RTC, RNIS ou ATM.

On peut avoir autant de passerelles différentes que nécessaire, suivant la nature des réseaux non-IP à interconnecter.

Aujourd'hui, H.323 tend à disparaître et à se marginaliser. Bien souvent, sa présence n'est justifiée que pour des raisons historiques. Le protocole qui devrait s'imposer comme son remplaçant, SIP, a pour sa part été entièrement conçu selon la philosophie du monde IP.

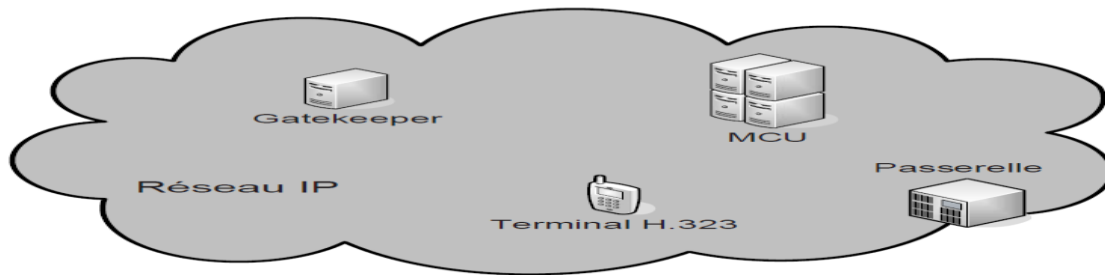


Figure 15 : Composantes de l'Architecture H.323

2-Le protocole SIP :

Le protocole SIP (Session Initialisation Protocol) a été initié par le groupe MMUSIC (Multiparty Multimedia Session Control) [RFC 2543] et désormais repris et maintenu par le Groupe SIP de l'IETF [RFC 3261].

SIP est un protocole de signalisation appartenant à la couche application du modèle OSI. Il a été conçu pour l'ouverture, le maintien et la terminaison de sessions de communications interactives entre des utilisateurs. De telles sessions permettent de réaliser de l'audio, de l'enseignement à distance et de la voix (téléphonie) sur IP essentiellement.

Pour l'ouverture d'une session, un utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de négocier sur les algorithmes et codecs à utiliser. SIP permet aussi de relier des stations mobiles en transmettant ou redirigeant les requêtes vers la position courante de la station appelée. Enfin, SIP est indépendant du médium utilisé et aussi du protocole de transport des couches basses.

a-Architecture protocolaire :

SIP est un protocole indépendant des couches de transport, il appartient aux couches applications du modèle OSI. Le SIP gère la signalisation et l'établissement des sessions interactives de communication multimédias et multipartites. Il est aussi basé sur le concept Client / Serveur pour le contrôle d'appels et des services multimédias.

Conçu selon un modèle de type IP, il est hautement extensible et assez simple en conception architecturale, de sorte qu'il peut servir de base à la création d'applications et de services. Il est basé sur le protocole HTTP et peut utiliser UDP ou TCP.

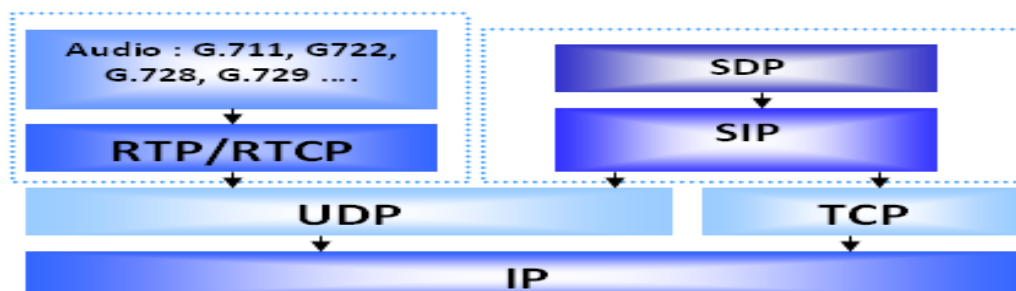


Figure 16 : Architecture protocolaire

b-Architecture d'une plate-forme 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 figure17 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.

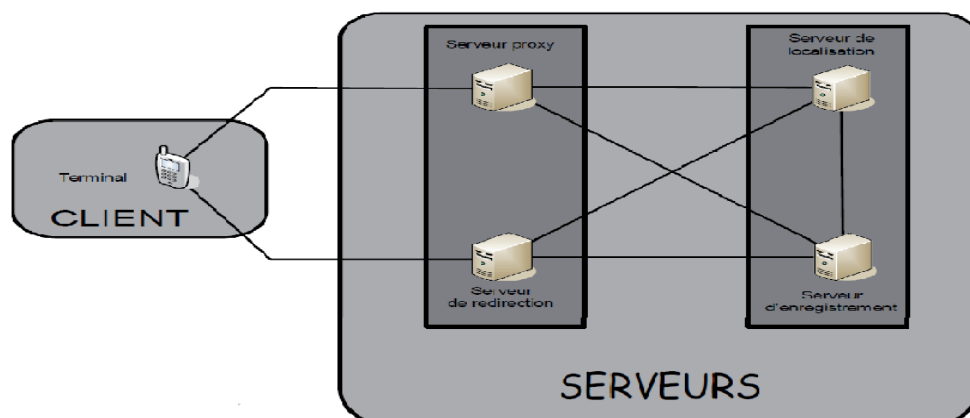


Figure 17 : *Echange entre terminal et services associés*

Explication :

Terminal SIP UA (User Agent):

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). Il est constitué de deux sous-entités, comme illustré à la figure ci-dessous :

- 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.

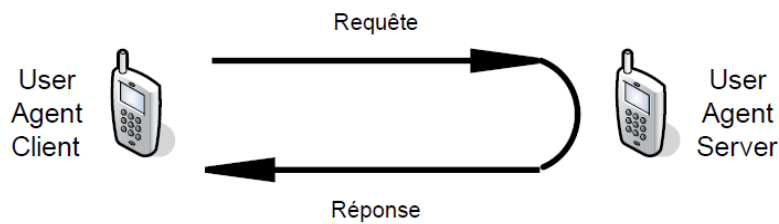


Figure 18 : *Dialogue entre deux entités*

La communication peut être clôturée indifféremment par l'un ou l'autre. 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

Le serveur d'enregistrement (Registrar Server) offre un moyen de localiser un correspondant avec souplesse, tout en gérant la mobilité de l'utilisateur. Il peut en outre supporter l'authentification des abonnés. Dans la pratique, lors de l'activation d'un terminal dans un réseau, la première action initiée par celui-ci consiste à transmettre une requête d'enregistrement auprès du serveur d'enregistrement afin de lui indiquer sa présence et sa position de localisation courante dans le réseau.

C'est la requête REGISTER, que l'utilisateur envoie à destination du serveur d'enregistrement. Celui-ci sauvegarde cette position en l'enregistrant auprès du serveur 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

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.

Lorsqu'un utilisateur demande à un serveur proxy de localiser un correspondant, ce dernier effectue la recherche, mais, au lieu de retourner le résultat au demandeur (comme le serveur de redirection), il utilise cette réponse pour effectuer lui-même l'initialisation de la communication en invitant le correspondant à ouvrir une session.

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.

3-Structure des messages SIP

Les messages SIP sont caractérisés par une ligne de début, plusieurs entêtes et le corps du message.

➤ Les entêtes des messages SIP

Les entêtes ont pour rôle de fournir des informations sur le message et de permettre le traitement du message. A cet effet, le protocole SIP est doté d'un certain nombre d'entête dont la structure dépend de la nature et du rôle de chaque entête. La structure générale d'un entête est articulée autour de plusieurs champs et chaque champ obéit à un format général : `nom_du_champ : valeur_du_champ`.

Les types d'entête utilisés par les messages du protocole SIP sont au nombre de quatre:

❖ L'entête général

Il est toujours présent et contient les informations de base permettant le traitement du message.

Il a des champs obligatoires suivants :

- Via : il identifie l'entité de relais. En effet, chaque entité qui émet ou re-laye un message SIP insère son identité afin de prévenir les boucles et indiquer le chemin de réponse.
- From : il identifie l'initiateur de la requête.
- To : il identifie le destinataire de la requête.
- Call-Id : c'est l'identificateur unique de la session.
- Cseq : il identifie la séquence d'un appel : par exemple plusieurs messages « invite » avec de Cseq différents.

❖ L'entête de requête

Cet entête est non toujours utilisé. Il contient des informations supplémentaires à destination du serveur SIP permettant le traitement de la requête par celui-ci.

❖ L'entête de réponse

Cet entête est non toujours utilisé tout comme l'entête de requête. Il contient des informations supplémentaires ajoutées par le serveur SIP permettant le traitement de la réponse.

❖ L'entête d'entité

Cet entête est toujours utilisé. Son rôle est de définir le type et le format des informations contenues dans les messages.

4-Le corps du message

Il fournit suffisamment d'informations pour permettre la participation à une session multimédia. Ces informations sont : le codec, destination (adresse IP et port UDP), nom de la session, etc. Le message du corps est codé conformément au protocole SDP (Session Description Protocole).

SDP est sans doute le protocole le plus important de l'architecture SIP, SDP a fait l'objet de la proposition de norme RFC 2327. C'est un protocole dont l'objectif est d'établir un descripteur de sessions multimédia à ouvrir, il porte les informations suivantes :

- Adresses de destination SIP: //UserX@ensa.ac.ma.
- Algorithmes de codage Audio et Vidéo.
- Type de trafic RTP.

5-Requêtes et Réponses SIP

SIP est un protocole de type client-serveur. A cet effet, les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes et de réponse SIP

Voici une liste exhaustive des requêtes SIP :

- INVITE : Cette requête indique que l'application (ou utilisateur) correspondante à l'Url SIP spécifié est invitée à participer à une session.
- ACK : Cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à requête INVITE.
- BYE : Cette requête est utilisée par le terminal de l'appelé pour signaler qu'il souhaite mettre un terme à la session.
- CANCEL : cette requête est envoyée par un terminal ou un serveur mandataire afin d'annuler une requête non validée par une réponse finale.
- REGISTER : Cette méthode est utilisée par le client pour enregistrer l'adresse listée dans le TO par le serveur auquel il est relié.

- **OPTION** : Un serveur mandataire en mesure de contacter le terminal appelé, doit répondre à une requête **OPTIONS** en précisant ses capacités à contacter le même terminal.

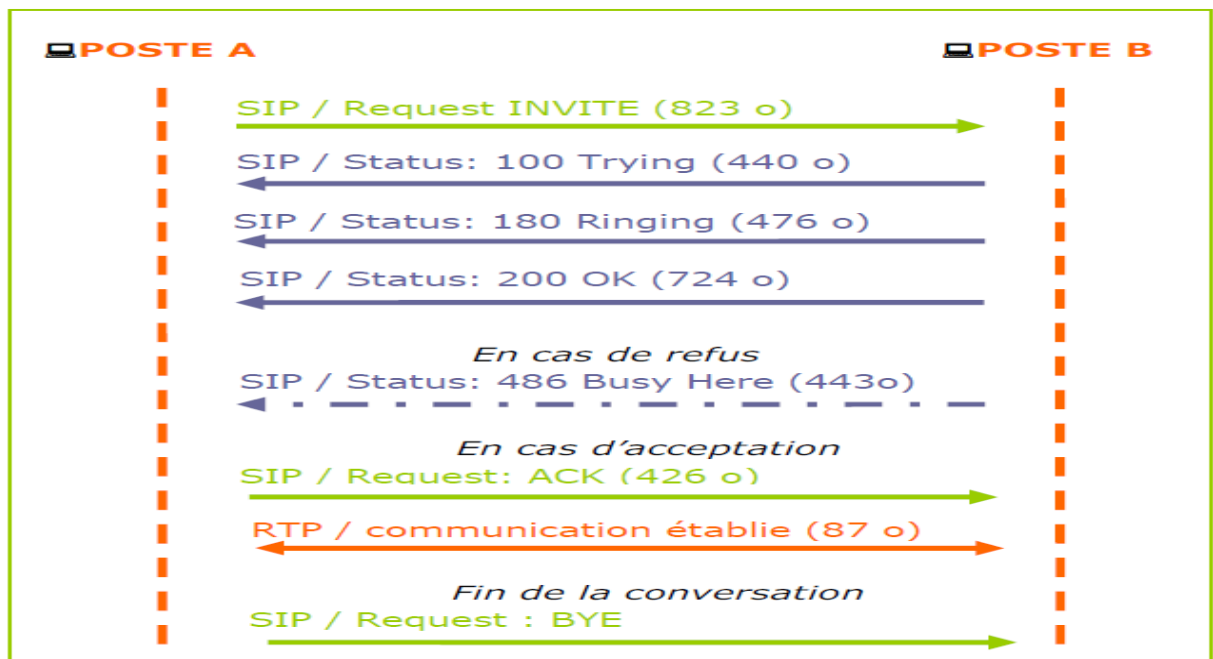


Figure 19 : illustration des requêtes et des réponses

A ces requêtes sont associées des réponses qui sont dans le même format que celles du protocole HTTP. Voici les plus importantes d'entre elles :

- 1XX - messages d'informations (100 – essai, 180 – sonnerie, 183 – en cours)
- 2XX – succès de la requête (200 – OK)
- 3XX – Redirection de l'appel, la demande doit être dirigée ailleurs
- 4XX – Erreur du client (La requête contient une syntaxe erronée)
- 5XX – Erreur du serveur (le serveur n'a pas réussi à traiter une requête correcte)
- 6XX – Echec général (606 – requête non acceptable par aucun serveur)

6-Fonctionnement

SIP intervient aux différentes phases de l'appel :

- Localisation du terminal de l'interlocuteur.
- Analyse du profil et des ressources du destinataire.
- Négociation du type de média (voix, audio, vidéo...) et des paramètres de communication.

- Disponibilité du correspondant, détermine si le poste appelé souhaite communiquer, et autorise l'appelant à le contacter.
- Etablissement et suivi de l'appel, avertit les parties appelant et appelé de la demande d'ouverture de session, gestion du transfert et de la fermeture des appels.
- Gestion de fonctions évoluées : retour d'erreurs, ...

Le schéma suivant illustre le scénario d'une communication SIP.

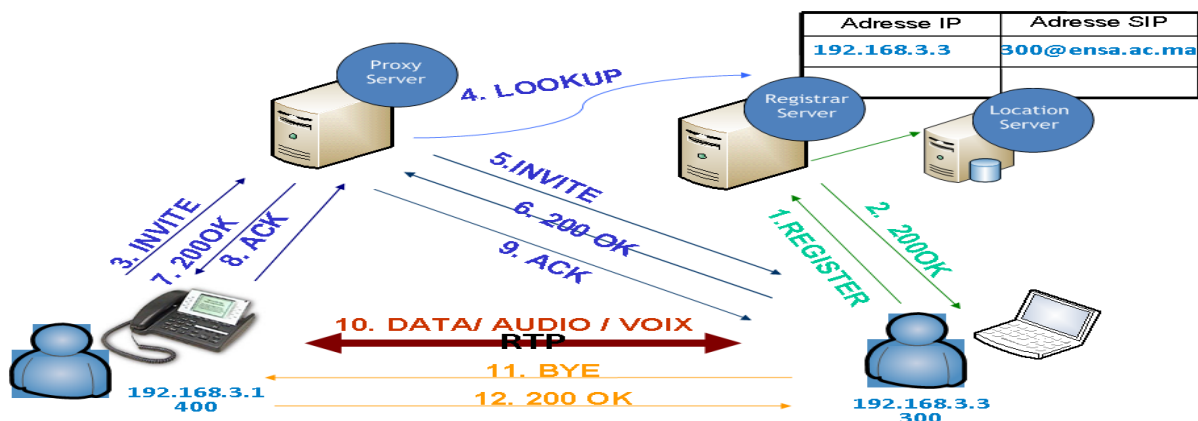


Figure 20 : scénario d'une communication SIP

7-Transport

Lors d'une communication ToIP, une fois la phase de signalisation réalisée, la phase de communication est initiée. Dans cette phase, un protocole de transport permet d'acheminer les données voix entre plusieurs utilisateurs vu que la couche TCP propose un transport fiable mais lent, et la couche UDP un transport rapide mais non fiable. La communauté IETF a mis en place un nouveau couple de protocole RTP (Real-Time transport Protocol) et RTCP (Real-Time Control Protocol) pour apporter la fiabilité à l'UDP tout en exploitant sa rapidité.

RTP et RTCP sont les deux protocoles qui sont principalement utilisés pour le transport de flux média sur le réseau IP. RTP permet de transporter les données entre plusieurs utilisateurs en plus de la gestion temps réelle de sessions. Tandis que, RTCP est utilisé pour transmettre régulièrement des paquets de contrôle, qui contient diverses statistiques, ce qui permet de vérifier la qualité de transmission.

8-Comparaison SIP/H.323

a- Avantages du protocole H.323

- Il existe de nombreux produits (plus de 30) utilisant ce standard adopté par de grandes entreprises telles Cisco, IBM, Intel, Microsoft, Netscape, etc.
- Un niveau d'interopérabilité très élevé, ce qui permet à plusieurs utilisateurs d'échanger des données audio et vidéo sans faire attention aux types de média utilisés.

b- Avantages du protocole Sip

- Sip est un protocole plus rapide. 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.
- Le nombre des en-têtes est limité (36 au maximum et en pratique, moins d'une dizaine d'en-têtes sont utilisées simultanément), ce qui allège l'écriture et la lecture des requêtes et réponses.
- De plus, il sépare les flux de données de ceux la signalisation, ce qui rend plus souple l'évolution "en direct" d'une communication (arrivée d'un nouveau participant, changement de paramètres...).
- Sip est un protocole indépendant de la couche transport. Il peut aussi bien s'utiliser avec TCP qu'UDP.

Le tableau qui suit est un tableau récapitulatif des différentes caractéristiques de SIP et de H.323

	SIP	H323
Nombre échanges pour établir la connexion	1,5 aller-retour	6 à 7 allers-retours
Maintenance du code protocolaire	Simple par sa nature textuelle à l'exemple de http	Complexe et nécessitant un compilateur
Evolution du protocole	Protocole ouvert à de nouvelles fonctions	Ajout d'extensions propriétaires sans concertation entre vendeurs
Evolution du protocole	Distribuée	Centralisée
Détection d'un appel en boucle	Oui	un appel routé sur l'appelant provoque une infinité de requêtes
Fonction de télé services	Oui, par défaut	H.323 v2 + H.450

Tableau 3 : Comparaison de SIP et H.323

La simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, du protocole Sip sont autant d'arguments qui pourraient permettre à Sip de nous convaincre s'utiliser ce protocole pour notre solution. De plus, ses avancées en matière de sécurité des messages sont un atout important par rapport à ses concurrents.

II-Standard ENUM

La fourniture à grande échelle du service ToIP suppose l'identification aisée des terminaux IP connectés au réseau désireux accéder à ce service. Cette identification est basiquement faite à travers les adresses IP. Afin d'étendre les possibilités d'adressages, l'UIT-T a travaillé sur le standard ENUM.

ENUM (tElephone NUmber Mapping) est un protocole défini par l'IETF dans le RFC 3761[11] permettant d'utiliser un numéro de téléphone (E.164) comme clé de recherche dans le DNS pour trouver la manière de joindre une personne (par exemple : n° de téléphone mobile, n° de fax, adresse de téléphonie IP, adresse e-mail, adresse de messagerie instantanée, etc.).

Le principe d'ENUM repose sur la création d'un nom de domaine Internet pour chaque numéro de téléphone du plan de numérotation international E.164. Les coordonnées que les utilisateurs souhaitent publier pour leur propre numéro de téléphone sont ensuite "stockées" dans le système des noms de domaine Internet (DNS) et ainsi rendues accessibles de manière globale pour tous.

Voici un schéma expliquant le principe de fonctionnement d'ENUM :

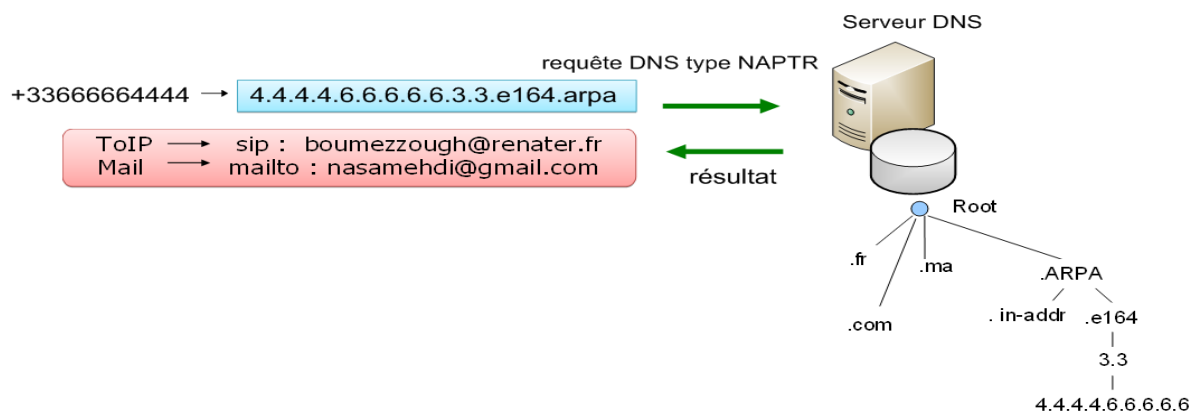


Figure 21: principe de fonctionnement d'ENUM

Dans ce schéma le numéro +33666664444 est transformé en nom de domaine en l'inversant (comme on fait pour trouver un nom de domaine à partir d'une adresse IP), cela donnerait 4.4.4.4.6.6.6.6.3.3.e164.arpa. On cherche alors les enregistrements NAPTR pour ce nom de domaine. Dans cet exemple, le titulaire du numéro de téléphone +33666664444 peut être joint en SIP en utilisant l'URI sip : boumezzough@renater.fr et par courrier électronique à nasamehdi@gmail.com.

L'avantage d'ENUM serait de joindre une personne avec un seul numéro sur différents services de communication aussi à travers ENUM une personne peut très bien spécifier l'ordre de préférence des services et des terminaux à utiliser.

La figure ci-dessous présente un exemple d'utilisation d'ENUM.

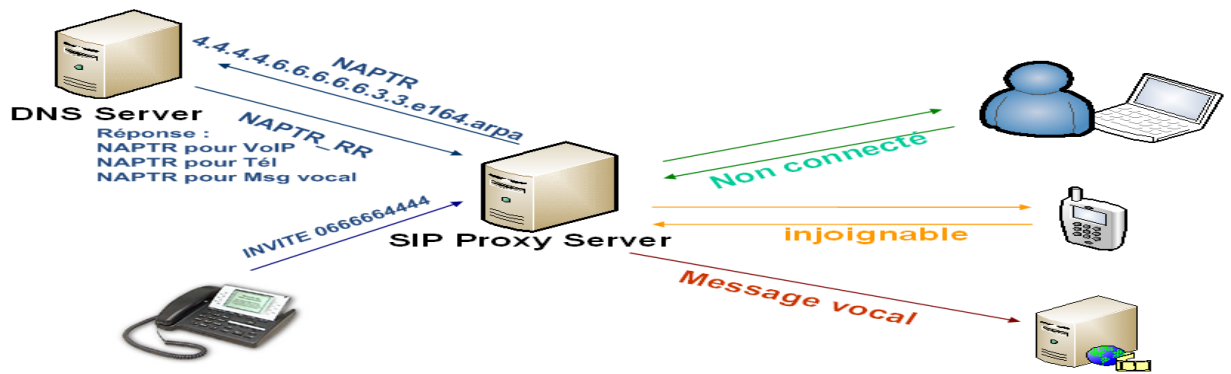


Figure 22 : utilisation d'ENUM

III-Problématique ToIP avec les NAT et les pare-feux

Dans une architecture ToIP, les NAT et les pare-feux représentent un problème pour les flux de signalisation et média. L'objectif de ce paragraphe est de comprendre cette problématique et de présenter des exemples de solutions existantes pour résoudre ce problème.

1-Problème de NAT

Le mécanisme NAT (Network Address Translation) est défini dans le RFC 16231[12]. Le NAT permet de faire correspondre les adresses IP internes souvent non routables d'un domaine à un ensemble d'adresses routables. Avec la ToIP, ce mécanisme représente un problème pour le transit des flux multimédia.

En effet, les informations utilisées pour la signalisation ou la communication sont incluses au niveau 4 et les couches supérieures du modèle OSI, tandis que les NAT travaillent sur la couche 3.

Voici un schéma expliquant le problème de NAT avec la ToIP :

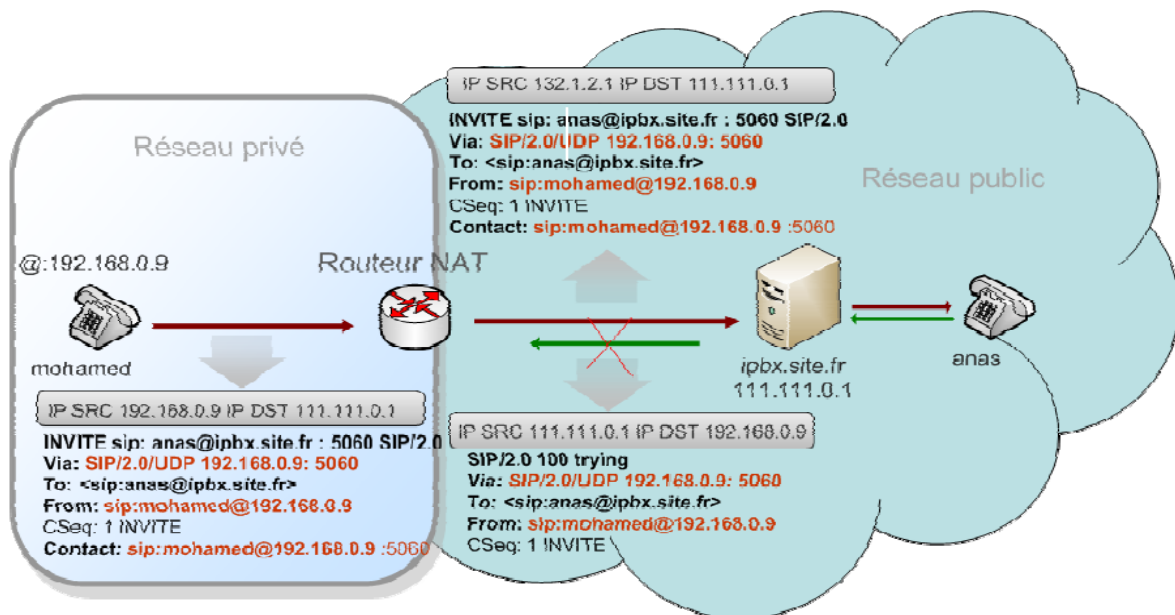


Figure 23 : problème de NAT avec la ToIP

Dans cet exemple, Mohamed ne pourra établir de communication avec Anas étant donné que l'IPBX n'arrive pas à relayer les réponses SIP de Anas. En effet, lors de la traduction d'adresse effectuée par le routeur NAT, seuls l'adresse et le numéro de port contenus dans le corps de la requête INVITE du message SIP ne sont pas modifiés. Hors cette adresse est non routable.

2-Problème de pare-feux

Un pare-feu (firewall) est un équipement permettant d'assurer la sécurité d'un site en filtrant le trafic non désiré, il permet de filtrer les paquets venant du réseau public.

Le mode de fonctionnement de la plupart des pare-feux pose un problème pour l'établissement des communications SIP.

SIP, par son fonctionnement interne qui permet la localisation des utilisateurs au sein d'un réseau et la négociation des paramètres de la session (codecs, port RTP, etc.), pose des problèmes pour les flux multimédias qui traversent les firewalls. En effet, dans l'architecture de SIP, plusieurs informations critiques telles que l'adresse IP ainsi que le port à utiliser sont contenues dans les messages SIP.

La problématique engendrée par l'utilisation de SIP au travers des pare-feux vient du fait que ceux-ci sont généralement déployés en utilisant des politiques de filtrage qui rejettent tous les paquets qui ne proviennent pas ou qui ne sont pas destinés à une adresse IP et un port définis. Ces politiques, qui sont généralement statiques, ne permettent pas la traversée d'un flux de données à des protocoles comme SIP qui peut négocier des adresses IP et des numéros du port inconnus par le pare-feu lors de l'établissement de session.

Afin de bien comprendre la problématique engendrée par les pare-feux pour les flux multimédias, voici le schéma d'un scénario d'établissement de session et comment le firewall bloque le contenu multimédia.

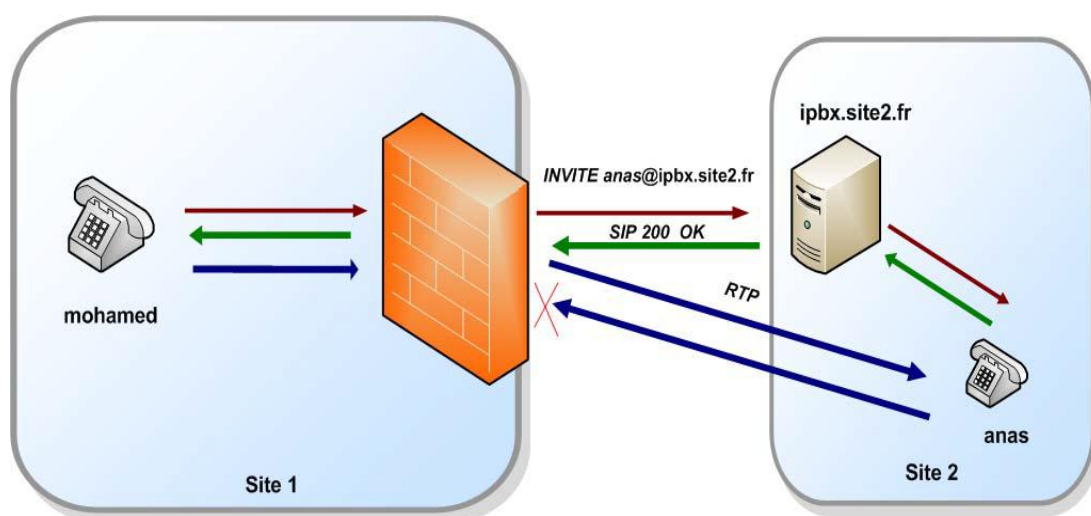


Figure 24 : scénario d'établissement de session avec blocage de contenu multimédia par firewall

Dans cet exemple, l'utilisateur SIP mohamed@poste.site.fr invite l'utilisateur anas@ipbx.site2.fr afin d'ouvrir une session. Mohamed envoie donc une requête d'invitation INVITE contenant les informations de la session à ouvrir à Anas. Anas répond avec le message 200 OK contenant des informations supplémentaires sur la session à ouvrir.

Comme on peut le constater, l'adresse ainsi que le port à utiliser lors de l'ouverture de la session audio sont contenus dans le corps des messages INVITE et OK. Ces deux informations servent à l'établissement du flux audio entre Mohamed et Anas. Dans notre exemple, Mohamed et Anas utilisent respectivement les ports 3456 et 5004. Par conséquent, comme le firewall a des règles de filtrage strictes et statiques, le contenu multimédia d'Anas sera donc tout simplement bloqué par le firewall.

```

INVITE sip:anas@195.98.238.13 SIP/2.0
Via: SIP/2.0/UDP 194.214.126.10:5060
From: <sip:mohamed@194.214.126.10>
To: <sip:anas@195.98.238.13>
Contact: <sip:mohamed@194.214.126.10>
Call-ID: e44be05d33f0eb557@194.214.126.10
CSeq: 102 INVITE
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 345

v=0
o=root 4033 4033 IN IP4 194.214.126.10
s=session
c=IN IP4 194.214.126.10
b=CT:384
t=0 0
m=audio 3456 AVP 8 0 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000

SIP/2.0 200 OK
Via: SIP/2.0/UDP 194.214.126.10:5060
From: <sip:mohamed@194.214.126.10>;
To: <sip:anas@195.98.238.13>;
Call-ID: e44be05d33f0eb557@194.214.126.10
CSeq: 102 INVITE
Contact: <sip:anas@194.214.218.130:5060>
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 305

v=0
o=CiscoSystemsSIP 9397 IN IP4 194.214.218.130
s=SIP Call
c=IN IP4 194.214.218.130
t=0 0
m=audio 5004 RTP/AVP 0 101
c=IN IP4 194.214.218.130
a=rtpmap:0 PCMU/8000

```

Figure 25 : Fonctionnement du firewall

IV-Solutions de traversées des NAT et des pare-feux

Afin de faire face aux problèmes que posent les pare-feux et les NAT, plusieurs solutions ont été proposées notamment ALG, STUN et ICE.

Le tableau qui suit résume les principes, avantages et inconvénient des solutions présentées :

solution	principe	Avantages	Inconvénients
ALG	Firewall et routeur NAT « Intelligents » capables de travailler au niveau 7	Technique simple	- Temps de latence importants dus au traitement complet et individuel des paquets.
STUN	Détermine le couple (adresses, ports) publics qu'on doit utiliser dans le paquet SIP pour obtenir une réponse	- Protocole standardisé. - Peu d'infrastructure : seul 1 serveur doit être déployé pour effectuer les requêtes.	- il ne fonctionne pas avec les NATs symétriques
TURN	- Basé sur STUN pour l'échange de clés - Le serveur TURN sert de relais entre l'émetteur et le récepteur	- Technique simple	- Modification des programmes nécessaire pour qu'ils puissent intégrer TURN
ICE	- intègre STUN et TURN au sein des clients SIP pour déterminer toutes les connexions possibles entre deux postes.	Traverse tous types de NAT	- Temps d'établissement d'un appel long. - Modification des serveurs et clients

Tableau 4 : Récapitulatif des avantages et inconvénients des solutions

V-ToIP et la sécurité des communications voix

La téléphonie sur IP, malgré ses très nombreux avantages, notamment financiers, comporte des risques majeurs en termes de sécurité des communications voix.

1-Vulnérabilités de la ToIP

Un appel téléphonique ToIP se décompose en deux phases : la signalisation qui permet d'établir l'appel, et la phase de transport des flux de medias qui transportent la voix.

Au cours de la phase de signalisation, les messages SIP codés en mode texte sont transmis de façon non chiffrée dans le réseau, ce qui permet à un pirate d'écouter facilement les messages SIP et d'accéder aux informations de transport des flux média.

En outre durant le transport des flux voix, le protocole RTP présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrement. Par voie de conséquence, plusieurs attaques ToIP peuvent avoir lieu.

Exemples d'attaques sur l'infrastructure ToIP

Il existe de nombreuses attaques possibles sur le réseau ToIP dont les plus répandues sont :

- Dénis de service (attaque DoS) : l'objectif d'une attaque DoS est de rendre un élément du réseau indisponible. Un exemple de ce type d'attaque est l'envoi illégitime de paquets SIP BYE.
- Ecoute clandestine : L'objectif de cette attaque est d'écouter le trafic de signalisation et/ ou de données, en utilisant des outils d'écoute réseau tels que VOMIT (Voice Over Misconfigured Internet Telephone), SiVus (SIP Vulnerability Scanner), et wireShark.
- Détournement du trafic : l'attaquant redirige à son profit le trafic ToIP. Elle se base sur l'envoi d'un message de redirection indiquant que l'appelé s'est déplacé et donne sa propre adresse comme adresse de renvoi, de cette façon tous les appels destinés à l'utilisateur sont transférés à l'attaquant.
- Usurpation d'identité : Ce type d'attaque consiste à usurper l'identité de l'expéditeur du message SIP en modifiant l'identité de l'expéditeur d'un message.
- Vols de services : le pirate peut emprunter l'identité d'un utilisateur et l'utiliser pour faire passer des appels sur le réseau ToIP sans avoir payer le fournisseur de service.

2-Solutions de sécurité de la ToIP

Les mécanismes de sécurité proposés dans une architecture ToIP sont :

- La sécurité de l'infrastructure IP : c'est le premier niveau de sécurité, car la sécurité de l'infrastructure ToIP est liée à la sécurité du réseau IP. Un exemple est la séparation logique des réseaux Data et Voix par des VLANs.
- L'authentification : L'authentification du téléphone IP par le serveur et l'authentification du serveur par le téléphone IP avant d'autoriser un quelconque appel. Il existe différents moyens d'authentification tels que : SIPS, IPsec.
 - SIPS (Session Initiation Protocol Secure) : est un mécanisme de sécurité défini par RFC 3261 pour l'envoi de messages SIP au-dessus du protocole de sécurisation TLS (Transport Layer Security).
 - IPsec (Internet Protocol Security) : est un ensemble de protocoles (couche 3 du modèle OSI) défini par IETF (RFC 2401), permettant le transport sécurisé des données sur un réseau IP [6].
- Le chiffrement : c'est un moyen efficace de protéger les données. Plusieurs solutions peuvent être utilisées : le chiffrement des flux de signalisation avec SIPS, le chiffrement des flux voix SRTP, des solutions propriétaires.
 - ✓ SRTP (Secure Real-time Transport Protocol) : définit un profil de RTP, qui a pour but d'apporter le chiffrement, l'authentification et l'intégrité des messages, et la protection contre le replay de données RTP en unicast et multicast. SRTP a été conçu par Cisco et Ericsson, et est ratifiés par l'IETF en tant que RFC 3711. [6]

3- La ToIP et IPv6

IPv6 est le protocole Internet de nouvelle génération conçu par l'IETF. Il permet principalement de disposer d'un plus grand nombre d'adresses pour chaque élément du réseau. Il offre également une plus grande facilité de configuration et améliore les mécanismes de gestion de la mobilité IP. Il intègre nativement la sécurité, les classes de service et la diffusion multicast.

Le déploiement du protocole IPv6 pour le support de la ToIP va permettre d'éviter d'avoir recours aux NATs grâce à sa grande capacité d'adressage et de simplifier ainsi l'architecture. Néanmoins, la mise en place de la ToIP en IPv6 n'est pas encore répandue parce que la plupart des équipements de ToIP ne supportent pas encore cette version du protocole IP. Voici des exemples de solutions ToIP qui supportent IPv6 : Kamailio (routeur d'appels), Linphone et SJPhone (qui sont des « softphones », applications logicielles à installer sur un ordinateur).

VI-Asterisk

Définition

Asterisk est un PABX logiciel libre, multi plateforme, publié sous licence GPL. Asterisk permet, entre autres, la messagerie vocale, la conférence, les serveurs vocaux, la distribution des appels.

Asterisk implémente les protocoles H.323 et SIP, ainsi qu'un protocole spécifique nommé IAX. Il permet la communication entre client et serveur Asterisk ainsi qu'entre deux serveurs. [1]

Serveur Asterisk site officiel : <http://www.asterisk.org>

1-Historique

Le PBX open source Asterisk a vu le jour quand Mark Spencer, a voulu acquérir un PBX traditionnel pour sa société. Le créateur d'Asterisk, trouvant que le prix d'acquisition d'un PBX traditionnel était démesuré, initia un projet open source. Il a donc commencé à développer Asterisk. [1]

Remarque :

Il faut savoir que le prix d'un petit PABX (100 postes) est de 3000 euros. Son équipe s'est rapidement rapprochée de celle de Jim Dixon (Zapata Telephony Project), dans le but de construire des cartes d'interface "bon marché" avec le réseau téléphonique classique. Leur but était de construire des cartes compatibles avec des plateformes basées sur Intel et ainsi de permettre à n'importe quel PC, avec le système d'exploitation Linux, une carte d'interface et le logiciel Asterisk d'avoir un PBX entièrement fonctionnel.

Pour info :

Le nom Asterisk fait référence au symbole "*" qui signifie "wildcard" en ligne de commande Unix et DOS. Ce choix a été fait car Asterisk est conçu dans le but d'offrir une très grande souplesse dans des réseaux de voix. [1]

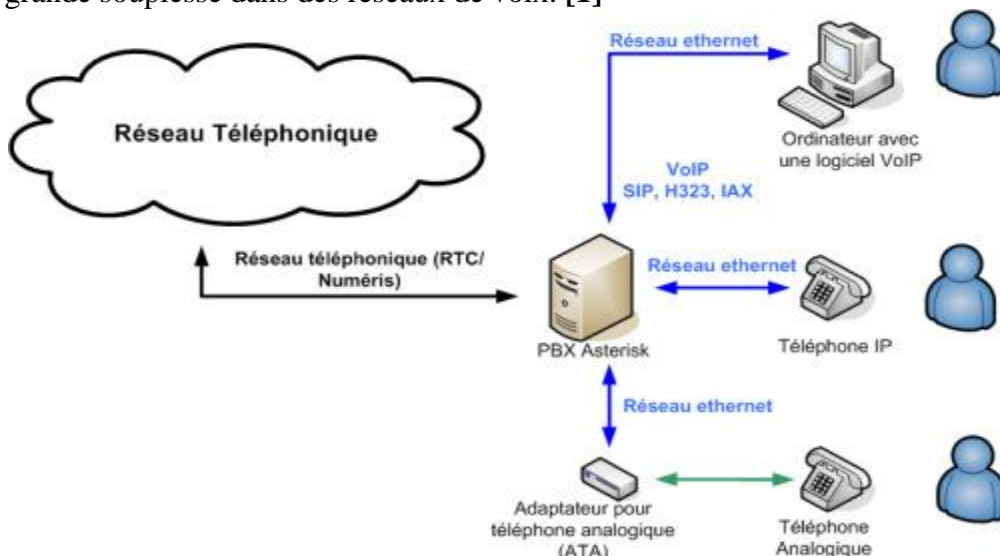


Figure 26 : Mode de fonctionnement d'un PABX

2-Fonctionnalités :

Asterisk offre les fonctionnalités suivantes :

- Messagerie vocale
- Conférence téléphonique
- Répondeur vocal interactif
- Mise en attente d'appels
- Services d'identification de l'appelant
- VoIP etc.....

3-De la téléphonie à moindre coût :

Dans l'interconnexion avec les équipements de téléphonie numériques et analogiques, Asterisk reconnaît une large gamme de dispositifs matériels, et notamment ceux fabriqués par ses sponsors, tels que Digium ou encore Quick net. [1]

4-Une particularité modulaire :

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. [1]

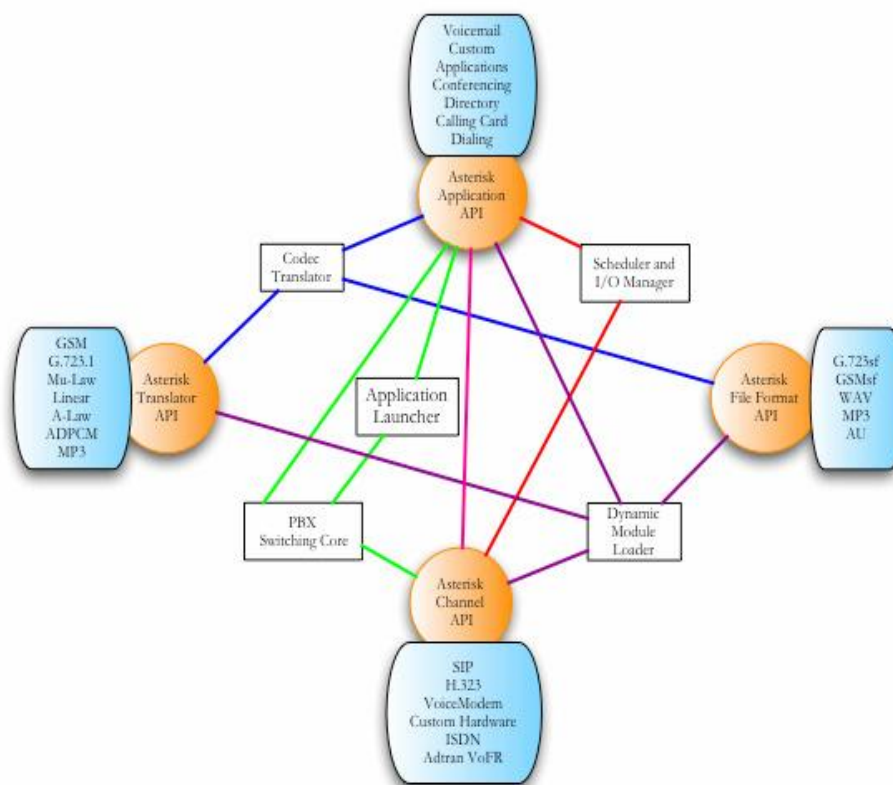


Figure 27 : Architecture détaillée d'Asterisk

5-Principales fonctions:

a-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.

b-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).

c-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. [1]

d-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. [1]

6-Les APIs :

a-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. [1]

b-Asterisk Translator API:

Charge les modules de codec pour supporter divers formats de codage et de décodage audio tels que le GSM, la Mu-Law, l'A-Law, et même le MP3. [1]

c-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. [1]

d-Asterisk File Format API:

Elle permet la lecture et l'écriture de divers formats de fichiers pour le stockage de données dans le file system. 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. [1]

La capacité de charger des modules de codec permet à Asterisk d'être compatible avec le codec extrêmement compact nécessaire à la Voix sur IP sur des connexions lentes comme un modem téléphonique tout en maintenant une haute qualité audio sur des types de connexion moins "étroites". [1]

7-Fonctionnement évolué :

Asterisk ne permet pas seulement l'utilisation d'équipements traditionnels de téléphonie, il augmente aussi en nombre leurs capacités. En utilisant le protocole de voix sur IP Inter-Asterix eXchange (IAX ou inter central Asterisk), Asterisk mêle progressivement la voix et le trafic de données à travers des réseaux disparates. [1]

Tant que l'on transporte la voix par paquets, il est possible d'envoyer des données telles que des documents URL et des images, en conformité avec le trafic Voix, permettant ainsi une intégration plus grande des informations.

8- Choix d'Asterisk pour notre projet

Le choix d'une solution de téléphonie d'entreprise n'est pas facile car les arguments des uns s'opposent à ceux des autres. Les solutions propriétaires sont chères, de plus les constructeurs proposent des modèles fermés, rigides, peu évolutifs, et surtout limités en termes de fonctionnalités.

C'est pourquoi aujourd'hui, le meilleur choix c'est l'Open Source car elle est gratuite, elle ne cesse chaque jour de s'améliorer, elle offre à ses utilisateurs des fonctionnalités exceptionnelles, elle s'adapte aux besoins, elle est évolutive, elle permet une intégration avec d'autres systèmes.

Par défaut, l'installation du serveur Asterisk, sous linux ou autres distributions de linux, donne automatiquement droit à une interface graphique appelée FreePBX. Elle est obtenue à travers un navigateur (Mozilla, Internet Explorer, Google chrome, etc....)

Conclusion

La téléphonie sur IP est une technologie qui utilise les réseaux informatiques comme support de communication. Les solutions ToIP sont de plus en plus basées sur des standards ouverts. Beaucoup de ces solutions utilisent SIP comme protocole de signalisation ToIP. Les principaux protocoles utilisés pour le transport de la voix sont : RTP et RTCP. Et pour garantir la compatibilité entre la ToIP et le réseau téléphonique classique, l'IETF a travaillé sur le standard ENUM.

Le déploiement de la technologie ToIP dans les réseaux actuels a provoqué l'apparition des nouvelles problématiques notamment au niveau des dispositifs de sécurité tels que les pare-feu et les routeurs NAT, ainsi que les vulnérabilités de ToIP en termes de sécurité. Les problèmes de NAT et de pare-feux ont été solutionnés en utilisant plusieurs techniques qui sont résumées dans le tableau 2, tandis que de nombreux mécanismes de sécurité ont été présentés notamment la sécurité de l'infrastructure IP, l'authentification, et le chiffrement.

Notre but est d'administrer le serveur Asterisk en créant une interface graphique, plus simple et plus facile à manipuler pour toute personne quelle soit informaticien ou pas. Cet objectif sera exposé, expliqué, et appliqué dans le chapitre 4 : Implémentation du serveur Asterisk.

Chapitre IV : Implémentation

I-Installation et configuration du serveur Asterisk

1-Installation du système d'exploitation

Notre serveur sera installé sur une machine virtuelle sous laquelle est installé un système d'exploitation Linux. La distribution choisie est ubuntu 12.4 qui est une version stable parmi tant d'autres. Nous allons dans ce qui suit détailler son téléchargement ainsi que son installation.

Pour cela il suffit juste de récupérer l'image iso ubuntu 12.4 stable à cette adresse <http://www.ubuntu.org/cd/http-ftp/>, un fichier de 705 536 Ko, de la graver sur un CD au cas où on voudrait utiliser un ordinateur réel, ou alors passer à l'installation directement à partir de la machine virtuelle, jusqu'à l'étape Sélection de logiciels.

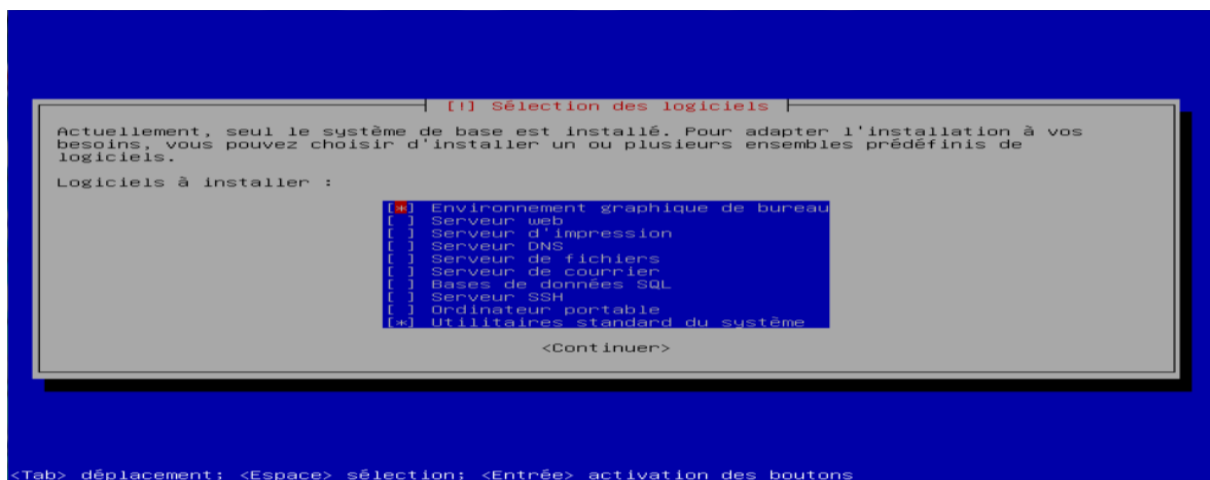


Figure 28 : sélection de logiciels à installer

Une fois l'installation terminée, l'ordinateur redémarre, on se log en root, afin d'installer tous les autres paquets dont nous aurons besoin si ça en vaut la peine.

2-Installation du serveur Asterisk

Avant de passer au téléchargement du serveur Asterisk, certains paquets doivent préalablement être installés :

```
root@ubuntu:~#apt-get install glibc-source
root@ubuntu:~#apt-get install ncurses-dev
root@ubuntu:~#apt-get install zlib1g-dev
root@ubuntu:~#apt-get install build-essential
```

Maintenant nous pouvons passer au téléchargement et à l'installation de notre serveur grâce aux deux commandes suivantes :

```
root@ubuntu :~# apt-get update : pour mettre à jour le système d'exploitation.
root@ubuntu:~# apt-get install asterisk: pour télécharger et installer Asterisk.
```


➤ Contextes & Comptes utilisateurs :

-Administration pour tout le personnel Universitaire sauf les étudiants (Doyen, Secrétariat, Professeurs)

-Labo pour tous les labos existant dans l'université

4-Configuration basique du serveur Asterisk

Tous les fichiers de configuration du serveur se trouvent dans **/etc/asterisk/**. On y accède à l'aide de la commande suivante :

```
root@debian:~#cd /etc/asterisk/
```

Pour qu'Asterisk fonctionne de manière basique, il est nécessaire de modifier seulement deux fichiers de configuration: **sip.conf** et **extensions.conf**.

C'est dans le fichier **sip.conf** que l'on déclare les comptes utilisateurs de la manière suivante (ceci se fait tout en bas du fichier lorsqu'il est ouvert, Nous en déclarerons trois) :

```
[generale]
Context=administration ; contexte pour le personnel de la université
Context=labo ; contexte pour tous les labos
Language=fr ; langue d'accueil du serveur
Videosupport=yes ; active la vidéoconférence

[doyen] ; nom d'utilisateur
type=friend ; signifie que le client peut recevoir et passer des appels
username=doyen ; login
secret=doyen ; mot de passe
host=dynamic ; le client peut se connecter depuis n'importe quelle adresse IP
context=administration ; contexte auquel le compte est associé
disallow=all ; désactivation de tous les codecs
allow=gsm, ulaw, alaw ; puis on les active l'un après l'autre
language=fr ; définit la langue d'accueil

[secretaire1]
type=peer ; signifie que le client peut recevoir des appels uniquement
username=secretaire1
secret=secretaire1
host=dynamic
context=administration
disallow=all
allow=gsm, ulaw, alaw
language=fr
```

```
[labo1]
type=friend                ; signifie que le client peut recevoir des appels uniquement
username=labo1
secret=labo1
host=dynamic
context=labo
disallow=all
allow=gsm, ulaw, alaw
language=fr
```

Ensuite, nous allons créer le dialplan dans **extensions.conf** pour les utilisateurs créés dans le fichier **sip.conf**, (idem pour celui-ci la création de fait tout en bas du fichier)

```
[administration]          ; contexte utilisateur
exten => 321,1, Dial (SIP/doyen) ; si on compose le numéro 321, le doyen sera appelé
exten => 321, 2, Hangup ()      ; coupe l'appel
exten=>322, 1, Dial (SIP/secretaire) ; si on compose le numéro 322, la secretaire sera appelé
exten => 322, 2, Hangup ()

[labo]                      ; contexte utilisateur
exten => 323, 1, Dial (SIP/lab01) ; compose le numéro 323, le labo1 sera appelé
exten => 323, 2, Hangup ()
```

Pour que le serveur Asterisk prenne en considération toutes ces modifications, on se logue sur sa console avec :

```
root@ubuntu# asterisk -r
```

Puis on recharge Asterisk avec :

```
ubuntu*CLI>reload
```

Cette commande recharge le fichier sip

```
ubuntu*CLI>sipreload
```

La commande suivante permet de recharger uniquement le dialplan (extensions.conf)

```
ubuntu*CLI>dialplanreload
```

Par défaut seul les utilisateurs de même contexte peuvent s'appeler. Pour que les utilisateurs de contextes différents puissent s'appeler, on insère dans leurs contextes dans le fichier extensions.conf la ligne **include => contexte**

Par exemple si on veut que l'etudiant1 appelle l'enseignant1, on modifie le fichier extensions comme suit :


```
[administration]
include =>labo
exten => 321,1, Dial (SIP/doyen)
exten => 321, 2, Hangup ()
exten => 322, 1, Dial (SIP/secretaire)
exten => 322, 2, Hangup ()

[labo]
include =>administration
exten => 323, 1, Dial (SIP/lab01)
exten => 323, 2, Hangup ()
```

5-Configuration avancée du serveur Asterisk

Que se soit le **Transfert d'appel, la mise en attente**, il existe des commandes intégrées dans le serveur Asterisk permettant de les configurer mais vu que nous utilisons aussi des softphones ayant eux aussi des touches préconfigurées pour ses fonctions, cela va de soit de ne pas se compliquer encore la vie.

Pour la **messagerie vocale**, nous avons été obligés de le configurer pour permettre à notre serveur d'être si on peut le dire pleinement fonctionnel. Et permettrai en même temps à toute personne injoignable, ou occupé d ne pas perdre toutes informations aussi futiles soit elle.

Nous commençons par la création de la boîte vocale mère qui sera partagée par tous les utilisateurs. Nous l'appellerons 2013@default. Dans le fichier voicemail.conf, section [general], on ajoute la ligne suivante :

```
mailbox = 2013@default
```

Nous allons ensuite créer trois boites vocales correspondant aux trois utilisateurs doyen, secretaire et labo1 créés dans le fichier sip.conf. Le fichier **voicemail.conf** va être configuré à cet effet. Au bout de ce fichier on ajoute les lignes suivantes :

```
[default]
400 => 10,doyen,doyen@yahoo.fr
401 => 11,secretaire,secretaire@yahoo.fr
402=> 12, labo1, labo1@yahoo.fr
```

Le 400 est le numéro associé la boîte vocale de l'utilisateur doyen. Le 10 est le mot de passe d'accès à sa messagerie. Suivant le nom de l'utilisateur, ainsi que son mail. Il en est de même pour toutes les autres boîtes. Le mail servira à l'alerter en cas de réception de message vocal. Les boîtes vocales sont maintenant déclarées, on ajoute dans le fichier sip.conf cette

ligne mailbox = numéro_utilisateur@default pour chaque compte. Il faut ensuite modifier ensuite le fichier extensions.conf comme suit :

Lorsque l'on compose le 321 le doyen est appelé, le 10 est le timeout avant de passer à la deuxième séquence. Une fois le timeout atteint, on bascule sur la deuxième séquence qui est l'appel de sa boîte vocale avec la fonction **Voicemail ()**. Enfin, on raccroche avec la fonction **Hangup ()**. Il en est de même pour tous les utilisateurs.

```
[doyen]
include => labo
exten=>321,1, Dial (SIP/doyen, 10, rtT)
exten => 321, 2, voicemail (400, u)
exten => 321, 3, Hangup ()
```

Chaque utilisateur aura besoin d'un numéro lui permettant d'accéder à la messagerie vocale une fois que le message vocale lui sera notifié (généralement par une petite enveloppe qui apparaît à l'écran du Softphone ou alors par une sonnerie personnalisée). Dans notre cas nous attribuons un même numéro d'accès à la boîte vocale (**2013@default**) pour tous les utilisateurs du même contexte (d'autres règles existent). L'utilisateur sera identifié par le numéro de sa boîte et son mot de passe qui lui sont demandés par le serveur.

Pour définir le numéro d'accès à la boîte vocale, on fait appel à la fonction **voicemailmain ()** comme suit (pour le contexte doyen par exemple) :

```
[doyen]
include => labo
exten => 321,1, Dial (SIP/doyen, 10, rtT)
exten => 321,2, voicemail(400,u)
exten => 321,3, Hangup ()
exten => 602,1, Answer()
exten => 602,2, VoicemailMain(2013@default)
exten => 602,3, Hangup()
```

C'est le 602 qui sera composé pour accéder à la messagerie vocale. Une fois identifié, l'utilisateur n'aura qu'à suivre un menu interactif vocal qui lui permettra de réaliser toutes les opérations en rapport avec la messagerie vocale.

6-Asterisk en temps réel avec MySQL

Comme nous venons de le voir, pour que toute modification de sip.conf ou extensions.conf soit prise en compte, il est nécessaire de recharger le serveur Asterisk. Si on a un vrai besoin d'une prise en compte en temps réel et d'une plus grande souplesse dans la configuration, la migrer vers MySQL peut être extrêmement intéressant.

On peut en fait se servir de tables au lieu de fichiers de configuration. Lorsque nous modifierons ces tables, celles-ci seront prises en compte instantanément, sans avoir besoin de recharger le serveur.

a-La base de données Real-time :

L'architecture Real-time d'Asterisk ARA (Asterisk Real-time Architecture), apparue avec la version 1.2, permet de stocker des informations diverses dans une base de données de type SQL, cela peut être les informations des fichiers sip.conf, extensions.conf, voice-mail.conf.

La possibilité d'externaliser ce genre d'informations permet de disposer :

- ❖ D'une meilleure mise à jour et d'une meilleure lisibilité des données ;
- ❖ D'éviter de re-loader une configuration statique en cas de chargement ;
- ❖ D'externaliser la base sur un serveur dédié, différent du serveur Asterisk.

Pour mener à bien notre travail, nous créons une base de données de tous les utilisateurs dans un premier temps, indiquerons nous par la suite au serveur Asterisk, à travers certains de ses fichiers, qu'il faudra aller chercher les utilisateurs au niveau du serveur MySQL.

Cela nous permettra plus tard de créer une application conviviale pour l'administration de notre serveur. Toutes les configurations faites jusqu'ici sont à oublier. Nous supposons que le serveur Asterisk n'a pas encore été configuré.

b-Création et configuration de Real-time avec une base de données MySQL

Il faut au préalable avoir installé tous les paquets MySQL (voir les étapes précédentes). L'accès à la base faire à l'aide d'un outil de type phpMyadmin (<http://www.phpMyadmin.net>) permettant de disposer d'une interface web : ajout, suppression, modification, interrogation. Le package asterisk-addons doit être installé (<http://www.asterisk.org/>).

Après l'installation du serveur MySQL et de phpMyadmin, nous utiliserons l'interface web de ce dernier pour créer notre base de données nommée 'Asterisk' dans MySQL. Nous procédons ensuite à la création de tables pour notre base dont le MCD (Modèle Conceptuel de Données) ci-dessous :

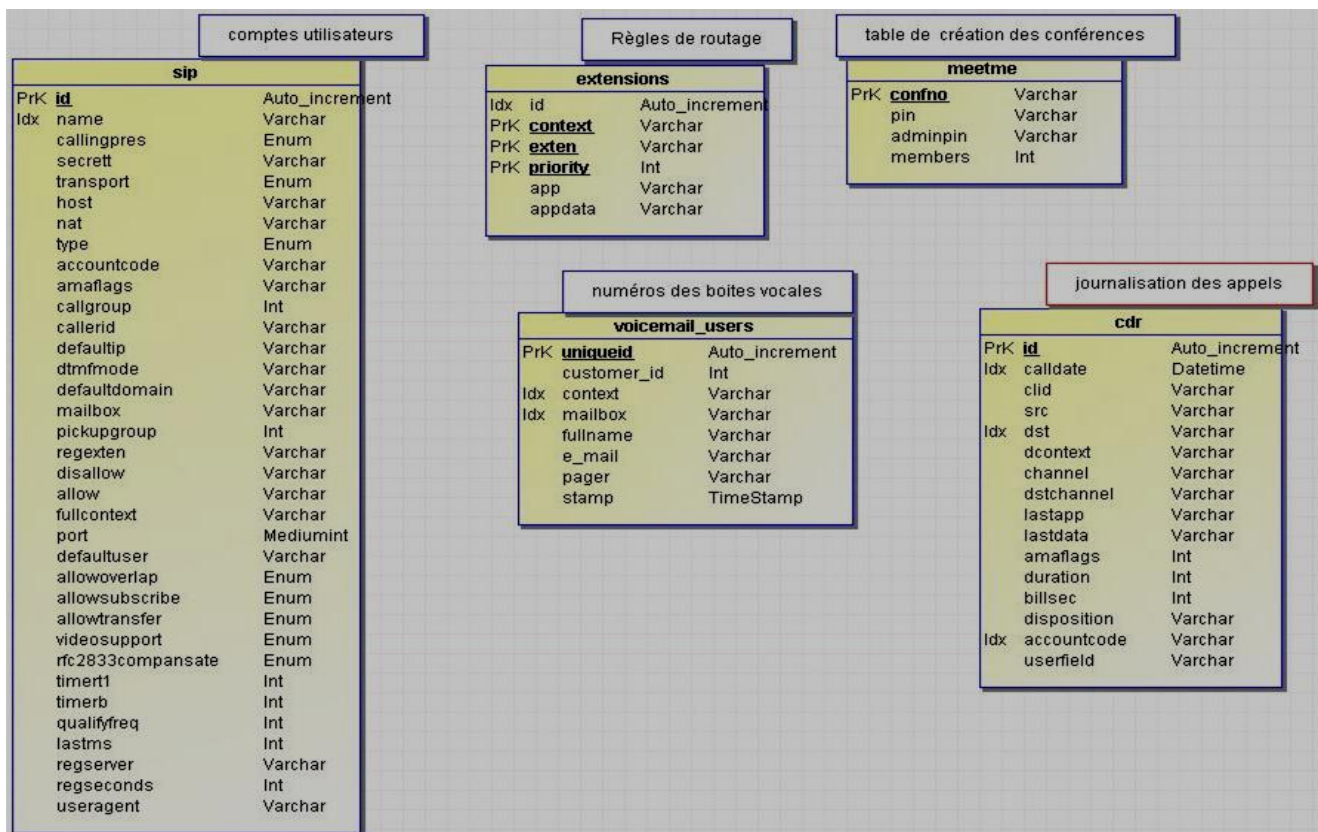


Figure 30: MCD de la base de données

Ensuite, nous devons maintenant configurer le serveur Asterisk pour qu'il puisse s'y connecter. De ce fait la configuration de trois fichiers est nécessaire pour la cohabitation des deux serveurs. Il s'agit de :

- ❖ **res_mysql.conf** : ce fichier se trouve à l'emplacement '**etc/asterisk/res_mysql.conf**'.

Il contient les paramètres pour se connecter à la base : adresse du serveur, nom de la base realtime, numéro du port, nom de l'utilisateur de la base, mot de passe de l'utilisateur de la base.

```
[general]
dbhost = 127.0.0.1          ; serveur mysql si c'est local
dbname = asterisk          ; nom de la base de donnée
dbuser = nom_d'utilisateur ; nom d'utilisateur
dbpass = mot_de_pass       ; mot de passe utilisateur
dbport = 3306              ; port mysql
dbsock = /var/run/mysql/mysql.sock
```

- ❖ **extconfig.conf**: permet de modifier la façon dont Asterisk cherche les fichiers de configuration (statique ou temps réel). Nous le configurons en mode temps réel dans la section [settings] comme suit :

```
[settings]
sipusers =>mysql, general, sip; fait référence la table sip
sippeers =>mysql, general, sip; fait référence la table sip
extensions =>mysql, general, extensions; fait référence à la table extensions
voicemail =>mysql, general, voicemail_users; fait référence à la table voicemail_users
```

- ❖ **cdr_mysql.conf** : fournit automatiquement à MySQL l'état du serveur Asterisk en remplissant la table **cdr**.

```
[global]
hostname=127.0.0.1
dbname=asterisk
table=cdr
password=mot_de_pass
user=nom_d_utilisateur
port=3306
sock=/var/run/mysqld/mysqld.sock
```

- ❖ **extensions.conf** : Tous les contextes doivent être déclarés dans ce fichier et il faut indiquer quel contexte peut appeler l'autre à l'aide du mot clé **include=>contexte**.

Certaines informations peuvent rester dans ce fichier. Il s'agit des informations qui ne sont pas mises à jour fréquemment :

```
[administration]
switch =>Realtime      : redirige Asterisk vers MySQL
include =>parkedcalls  : active la mise en attente
include =>appel_groupe : active les appels inter-contextes
include =>labo
```

Les autres fichiers restent tels qu'ils ont été configurés avant MySQL.

7-Création d'une interface graphique pour l'administration du serveur Asterisk

A ce niveau nous disposons d'une base de données MySQL capable d'interagir avec notre serveur Asterisk, nous pouvons maintenant passer à la réalisation de notre application JAVA qui nous permettra d'effectuer facilement quelques-unes des opérations administratives à savoir ajout d'un utilisateur, suppression d'un utilisateur, recherche d'un utilisateur, modification d'un utilisateur, etc ...

Nous allons présenter le cadre général de notre projet, c'est-à-dire les différentes parties de l'exécution dont les captures d'écran sont ci-dessous :

Remarque : Initialement le serveur MySQL n'accepte que les connexions locales, alors pour que notre application puisse s'y connecter, nous allons accorder tous les droits à l'un des utilisateurs comme ci-dessous grâce à phpMyAdmin :

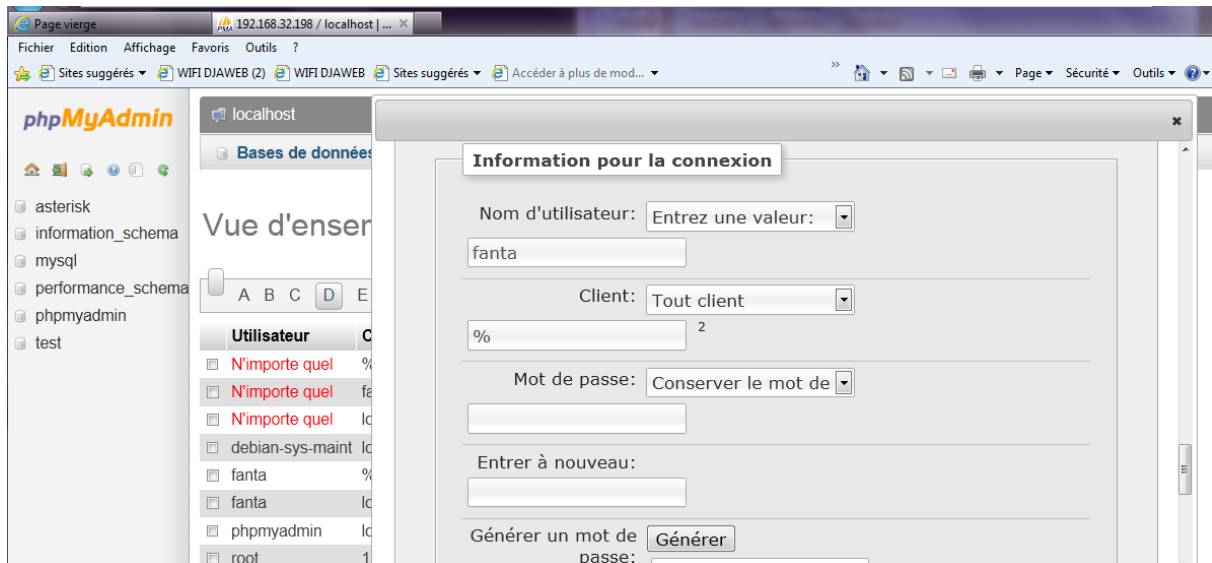


Figure 31: Ajout et configuration des droits d'accès d'un administrateur de base de données

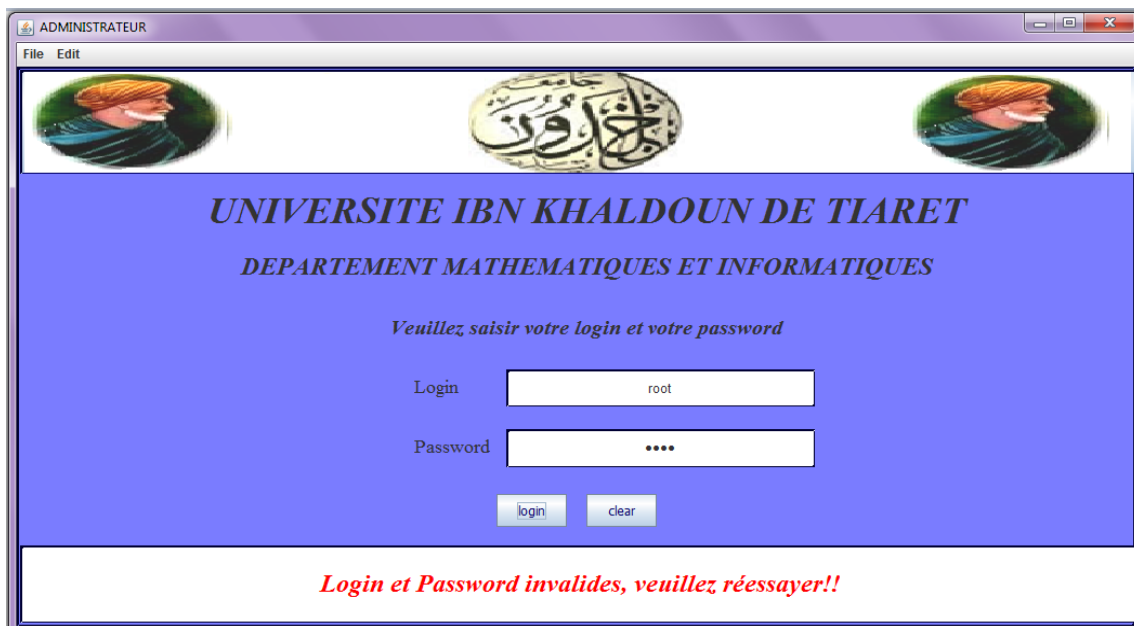


Figure 32: Identification Administrateur

La fenêtre ci-dessus permet à l'administrateur d'accéder à l'application. Si le 'Login' ou le 'Password' sont incorrectes un simple clic sur le bouton 'login' génère une erreur et le bouton 'clear' permet de revenir à l'état initial. Dans le cas contraire la page suivante s'affiche :



Figure 33: *accueil de de l'outil d'administration de notre seueur*

La fenêtre **Figure34** ci-dessous permet à l'administrateur de créer un nouvel utilisateur, lui attribuer son dialplan, ainsi que plusieurs fonctionnalités selon le grade qu'il occupe à l'aide du menu Asterisk.

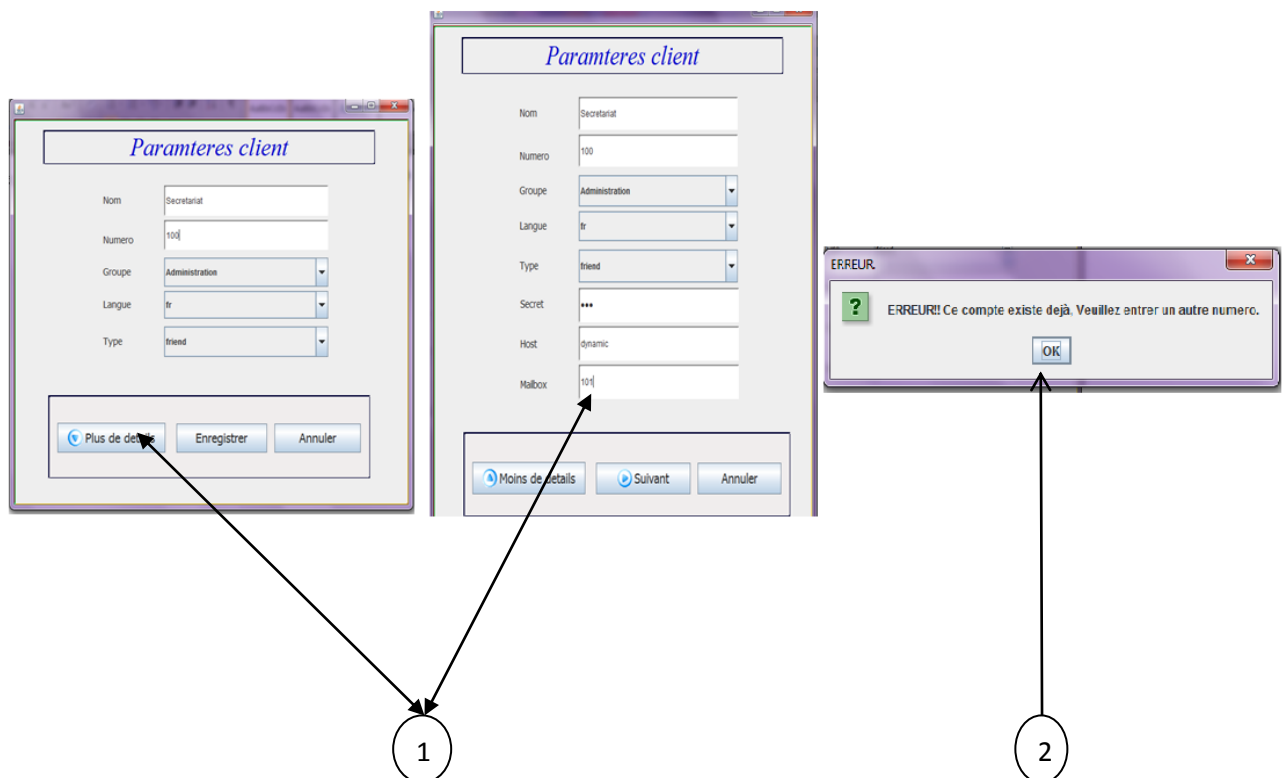


Figure 34: *Ajout d'un utilisateur*

En (1) , s'effectue l'insertion des paramètres nécessaires à la création d'un compte utilisateur. A cet niveau l'administrateur à le choix de créer soit un utilisateur sans ou avec boîte vocale. Si c'est le cas d'un compte sans boîte vocale un simple clic sur le bouton 'Enregistrer' permet de le créer dans la base de données. Si c'est d'un compte avec une boîte vocale,

l'administrateur doit cliquer sur le bouton 'Plus de détails' qui lui permettra d'accéder aux informations nécessaires à la création de la boîte vocale. Si le numéro utiliser existe déjà le (2) s'affiche.

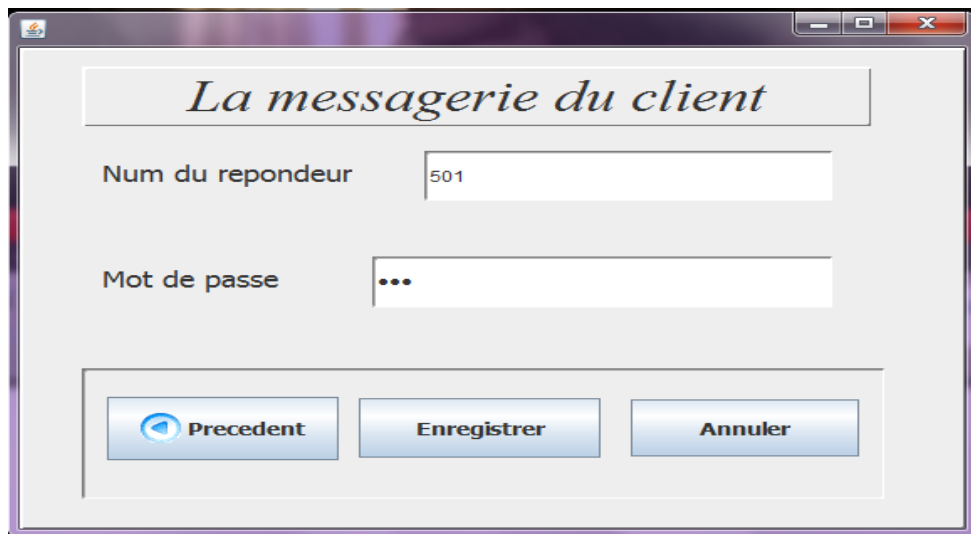


Figure 35: Ajout de la messagerie vocale

Un clic sur le bouton 'Suivant' permet d'afficher la fenêtre ci-dessus pour l'insertion du numéro et du mot de passe de la messagerie du client. Un clic sur le bouton 'Enregistrer' permet la sauvegarde des données dans la base de données.

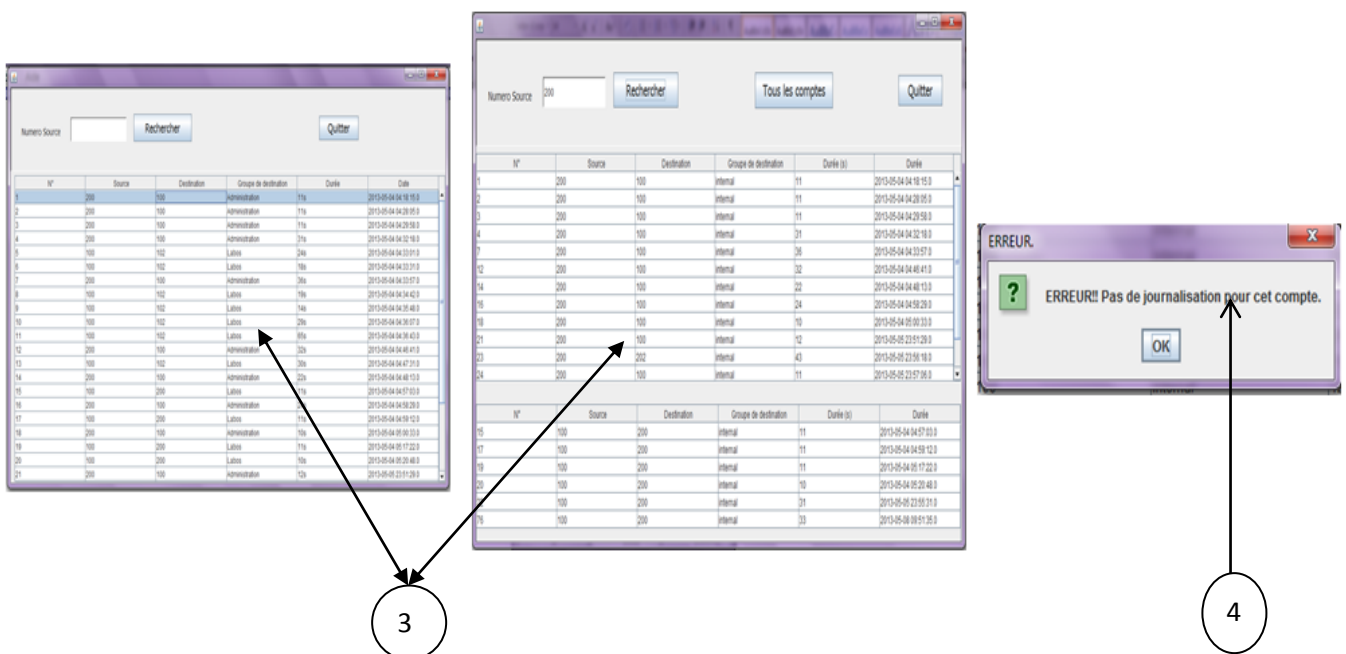


Figure 36: Rapport CDR (Call Detail Report)

Le (3) illustre l'affichage de tous les utilisateurs, et d'un utilisateur en particulier ayant passé des appels. Et le (4) est générer si l'utilisateur n'a pas passé d'appels.

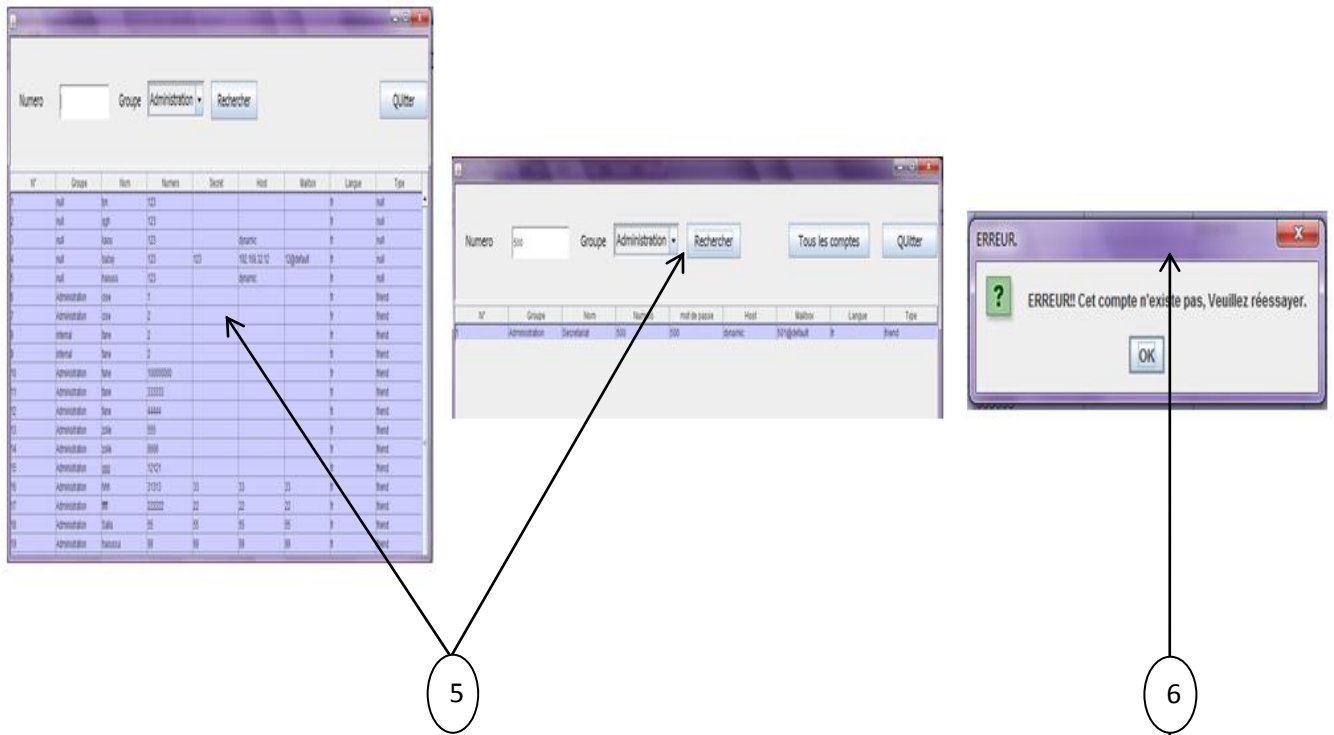


Figure 37: Recherche d'utilisateurs (numéro)

Le (5) illustre l'affichage de tous les utilisateurs, et d'un utilisateur en particulier grâce à son numéro téléphonique. Et le (6) est générer si le numéro entré n'existe pas.

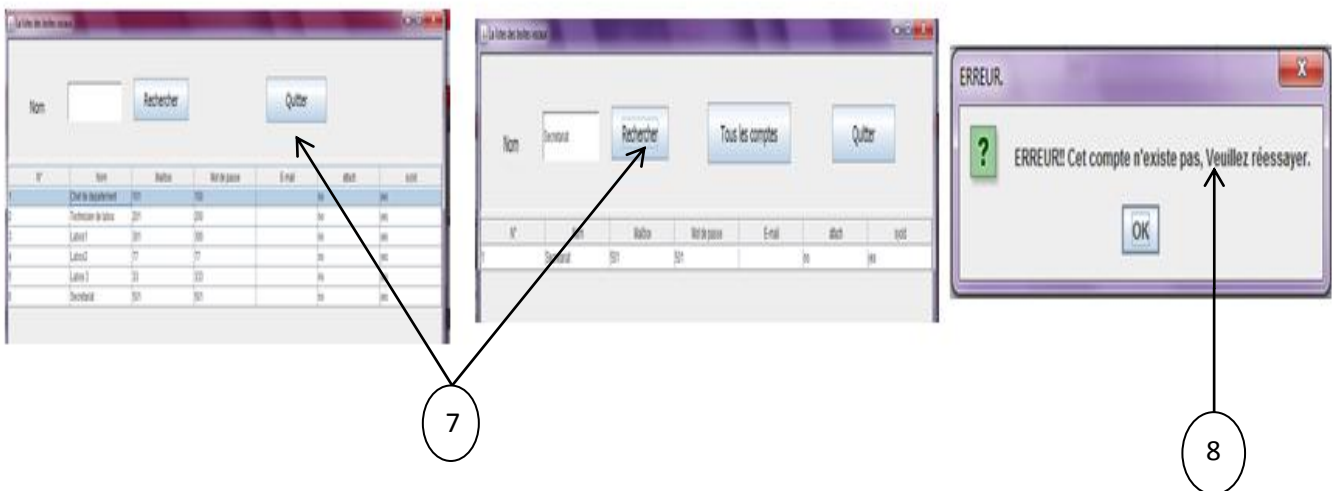


Figure 38: Recherche d'utilisateurs (Compte)

Le (7) illustre l'affichage de tous les utilisateurs, et d'un utilisateur en particulier grâce à son nom. Et le (6) est générer si le nom entré n'existe pas.

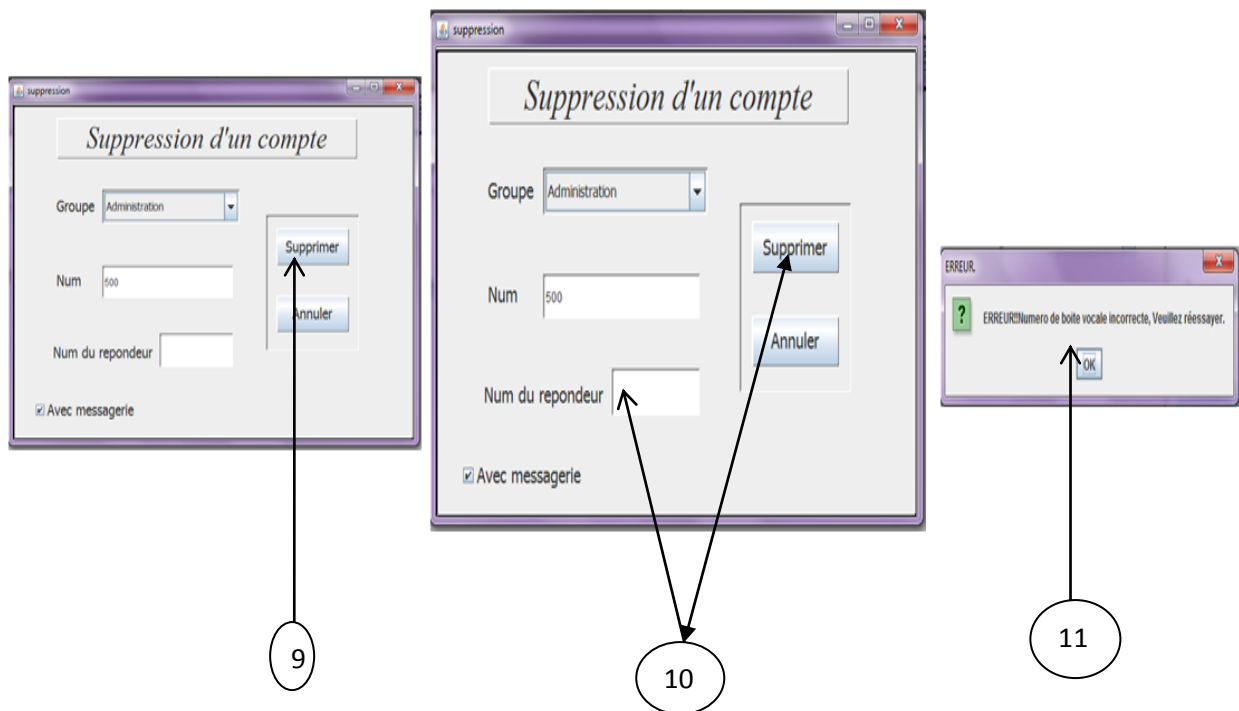


Figure 39: *suppression d'un compte*

Le (9) illustre une suppression d'un compte automatiquement si celui-ci n'a pas été configuré avec une messagerie vocale.

Le (10) illustre une suppression d'un compte avec sa messagerie vocale en y ajoutant bien sur le numéro de sa messagerie.

Le (11) apparait lorsque le numéro de la messagerie vocale n'est pas correct.

8-Test de fonctionnalités avec le client X-Lite

Définition

Le client SIP X-Lite permet de jouer le rôle d'un téléphone IP de manière logiciel. Il requière un système de son (carte son, baffles, micro,...) pour l'utiliser. Un tel client permet de remplacer des téléphones IP matériels onéreux.

a-Installation et configuration d'un client X-Lite

Son installation se fait comme toute application sous Windows. Il suffit de lancer l'exécutable et suivre les instructions en ne cliquant que sur suivant. Sa configuration se fait un simple clic droit sur l'interface *X-lite* -> *SIP Account Settings* puis *Add* et fournir les propriétés de la fenêtre SIP Accounts comme le montre les figures ci-dessous :

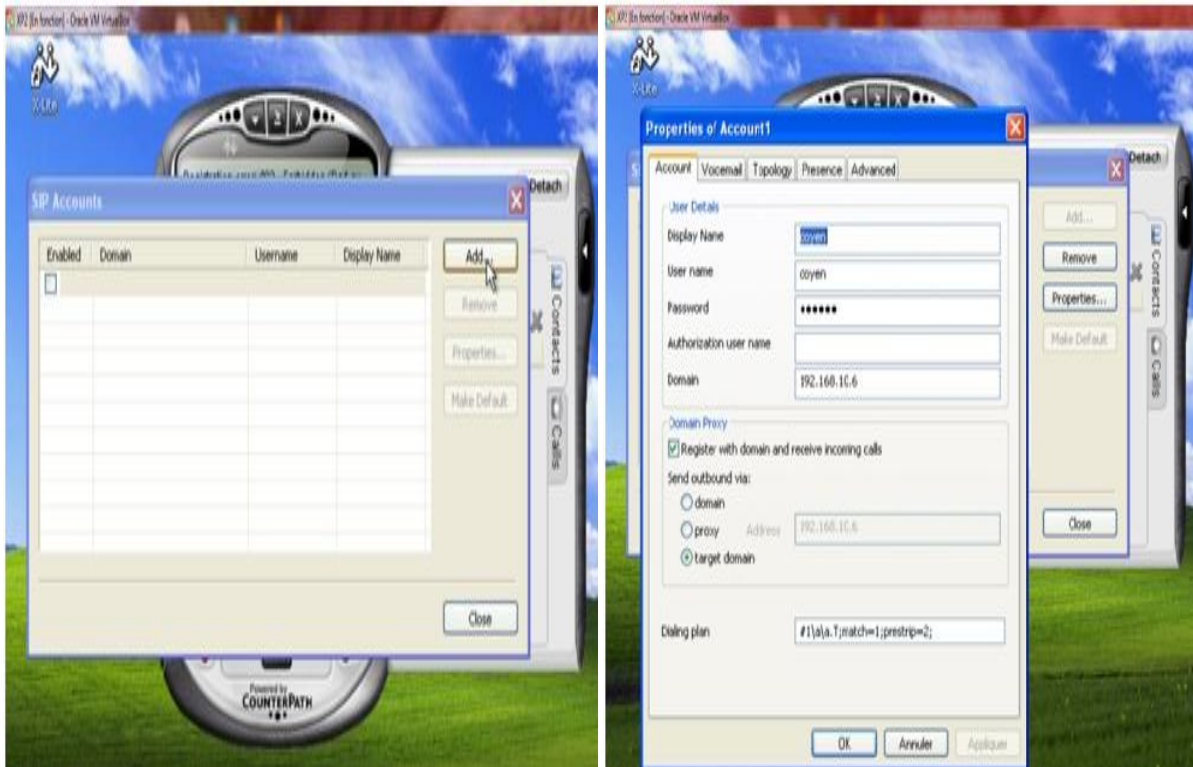


Figure 40: Ajout et configuration d'un client x-lite



Figure 41: Utilisateur connecté

La figure ci-dessus montre que l'utilisateur doyen est connecté au serveur Asterisk. A partir de là il peut appeler les autres postes connectés ou être appelé.

Conclusion

L'utilisation du serveur Asterisk en connivence avec le logiciel X-lite en entreprise ou au sein d'un institut est bénéfique.

Mais requiert, d'une connaissance assez ardue dans le domaine du réseau et des fichiers de configuration du dit serveur.

En outre une application basée sur des fichiers de configuration en ligne de commandes, est difficile à manipuler pour tous individus n'ayant pas connaissances en informatique et dans le domaine intitulé plus haut.

C'est pourquoi, il est préférable de l'accompagner d'une application, comme dans notre cas un logiciel permettant l'administration du serveur Asterisk. De manière à le rendre plus facile et plus conviviale à toutes personnes devant l'utiliser sans expériences acquises au préalable.

Conclusion Générale

Conclusion Générale

En conclusion, ce projet nous a permis de mettre en pratique nos connaissances théoriques acquises en cours de réseaux et de télécommunications.

Nous nous sommes initiés au travail collectif et avons acquis de multiples connaissances tant dans la conception d'un réseau VoIP, que dans les multiples fonctionnalités avancées d'un PABX logiciel. Nous avons de ce fait constaté que le logiciel libre Asterisk pouvait faire de l'ombre aux gros centraux téléphoniques.

Toutefois, la Voix sur IP pose de nombreux problèmes au niveau de sa régulation, ses modèles, sa mise en œuvre opérationnelle et son appropriation par le consommateur. La sécurité demeure au cœur de la problématique. En effet, une infrastructure VoIP a des exigences et des contraintes en matière de sécurité et de qualité de service très différentes du trafic de données traditionnelles. La transmission de la voix sur IP exige des délais de transit et une fluidité d'acheminement qui nécessite également d'adapter le réseau existant.

Notre projet avait pour objectif majeure d'administrer de manière simple et rapide un serveur Asterisk en le connectant avec un autre serveur de base de données nommé MySQL serveur, tout en réalisant un standard téléphonique VoIP utilisant des IPBX logiciels. Nous avons donc utilisé le serveur Asterisk pour la mise en place de notre solution VoIP et le Softphone X-Lite pour le test des différentes fonctionnalités implémentées. Asterisk est interopérable et compatible avec n'importe quel logiciel ou matériel. Cela nous a permis de n'avoir pas à nous soucier du client à utiliser. Le client X-Lite est très riche en fonctionnalités et il est basé sur le standard SIP.

Asterisk offre toute une multitude de fonctionnalités, et les mettre toutes en œuvre serait fastidieux. Alors nous nous sommes limités à quelques fonctionnalités déjà réalisées par nos prédécesseurs, tout en y ajoutant la messagerie instantanée qui malheureusement comme la vidéo n'est point stable actuellement.

. Cette expérience enrichissante représente pour notre futur professionnel un atout majeur dont nous ne manquerons pas de nous y référer.

Cependant, ne pourrions-nous pas dans un futur proche interconnecter le serveur Asterisk avec le Téléphone traditionnel de sorte à ce qu'on puisse passer des appels de manière bidirectionnelles?

Bibliographie

Documents et Livres :

- [1] Auteurs : Didier OURABAH, Maxime GUILLET, Léonard LECOUEY, Vincent BATOUFFLET, William ZIVIC : Asterisk_report.pdf, Rapport de projet 2005/2006 LICENCE ISDRN Session 2005/2006
- [2]Auteur : Daniel Gaspar : Rapport_de_stage_nalta.pdf, Mémoire Conservatoire national des arts et de métiers
- [3] Auteurs : Quentin Hourlier, Benoit Henryon, Romain Gegout, Luis Dominguez Lopez : Asterisk_ToIP_rapport.pdf, Mémoire de Licence Professionnelle IUT Nancy Charlemagne – Département Informatique
- [4] Auteur : Nicolas Dewaele : Documentation-sur-la-telephonie-sur-ip.pdf, Nicodewaele.free.fr
- [5] Auteur : Elaboré par Chaker KHADHRAOUI : Implémentation du serveur de téléphonie (Asterisk) dans le cadre de projet de création d'un centre d'appel, Rapport de projet, université virtuelle de Tunis
- [6] Voip.pdf
- [7] Auteurs : Laurent Ouakil Guy Pujolle : Téléphonie sur Ip.pdf (SIP, H.323, MGCP, QoS et sécurité, Asterisk) 1^{ère} Edition
- [8] Auteurs : Laurent Ouakil, Guy Pujolle ,Titre: Téléphonie sur IP (SIP, H.323, MGCP, QoS et sécurité, Asterisk, VoWiFi, offre multiplay des FAI,Skype et autres softphones, architecture IMS,) 2è édition
- [9] Auteur : Jlassi ép Dhakouani Khaoula : Interconnexion de deux serveurs Asterisk et mise en place d'un répondeur itératif au sein de l'université virtuelle de Tunis, Rapport de projet de Fin d'études
- [10] Auteur : Yannick Yani Kalomba : Etude et mise au point d'un système de communication VOIP : application sur PABX-IP, open source « cas de l'agence en douane Getrak », Université protestante de Lubumbashi, Ingénieur en Réseaux et Télécoms 2009.
- [11] VoIP.doc : Quoi de neuf sur dans la voix sur ip

Webographie

- Site WEB Asterisk : <http://www.asterisk.org/>
- Site WEB AsteriskNOW : <http://www.asterisknow.org/>
- Site WEB Asterisk GURU : <http://www.asteriskguru.com/tutorials/>
- Forum Asterisk : <http://www.asterisk-france.net/community/>
- Site WEB VOip : <http://www.voip-info.org/wiki/index.php?page=Asterisk>
- Site WEB Freephonie : <http://www.freephonie.org/portal.php>