الجمهورية الجزائرية الديمقراطية الشعبية

**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

وزارة التعليم العالي والبحث العلمي

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

جامعة أبي بكر بلقايد – تلمسان –

**Université Aboubakr Belkaïd – Tlemcen –**

Faculté de TECHNOLOGIE

# MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

**En** : Télécommunications

**Spécialité** : Réseaux et Télécommunications

**Par** : Bibi Triki Arslane

Gadiri Riyad

**Thème**

# Développement d'un serveur voip client basé sur l'Asterisk

Soutenu le 04 /07/2021 devant le jury composé de :

| | | | |
|---|---|---|---|
| M. MOUSSAOUI Djillali | MCB | Univ. Tlemcen | Président |
| M. MERZOUGUI Rachid | PR | Univ. Tlemcen | Examinateur |
| M. HADJILA Mourad | MCA | Univ. Tlemcen | Encadrant |
| M.Bibi Triki Chakib | Ing | ICosnet | Co-encadrant |

Année Universitaire 2020-2021

# Remerciements

***Nous tenons tout d'abord à remercier les membres du jury pour leur présence, pour leur lecture attentive de notre mémoire.***
***Nous tenons à exprimer toute notre reconnaissance à notre directeur de mémoire, Mr.Hadjila Mourad. et notre c.o directeur Mr.Bibi Triki Chakib .Nous les remercions de nous avoir encadré, orienté, aidé et conseillé.***

***Nous adressons nos sincères remerciements à tous les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé nos réflexions et ont accepté de nous rencontrer et de répondre à nos questions durant nos recherches.***

***nous remercions nos très chers parents, qui ont toujours été là pour nous. Nous remercions nos frère , pour leurs encouragements.***

***Enfin, nous remercions nos amis , qui ont toujours été là pour moi. Leur soutien inconditionnel et leurs encouragements ont été d'une grande aide.***

***À tous ces intervenants, Nous présentons nos remerciements, notre respect et notre gratitude***

# Dédicace

*Je dédie ce mémoire à :*

*Mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse,*

*leur soutien et leurs prières tout au long de mes études,*

*Mes chers frères, Chakib et Fayçal pour leur appui et leur encouragement,*

*Toute ma famille pour leur soutien tout au long de mon parcours universitaire,*

*Que ce travail soit l'accomplissement de vos vœux tant allégués, et*

*le fruit de votre soutien infaillible,*

*Merci d'être toujours là pour moi.*

***Arslane Bibi Triki*** ✍

# Dédicace

*La vie n'est qu'un éclair, Et un jour de réussite est un jour très cher*

*A mon cher père, et ma chère mère.Pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance, et pour leurs patiences et leurs sacrifices*

*A mon cher frère ;*

*A tous mes proches ;*

*A tous ceux qui m'aiment ;*

*A tout mes ami(e)s ;*

*A tous ceux que j'aime.*

Je dédie ce mémoire.

***Riyad Gadiri*** ✍

# Résumé

Ce travail vise à la présentation générale de la VoIP, en tant que solution alternative attrayante pour un usage personnel et professionnel. Asterisk est un autocommutateur privé et gratuit (PABX) pour les systèmes GNU/Linux. Premièrement nous avons présenté la solution VoIP basée sur Asterisk , par la suite, le fonctionnement de cette solution ,plus loin dans cette partie, l'étude des divers protocoles et mécanismes qui font fonctionner une infrastructure VoIP. Deuxièment, nous avons présenté la partie pratique, une mise en place d'une solution VoIP qui contient la création de la machine virtuelle, l'installation du serveur Asterisk avec ça configuration. Nous avons finit ce travail, en découvrant les problèmes de sécurité qui existent et quelque solutions importantes .

**Mot clés** : VoIP , SIP , IP , Asterisk , Ubuntu , Sécurité .

# Abstract

This work aims at the general presentation of VoIP, as an attractive alternative solution for personal and professional use.The Asterisk is a free private branch exchange (PABX) for GNU / Linux systems. the first chapter, we present the VoIP solution based on Asterisk, then the operation of this solution, later in this part, the study of the various protocols and mechanisms that make a VoIP infrastructure work. The 2nd chapter presents the practical part, an implementation of a VoIP solution which contains the creation of the virtual machine, the installation of the Asterisk server with this configuration. We finish this thesis, by discovering the security problems that exist and some important solutions.

**Keywords** : VoIP , SIP , IP , Asterisk , Ubuntu , server , Security .

## Chapitre III: Vulnérabilités contre la voix sur IP et quelques moyens de sécurisation

# Listes des figures

## Chapitre I



## Chapitre II



## Chapitre III

# Liste des tableaux

# Introduction générale

Aujourd'hui, le qualificatif IP est utilisé pour tous les assaisonnements, bons ou mauvais. C'est évidemment le résultat du formidable développement d'internet au cours des dix dernières années: des protocoles de communication IP et d'un réseau hétéroclite utilisé presque exclusivement par les scientifiques et les militaires avant 1990 pour l'échange de messages et de fichiers. C'est le plus grand réseau de télécommunications au monde qu'on a amélioré, et de nouvelles applications sont apparues les unes après les autres.

On est passée de la téléphonie à commutation de circuits à la téléphonie IP qui utilise la commutation par paquets et un logiciel approprié grâce au protocole IP . Il devient alors possible de transmettre la voix sur un réseau informatique et donc de communiquer par la voix entre ordinateurs ou en utilisant des téléphones IP. Aujourd'hui, passer à la VOIP n'est plus seulement un avantage , c'est une obligation. Outre le fait que la qualité de service offerte par la VOIP est bien supérieure à celle offerte par le RTC, les fournisseurs de solutions téléphoniques ont complètement cessé de vendre des solutions analogiques pour ne proposer que des solutions VOIP.

Puisque la VOIP est en développement continue et qui est indispensable dans la vie quotidienne et professionnelle, on s'est intéressé dans l'étude primaire de l'installation du serveur SIP pour la voix sur IP, et comme il y a toujours des failles de sécurité dans l'environnement professionnels d'informatique, on a essayé d'étudier quelque solutions.

Nous a structuré ce mémoire comme suit : le premier chapitre contient la présentation des généralités sur la technologie VOIP . Le chapitre 2 détaille les étapes à suivre pour installer la machine virtuelle , installer et configurer un serveur SIP sous un astérisque, faire les test d'appel pour confirmer la fonctionnalité du serveur. .Le troisième chapitre concerne la thématique de sécurité au niveau de la VOIP.

# CHAPITRE I

## Généralités sur la voix sur IP

# I.1. Introduction

Les téléphones traditionnels sont sur le point de disparaître et la VoIP devient de plus en plus populaire. Au cours des deux dernières décennies, les communications IP (Internet Protocol) ont été de plus en plus utilisées dans l'industrie téléphonique. Aujourd'hui, il n'est plus nécessaire de séparer le réseau voix et les données. Les entreprises recherchent des solutions de communication plus riches en fonctionnalités, qui leur permettent plus que de simplement passer des appels. De plus en plus d'opérateurs ne fournissent que des téléphones IP, ce qui signifie que les entreprises migrent rapidement vers des systèmes de type VoIP PABX, qui offrent de grands avantages dans la convergence des réseaux voix et données. Ce chapitre est une introduction générale autour de cette technologie. Nous allons d'abord définir la VoIP et présenter son fonctionnement. Ensuite, nous présenterons les protocoles de signalisation et de transmission VoIP, ainsi que leurs principes de fonctionnement et leurs principaux avantages et inconvénients.

# I.2. Présentation de la VOIP

## I.2.1. Définition

### *I.2.1.1. Internet Protocol IP*

L'*Internet Protocol*, généralement abrégé IP, est un protocole de communication de réseau informatique par commutation de paquets. IP est le protocole d'Internet. IP est un protocole de niveau 3 du modèle OSI et du modèle TCP/IP comme le montre la figure **1**.1 permettant un service d'adressage unique pour l'ensemble des terminaux connectés.

Le protocole IP assure l'acheminement au mieux (*best-effort delivery*) des paquets, non-orienté connexion. IP ne se préoccupe pas du contenu des paquets, mais recherche un chemin pour les mener à destination [1].

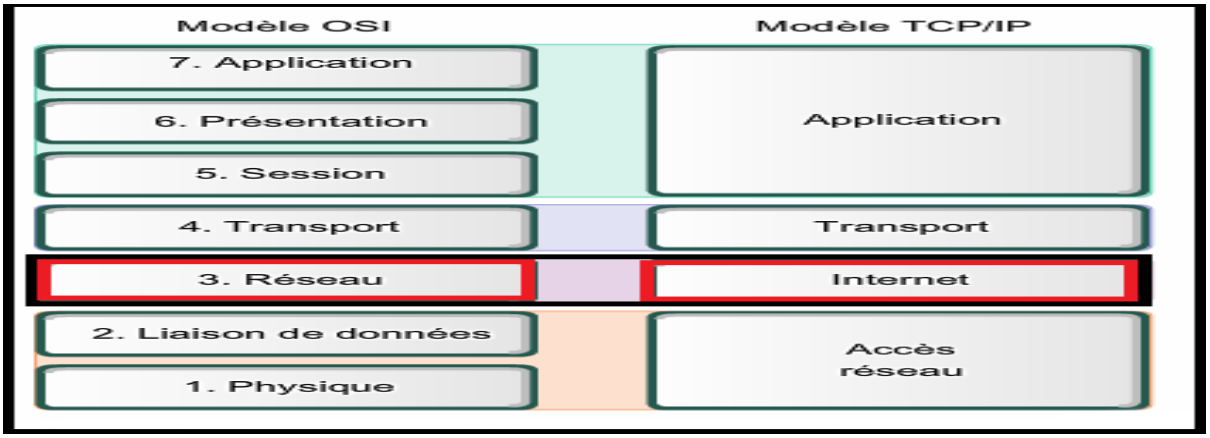


**Figure I.1.**Modèle OSI,modèle TCP/IP

### *I.2.1.2. VOIP*

Voix sur Internet Protocol, ou «VoIP» est une technologie informatique qui peut être utilisée sur Internet ou sur des réseaux privés (intranet) ou publics qu'ils soient filaires (câble / ADSL / fibre optique) ou non .

VoIP est un acronyme qui signifie Voice Over Internet Protocol, ou en d'autres termes, la transmission de la voix via Internet. C'est une technologie qui permet de délivrer des communications vocales ou multimédia (vidéo par exemple) via le réseau Internet (IP).

Les solutions VoIP à destination des entreprises incluent aussi des fonctionnalités de communications unifiées, telles que la conférence web, les informations de présence, le fax et la messagerie vocale par email, la messagerie instantanée, et plus encore. De plus, les applications pour smartphones permettent aux employés d'emporter leur extension professionnelle où qu'ils aillent. Les applications pour smartphones utilisent aussi la voix sur IP pour passer et recevoir des appels depuis le portable d'un utilisateur, exactement comme s'ils utilisaient leur propre extension professionnelle [2] .

### *I.2.1.3. PABX*

Un PABX ou PBX, pour **P**rivate **B**ranch **E**xchange, est l'anglicisme désignant un autocommutateur téléphonique privé. Le terme français étant très peu employé sur le marché, nous utiliserons les terminologies PABX et PBX ou IP PBX, IPBX ou PBX IP pour les versions utilisant les standards IP.

Un PABX est utilisé dans les systèmes de communication d'entreprise pour relier les standards et postes téléphoniques internes au réseau téléphonique. Il est le maillon local du système de téléphonie global basé sur des autocommutateurs locaux, régionaux, nationaux et internationaux, assurant le routage des communications. Un PABX permet ainsi aux entreprises de connecter l'ensemble des lignes internes à une ou plusieurs sorties opérateurs. Mais il offre également différentes fonctionnalités indispensables aux entreprises, comme par exemple :

- Possibilité de multiplier le nombre de lignes internes, sans pour autant avoir à augmenter les accès externes .
- Gestion de ses utilisateurs, de leurs extensions et de leurs droits d'appels
- Capacité à simplifier la collaboration et la communication des employés par le biais de conférences, transferts d'appels, renvois d'appels, …
- Permet de disposer d'une messagerie vocale personnalisée.

- Bénéficier de communication gratuite entre les utilisateurs de votre standard téléphonique PABX .
- Disposer de statistiques d'appels afin de comprendre les comportements de communication et les coûts de vos consommation .

Avec la fin du RTC, les PABX sont aujourd'hui très largement remplacés par des IPBX, basés sur le protocole internet (IP) et utilisant la VoIP. Les IP PBX offrent une richesse fonctionnelle étendue, une plus importante flexibilité opérationnelle et une plus forte efficience économique. Pour en savoir plus, n'hésitez pas à consulter notre article sur le sujet des IPBX [3].

## I.2.2. Fonctionnement de la voip

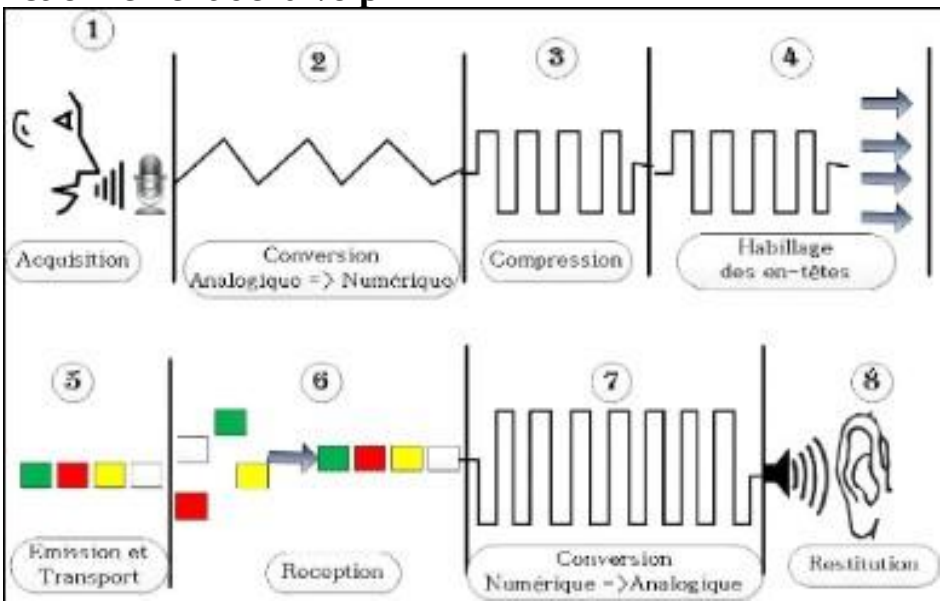


**Figure I.2**: fonctionnement de la voip

### I.2.2.1. Acquisition du signal

La VoIP suppose la transformation d'un signal continu analogique (la voix) en un signal discret numérique (composé d'une série de chiffres). 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.

### I.2.2.2. Numérisation

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

- l'échantillonnage du signal sonore, c'est-à-dire un prélèvement périodique de ce signal .
- la 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 (on parle de «résolution») de la conversion. Généralement, voix est échantillonnée à 8 kHz et chaque échantillon est codé sur 8 bits, ce qui donne un débit de 64 kbit/s (norme G711).

#### *I.2.2.3. 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 (bits) nécessaire pour l'exprimer. Plusieurs normes de compression et décompression (Codecs) sont utilisées pour la voix. L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal.

#### I.2.2.4. Habillage des en-têtes

Les données «brutes» qui sortent du DSP doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau. Trois «couches» superposées sont utilisées pour cet habillage :

- **La couche IP**

  La couche IP correspond à l'assemblage des données en paquets. Chaque paquet commence par un en-tête indiquant le type de trafic concerné, ici du trafic UDP.

- **La couche UDP**

  La deuxième couche, UDP, consiste à formater très simplement les paquets. Si l'on restait à ce stade, leur transmission serait non fiable : UDP ne garantit ni le bon acheminement des paquets, ni leur ordre d'arrivée.

- **La couche RTP (Real Time Protocol) / RTCP (Real Time Control Protocol)**

  Pour palier l'absence de fiabilité d'UDP, un formatage RTP est appliqué de surcroît aux paquets. Il consiste à ajouter des entêtes d'horodatage et de synchronisation pour s'assurer du réassemblage des paquets dans le bon ordre à la réception. RTP est souvent renforcé par RTCP qui comporte, en plus, des informations sur la qualité de la transmission et l'identité des participants à la conversation.

#### I.2.2.5. 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. Ils vont transiter sur le réseau (réseau local, réseau étendu voire Internet) en fonction des ressources disponibles et arriver à destination dans un ordre indéterminé.

#### I.2.2.6. 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. Ce point sera détaillé plus loin.

#### I.2.2.7. Conversion numérique analogique

La conversion numérique analogique est l'étape réciproque de l'étape 2, qui permet de transformer les données reçues sous forme de série discrète en un signal électrique «continu».

#### I.2.2.8. Restitution

Dès lors, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur [4] .

### I.2.3. Modes d'accès

Une communication dans un système de téléphonie VoIP est établie selon trois modes.

- *Téléphonie de PC à PC :*

Il consiste à équiper sur chaque PC, d'un microphone, d'un haut-parleur, d'une carte son (full duplex) et d'un logiciel de téléphonie (stimulateur téléphonique) sur IP qui tient lieu de téléphonie (figure 1.3).

Cette configuration est fréquemment couplée à des fonctionnalités de visioconférence à partir d'une webcam connecté à l'ordinateur.

Ce type de configuration peut être développé en entreprise, et se limitera à des usages restreints tels que la communication entre service technique.


**Figure I.3**: Communication de PC à PC.

- *Téléphonie de PC à Phone*

Ici l'un des correspondants est sur un PC et l'autre utilise un téléphone classique. Dans cette configuration, il faut passer via son fournisseur d'accès à Internet qui doit mettre en œuvre une « passerelle » (Gateway) avec le réseau téléphonique. C'est cette passerelle qui se chargera de l'appel du correspondant et de l'ensemble de la « signalisation » relative à la communication téléphonique, du côté du correspondant demandé .(figure 1.5)

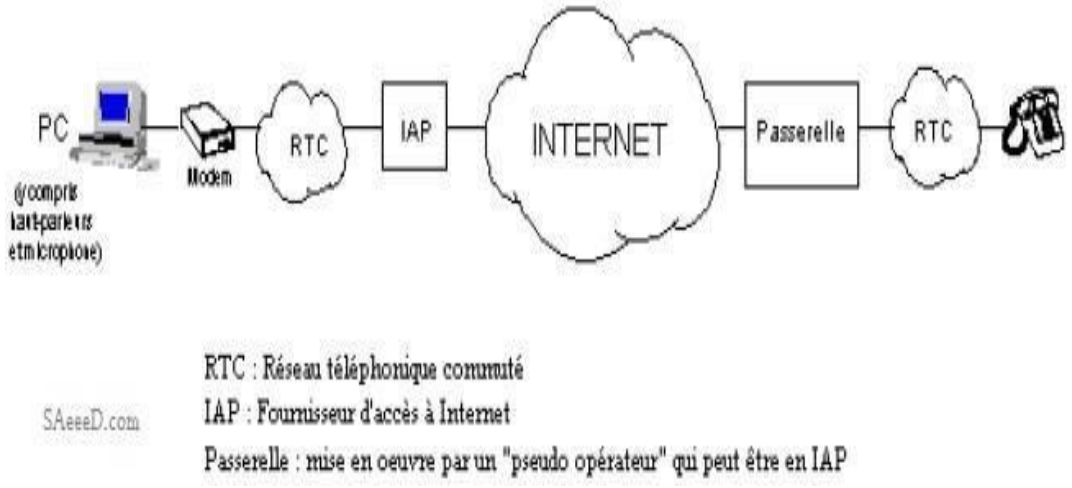


**Figure I.4 :** Communication de PC à téléphone classique

- *Téléphonie de phone à phone*

Ici les correspondants utilisent des téléphones analogiques. Pour faire dialoguer deux postes téléphoniques ordinaires via un réseau IP, des passerelles sont mises en place permettant ainsi d'accéder directement au réseau IP .(figure 1.5)

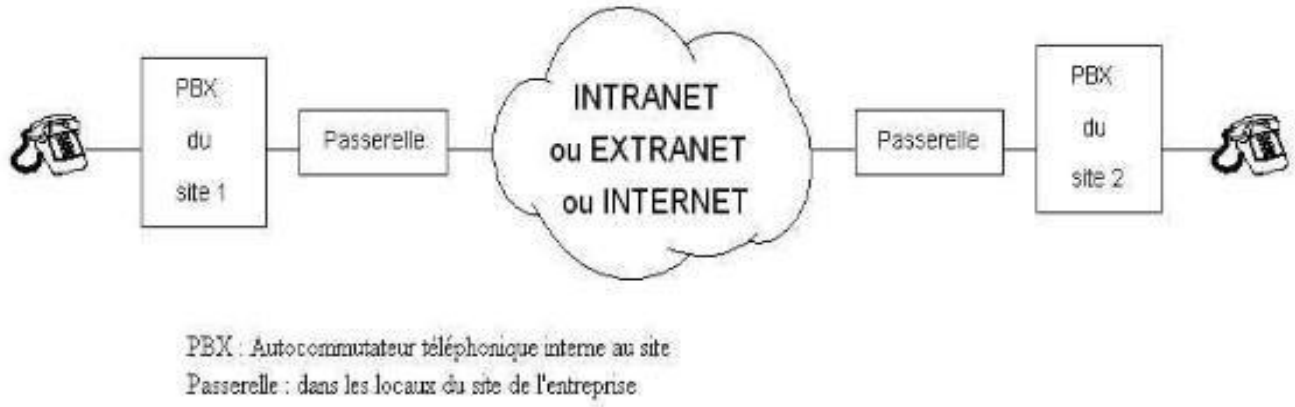


**Figure I.5 :** Communication entre postes téléphoniques classiques

[5]

# I.3. Avantages et désavantages

## I.3.1. Avantages

La VOIP offre en effet de très nombreux avantages et en fait une solution incontournable pour les entreprises quel que soit leur domaine d'activité, leur taille ou leur structuration.

### *I.3.1.1. Coûts*

L'utilisation d'une solution de téléphonie dématérialisée permet à votre entreprise de mieux maîtriser ses coûts de télécommunications. D'abord au niveau des infrastructures et du matériel : aucune installation supplémentaire n'est nécessaire puisque la technologie de Voix sur IP passe par votre connexion Internet. Vous n'avez donc plus besoin d'investir dans la maintenance de votre parc téléphonique et de vos infrastructures.

Ensuite, au niveau de vos factures téléphoniques : passer vos appels (nationaux et internationaux) par Internet vous permettra de réaliser des économies significatives .

### *I.3.1.2. Flexibilité*

Le temps du téléphone branché sur votre bureau est révolu. Avec une solution de téléphonie dans le cloud, vous restez joignable à tout moment sur votre numéro professionnel. Seule une connexion Internet suffit pour passer et recevoir vos appels professionnels depuis un logiciel d'appels téléphoniques installé sur votre ordinateur ou smartphone. Que vous ou vos collaborateurs soyez en voyage d'affaires, en déplacement professionnel ou en télétravail, vous ne perdrez plus jamais un appel important **[6] .**

#### *I.3.1.3. Intégration des services vidéo*

La VoIP intègre une gestion de la voix mais également une gestion de la vidéo. Si nous excluons la configuration des « multicasts » sur les composants du réseau, le réseau VoIP peut accueillir des applications vidéo de type vidéo conférence, vidéo surveillance, e-learning, vidéo on demand,…, pour l'ensemble des utilisateurs à un coût d'infrastructure réseau supplémentaire minime.[7]

#### *I.3.1.4. Une grande facilité d'utilisation*

L'utilisation d'un système numérique permet aux terminaux d'intégrer et de mixer un grand nombre de mode de communication et du supports différents (téléphones, visioconférence, ordinateurs, télécopieur, etc. )[8] .

### I.3.2. Désavantages

Où il y a un avantage, il y a nécessairement des inconvénients, parmi lesquelles, on cite

#### *I.3.2.1. Aucun service pendant une coupure électrique*

Pendant une panne d'électricité un téléphone normal est maintenu dans le service par le courant fourni par la ligne téléphonique. Ce n'est pas possible avec des téléphones d'IP, ainsi quand la puissance sort, il n'y a aucun service téléphonique de VOIP.

#### *I.3.2.2. Fiabilité*

Puisque VOIP se fonde sur une connexion internet, votre service de VOIP sera affecté par la qualité et la fiabilité de votre service d'Internet à bande large et parfois par les limitations de votre PC.

#### *I.3.2.3. Qualité de voix de VoIP*

VoIP a un peu à améliorer sur la qualité de voix, mais pas dans tous les cas. VoIP QoS (qualité du service) dépend de tant de facteurs : votre raccordement à bande large, votre matériel, le service a fourni par votre fournisseur, la destination de votre appel etc. [9]

## I.4. Les protocoles

H323, le premier protocole VoIP, existe depuis 1996 et a été initié par l'ITU (International Communication Union). Avant 2002, la VoIP n'a pas connue d'évolutions significative à cause de la complexité des premiers serveurs, le coût de la bande passante, la faible implantation du haut débit dans les entreprises, etc. Après 2002, une réelle accélération

de la VOIP avec l'émergence de nouveaux protocoles VOIP standardisés issus du monde IP: SIP, IAX .

## I.4.1. H323

Le protocole H323 regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP. C'est Un protocole développé par l'UIT-T qui le définit comme ″Systèmes de communication multimédia en mode paquet" . La norme H323 propose des bases pour le transport de la voix, de la vidéo et des données sur des réseaux IP. Il fonctionne en mode non connecté et sans garantie de qualité de service .Il définit les protocoles nécessaires à partir de la couche transport du modèle OSI [10].

### *I.4.1.1. Les protocoles de H323*

- Protocole de signalisation (H225, Q.931) : RAS (Registration Admission Status) pour l'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel.

- Protocole de négociation (H245) : La négociation est utilisée pour se mettre d'accord sur la façon de coder les informations qu'on va s'échanger.

- Protocole de transport de l'information (RTP/RTCP) : RTP pour le transport de la voix, la vidéo ou les données numérisées par les codecs, et le protocole RTCP pour faire du contrôle de qualité [11] .

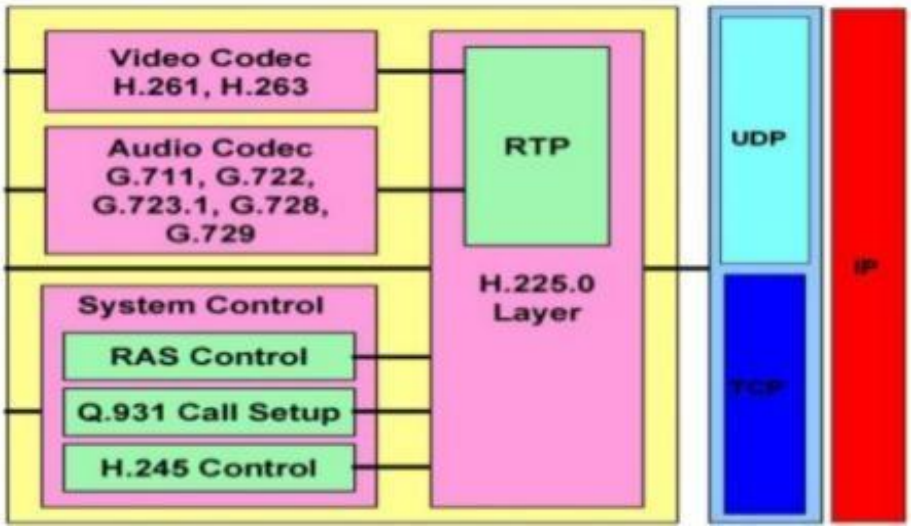


**Figure I.6** : Architecture des protocoles suivant H.323

Protocole du contrôle et de signalisation : H.225, H.245, Q.931, RTCP

Standards audio : G.711, G.722, G.723, G.726, G.728, G.729

Standards vidéo : H.261, H.263, H.263+, H.264

Pour les données : T.123, T.124, T.125

### *I.4.1.2. Les éléments du réseau H.323*

- *Un périphérique Terminal* : Un poste téléphonique IP raccordés directement au réseau Ethernet de l'entreprise.

-*Un PC multimédia* : sur lequel est installé une application compatible H.323 Gateway (Passerelle) :

- Il assure l'interconnexion entre le réseau H.323 et les autres réseaux téléphoniques (RTC, SIP,…) .
- La conversion entre les formats de transmission .

-*Gatekeeper (Portier) :*

- Il se charge de l'enregistrement des clients .
- La traduction d'adresse (numéro de téléphone - adresse IP) .

- *Multipoint Control Unit*: Il permet aux clients de se connecter aux sessions de conférence [11] .

### *I.4.1.3. le fonctionnement de H323:*

➢ communication "point à point" de deux clients simple:

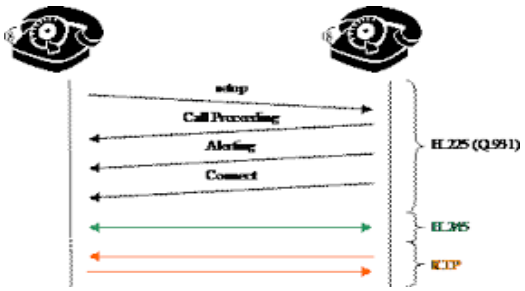


**Figure I.7:** communication "point à point" de deux clients simple

* L'appelant saisit l'adresse IP du destinataire dans le champ du logiciel réservé à cet effet.

* Les protocoles de signalisation proposent au logiciel du destinataire d'établir la communication et transmet son ID H323.

* Le logiciel du destinataire répond soit « occupé » soit « libre ».

* Si « libre », l'appelant énumère ses possibilités de codecs audio et vidéo (si disponibles).

* Le destinataire énumère les codecs compatibles à l'appelant pour accord.

* Si accord, d'autres ports TCP et UDP sont négociés pour l'audio (UDP), la vidéo (UDP) et les données (TCP).

- communication "point à point "entre deux clients enregistrer auprès d'un gatkeeper :

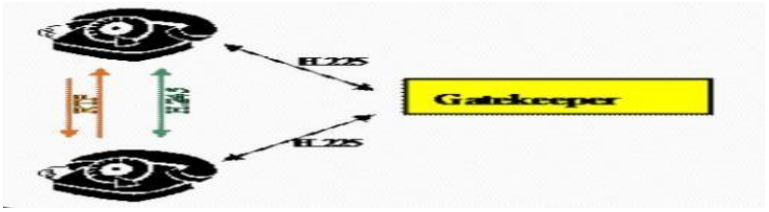


**figure I.8:** communication "point à point "entre deux clients enregistrer auprès d'un gatkeeper

-Le gatekeeper intervient sur la signalisation.

- À l'ouverture du logiciel, les clients A et B s'enregistrent auprès du gatekeeper en lui transmettant leur ID H323 et leur adresse IP respective.

- -communication "multipoint" entre plusieurs clients:

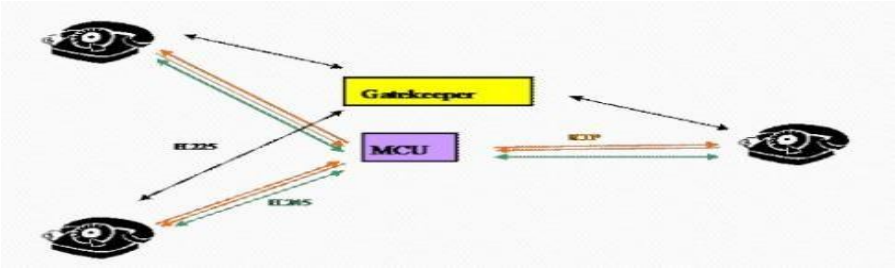


**Figure I.9:** communication "multipoint" entre plusieurs clients

Les MCU( multipoint control unit) ont des capacités de traitements du signal (diffusion, enregistrement, mixage, …). ils sont utilisés pour :

*permettre la conférence en mixant les flux audio .

* diffuser des messages réseau comme la tonalité, le bip de mise en attente

* voire réaliser des fonctions élémentaires de messagerie vocale [12].

## I.4.2. Le protocole SIP:

Session Initiation Protocol (SIP) est un protocole TCP/IP de couche application normalisé et standardisé par l'IETF (RFC 3261). Il a été conçu pour établir, modifier et terminer des sessions multimédia. Il prend en charge l'authentification et la localisation de multiples participants. S'il se charge de la négociation des médias, il laisse le soin à d'autres protocoles de transporter du texte, de la voix ou de la vidéo .

SIP prend en charge cinq facettes de l'établissement et de la terminaison de communications multimédia :

Localisation de l'utilisateur : détermination du système terminal à utiliser pour la communication . Disponibilité de l'utilisateur : détermination de la volonté de l'appelé à

s'engager dans une communication Capacités de l'utilisateur : détermination du support et des paramètres de support à utiliser.Etablissement de session : "sonnerie", établissement des paramètres de session à la fois chez l'appelant et l'appelé. Gestion de session : y compris le transfert et la terminaison des sessions, la modification des paramètres de session, et l'invocation des services [13].

### *I.4.2.1. Ces entités*

SIP définit deux types d'entités: les clients et les serveurs. Plus précisément les entités définies par SIP (Figure 1.10):

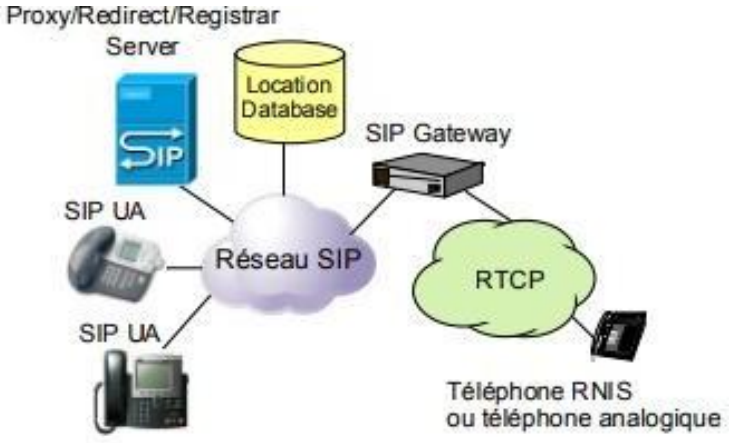


**Figure I.10** : Les entités d'un réseau SIP

- Le serveur proxy (Proxy server) : Il reçoit des requêtes de clients qu'il traite lui-même ou qu'il achemine à d'autres serveurs après avoir éventuellement réalisé certaines modifications sur ces requêtes.

- Le serveur de redirection (Redirect server) : Il s'agit d'un serveur qui accepte des requêtes SIP, traduit l'adresse SIP de destination en une ou plusieurs adresses réseau etles retourne au client. Contrairement au Proxy server, le Redirect server n'achemine pas de requêtes SIP. Dans le cas d'un renvoi d'appel, le Proxy server a la capacité de traduire le numéro de l'appelé dans le message SIP reçu, en un numéro de renvoid'appel et d'acheminer l'appel à cette nouvelle destination, et ce, de façon transparente pour le client origine ; pour le même service, le Redirect server retourne le nouveau numéro (numéro de renvoi) au client origine qui se charge d'établir un appel vers cette nouvelle destination.
- L'agent utilisateur (UA, User Agent) : Il s'agit d'une application sur un équipement de

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

- L'enregistreur (Registrar): Il s'agit d'un serveur qui accepte les requêtes SIP REGISTER. SIP dispose de la fonction d'enregistrement d'utilisateurs. L'utilisateur indique par un message REGISTER émis au Registrar, l'adresse où il est joignable (e.g., adresse IP). Le Registrar met alors à jour une base de données de localisation. L'enregistreur est une fonction associée à un Proxy server ou à un Redirect server. Un utilisateur peut s'enregistrer sur différents UAs SIP ; dans ce cas, l'appel lui sera délivré sur l'ensemble de ces UAs [14].

### *I.4.2.2. Mécanisme d'un appel SIP*

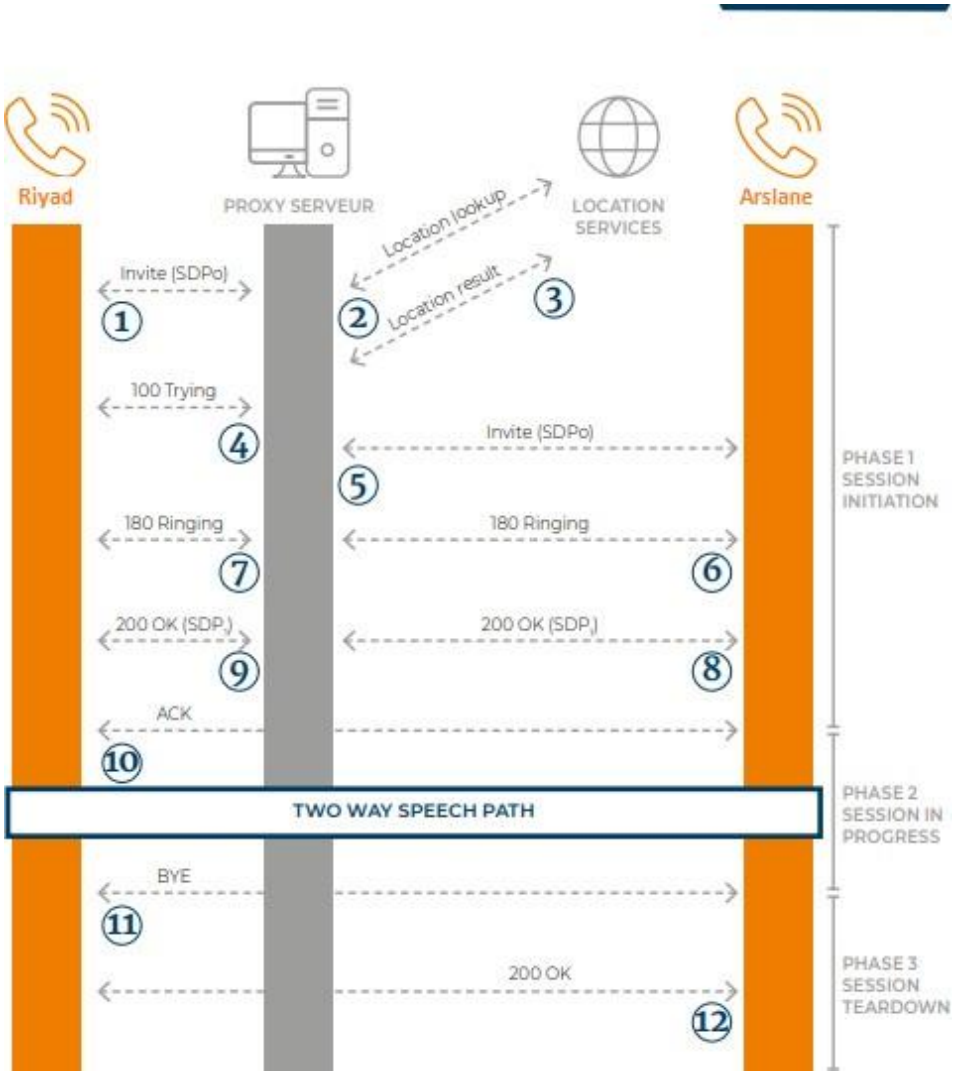

**Figure I.11:** Mécanisme d'un appel SIP

**1:** Riyad appelle Arslane et envoie une requête INVITE au Proxy Server.

**2:** Le Proxy Server regarde au sein du Location Service quelle est l'adresse IP réelle du poste appelé.

**3:** Le Proxy Server reçoit la réponse du Location Service, et génère une réponse « 100 Trying » indiquant qu'il va tenter de joindre le poste distant.

**4:** Le Proxy Server relaie l'INVITE vers le poste distant maintenant qu'il connaît sa localisation exacte.

**5:** Le poste distant accepte l'appel entrant et se met à sonner. Il en informe le proxy via une réponse « 180 Ringing ».

**6:** Le Proxy Server relaie la réponse à l'appelant.

**7:** Le poste distant est décroché par l'utilisateur, l'appel est pris. Il génère une réponse « 200 OK ».

**8:** Le Proxy Server relaie la réponse « 200 OK » au poste appelant

**9:** Le poste appelant envoie une requête « ACK » directement au poste appelé (elle peut passer par le serveur ou pas, suivant la négociation préalable et la configuration).

**10:** Le poste appelant envoie une requête « ACK » directement au poste appelé (elle peut passer par le serveur ou pas, suivant la négociation préalable et la configuration).

**11:** Quand l'appelant raccroche, il envoie une requête « BYE » au poste appelé (qui peut également passer par le Proxy Server ou pas).

**12:** La réception de la requête « BYE » est confirmée par l'émission d'un message « 200 OK » par le poste qui la reçoit [15].

## I.4.3. Comparaison entre H323 et SIP:

| | **H323** | **SIP** |
|---|---|---|
| **Inspiration** | Téléphonie | http |
| **Nombres d'échanges pour établir la connexion** | 6 à 7 aller-retour | 1 à 5 aller-retour |
| Complexité | Elevée | Faible |
| Adaptabilité / Modularité protocolaires | Faible | Elevée |
| Implémentation de nouveaux services | NON | OUI |

| Protocoles de transport | TCP | TCP ou UDP |
|---|---|---|
| Coût | Elevé | Faible |
| Avantages | - Maturité du protocole (Version 4)<br>- bien adopté par les constructeurs | - Interopérabilité très bonne<br>- Bonne gestion de la mobilité |
| **Inconvénients** | - Manque d'inter-opérabilité entre les différentes implémentations<br>- Difficultés avec les FireWall<br>- Support des fonctions avancées de la téléphonie très complexe | - En pleine maturation<br>- Problème avec la translation d'adresses |
| Exemples de solutions utilisant protocole | Livecom | Wengo, Yahoo! Messenger, MSN Messenger, Gizmo |

**Tableau I.1** Comparaison entre H323 et SIP

## I.4.4. Les protocoles de transports

### *I.4.4.1. UDP*

Le protocole de datagramme utilisateur (UDP) est le protocole de transport sans confirmation. UDP est un protocole simple qui permet aux applications d'échanger des datagrammes sans accusé de réception ni remise garantie.Le traitement des erreurs et la retransmission doivent être effectués par d'autres protocoles. UDP n'utilise ni fenêtrage, ni accusés de réception, il ne reséquence pas les messages, et ne met en place aucun contrôle de flux. Par conséquent, la fiabilité doit être assurée par les protocoles de couche application. Les messages UDP peuvent être perdus, dupliqués, remis hors séquence ou arriver trop tôt pour être traiter lors de leurs réception. UDP est un protocole particulièrement simple conçu pour des applications qui n'ont pas à assembler des séquences de segments. Son avantage est un temps d'exécution court qui permet de tenir compte des contraintes de temps réel ou de limitation d'espace mémoire sur un processeur, contraintes qui ne permettent pas l'implémentation de protocoles beaucoup plus lourds comme TCP. Dans des applications temps-réel, UDP est le plus approprié, cependant il présente des faiblesses dues au manque de

fiabilité. Des protocoles de transport et de contrôle temps-réel sont utilisés au dessus du protocole UDP pour remédier à ses faiblesses et assurer sa fiabilité [16]. Ces protocoles sont RTP et RTCP.

### *I.4.4.2. RTP*

Real-Time Transport Protocol (RTP) est un protocole Internet standard se plaçant au-dessus d'UDP, qui fournit aux programmes un moyen de gérer la transmission en temps réel de données multimédia sur les services réseau unicast ou multicast. Le protocole de transport en temps réel est un protocole réseau permettant de diffuser de l'audio et de la vidéo sur les réseaux IP. Le RTP est utilisé dans les systèmes de communication et de divertissement qui impliquent des médias en continu, tels que la téléphonie, les applications de vidéoconférence, y compris WebRTC, les services de télévision et les fonctionnalités de push-to-talk basées sur le Web. RTP fonctionne généralement sur le protocole UDP (User Datagram Protocol). RTP est utilisé en conjonction avec le protocole de contrôle RTP (RTCP). Alors que RTP transporte les flux multimédias (par exemple, audio et vidéo), RTCP est utilisé pour surveiller les statistiques de transmission et la qualité de service (QoS) et facilite la synchronisation de plusieurs flux. RTP est l'un des fondements techniques de la voix sur IP et, dans ce contexte, il est souvent utilisé en conjonction avec un protocole de signalisation tel que le protocole d'initiation de session (SIP) qui établit des connexions à travers le réseau. RTP a été développé par le groupe de travail sur le transport audio-vidéo de l'Internet Engineering Task Force (IETF) et publié pour la première fois en 1996 sous le nom de RFC 1889, qui a ensuite été remplacé par la RFC 3550 en 2003 [17].

### *I.4.4.3. RTCP*

RTP (RTCP) est le protocole sœur du protocole de transport en temps réel (RTP). Ses fonctionnalités de base et sa structure de paquets sont définies dans la RFC 3550. RTCP fournit des statistiques hors bande et des informations de contrôle pour une session RTP. Il partage avec RTP la livraison et le conditionnement des données multimédias, mais il ne transfère aucune donnée multimédia par lui-même.

La fonction principale du RTCP est de fournir des commentaires sur la qualité de service (QoS) dans la distribution des médias en envoyant périodiquement des informations statistiques telles que le nombre d'octets et de paquets envoyés, la perte de paquets, le

changement de délai de paquet et le temps de retard dans les deux sens aux participants dans une session de diffusion multimédia. L'application peut utiliser ces informations pour contrôler la qualité des paramètres de service, peut-être en limitant le flux ou en utilisant un codec différent.

#### *I.4.4.4. ICMP*

L'Internet Control Message Protocol est un protocole de couche Internet utilisé par les périphériques réseau pour diagnostiquer les problèmes de communication réseau. L'ICMP est principalement utilisé pour déterminer si les données atteignent ou non leur destination prévue en temps voulu. Généralement, le protocole ICMP est utilisé sur des périphériques réseau, tels que les routeurs.

Le but principal d'ICMP est de signaler les erreurs. Lorsque deux appareils se connectent via Internet, l'ICMP génère les erreurs à partager avec l'appareil d'envoi dans le cas où aucune des données ne parvenait à sa destination prévue.

Une utilisation secondaire du protocole ICMP consiste à effectuer des diagnostics réseau ; les utilitaires de terminal courants traceroute et ping fonctionnent tous deux à l'aide d'ICMP. L'utilitaire traceroute est utilisé pour afficher le chemin de routage entre deux périphériques Internet. Le chemin de routage est le chemin physique réel des routeurs connectés qu'une requête doit traverser avant d'atteindre sa destination. Le trajet entre deux routeurs est connu sous le nom de « saut », et un traceroute indique également le temps requis pour chaque saut le long du chemin. Cela peut être utile pour déterminer les sources de retard du réseau.[18]

# I.5. Asterisk


**Figure I.12: Asterisk**

## I.5.1. Définition

Asterisk est un PABX open source pour systèmes UNIX originellement crée en 1999 par Mark Spencerfondateur de la société Digium. Asterisk est publié sous licence GPL.

Asterisk est un PABX applicatif open source permettant d'interconnecter en temps réel des réseaux de voix sur IP et des réseaux de téléphonies classiques via des cartes d'interface téléphonique [19].

## I.5.2. Fonctionnalités

Asterisk propose toutes les fonctionnalités d'un standard téléphonique de niveau profes-sionnel, des plus élémentaires aux plus complexes. Non seulement, il permet de gérer le routage des appels au sein du réseau, mais en plus il supporte une large gamme de servi-ces, notamment les suivants :

• Authentification des utilisateurs appelants.

• Serveur vocal, ou standard d'accueil téléphonique automatisé, aussi appelé IVR (Inte-

ractive Voice Response). Cette fonction permet de demander à l'appelant le service qu'il souhaite utiliser et d'effectuer le routage correspondant.

• Numérotation abrégée pour définir des raccourcis.

• Transfert d'appel.

• Filtrage des appels.

• Messagerie vocale (répondeur automatique).

• Notification et écoute par e-mail des messages laissés sur son répondeur (voicemail).

• Gestion des conférences.

• Double appel.

• Mise en attente.

• Journalisation des appels.

• Facturation détaillée.

• Enregistrement des appels.

### I.5.3. Les protocoles supportés

Asterisk est capable d'utiliser différents protocoles utilisés dans la VoIP principalement H.323 et SIP (Session Initiation Protocol) qui sont les deux protocoles principaux.Bien sur Astérisk propose son propre protocole IAX (Inter-Astérisk Exchange).

### I.5.4. IAX

Le protocole IAX (Inter-Asterisk Exchange) est conçu pour fournir le contrôle et la transmission de données média sur Internet. Il permet la communication entre client et serveur ainsi qu'entre serveurs.IAX a le rôle d'un protocole contrôleur et transporteur de données média. Il est destiné spécialement pour les appels voix sur IP.

IAX est considéré comme protocole « all in one » pour manipuler les données multimédias. Il combine le contrôle, la transmission de données média dans un seul protocole. De plus, IAX utilise un port unique et statique pour simplifier la traversée et la translation d'adresse IP, et aussi pour éviter l'utilisation d'autres protocoles autour du serveur NAT. Le protocole IAX utilise un entête compact pour minimiser l'utilisation de la bande passante. Sa

nature open source permet également l'ajout de nouveaux types de contenu pour supporter des services supplémentaires [20].

## I.6. Conclusion

Actuellement pour effectuer une conversation on utilise la voip qui est la solution la plus rentable .C'est une technologie révolutionnaire qui enfreint les règles établies par la technologie de téléphonie PSTN. Elle est plus flexible, convivial, ne nécessite pas beaucoup d'investissements, coûte moins cher, offre de nouveaux services et de nombreux autres avantages tels que les communication interne et externe. Son objectif principal est d'améliorer l'environnement de travail des employés de l'entreprise en libérant les utilisateurs de la position du téléphone.

Dans le deuxième chapitre, nous détaillerons les étapes nécessaires à la création d'un serveur VoIP à l'aide de l'outil Asterisk.

# Chapitre II

# La mise en œuvre de la solution VoIP basée sur Asterisk

# II.1. Introduction

Asterisk est une plate-forme open source pour la création d'applications de communication en temps réel. C'est un outil très puissant. Vous pouvez créer un réseau de bureau simple avec quelques téléphones, ou vous pouvez créer des applications riches en fonctionnalités qui peuvent effectuer des recherches de base de données externes et prendre des décisions de routage d'appels intelligentes. Lors de la création d'applications utilisant la voix, la vidéo ou même les SMS, Asterisk offre des possibilités presque illimitées. Que vous souhaitiez créer un système téléphonique simple permettant aux utilisateurs internes de passer et recevoir des appels ou que vous souhaitiez écrire une application vocale complexe qui s'intègre à l'entreprise, Asterisk peut vous aider.

# II.2. Installation d'UBUNTU dans Virtualbox

## II.2.1. Création de la machine virtuelle Ubuntu dans VirtualBox

- *1ère étape:* -Donner un nom à la machine virtuelle

-Sélectionner le type et la version de notre virtuelle machine

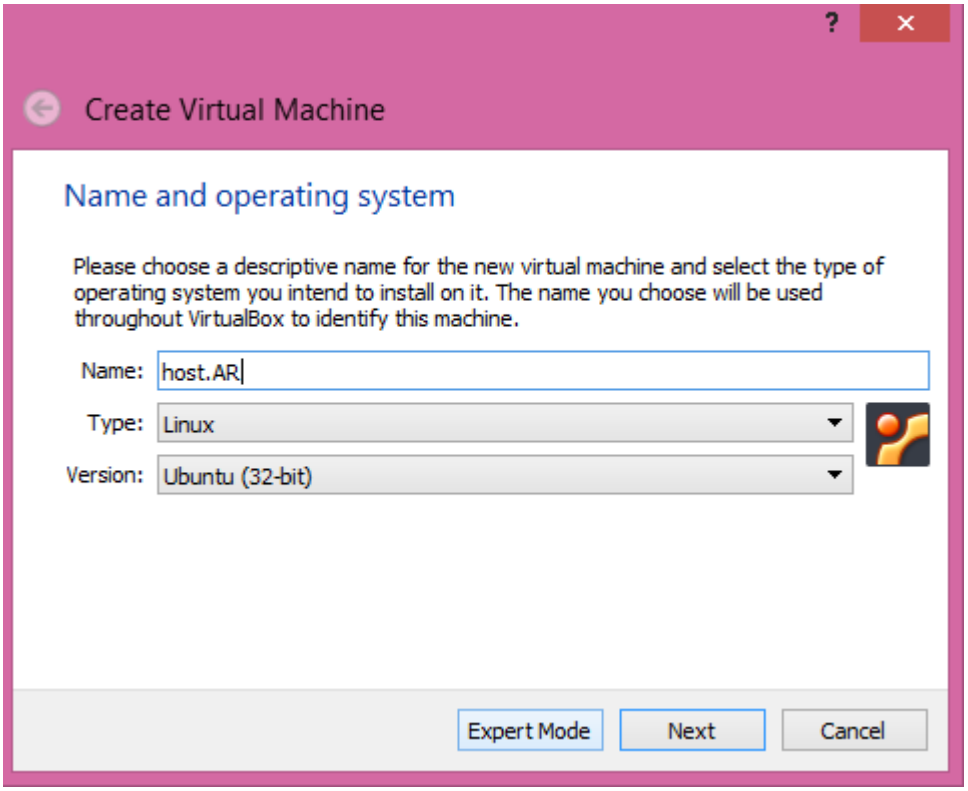


**Figure II.1.** Nom et système d'exploitation

- *2ème étape:* sélectionner la quantité de mémoire en méga-octets allouée à la machine virtuelle

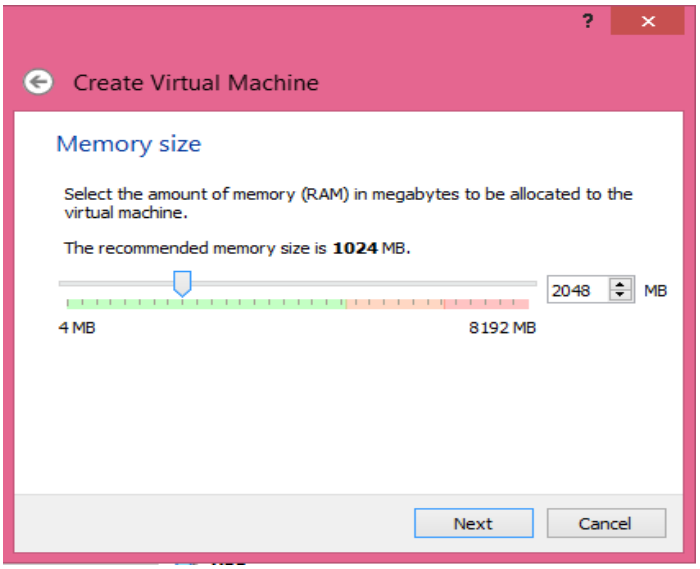


**Figure II.2** Taille de la mémoire vive

- *3ème étape*: créer un disque dur virtuel

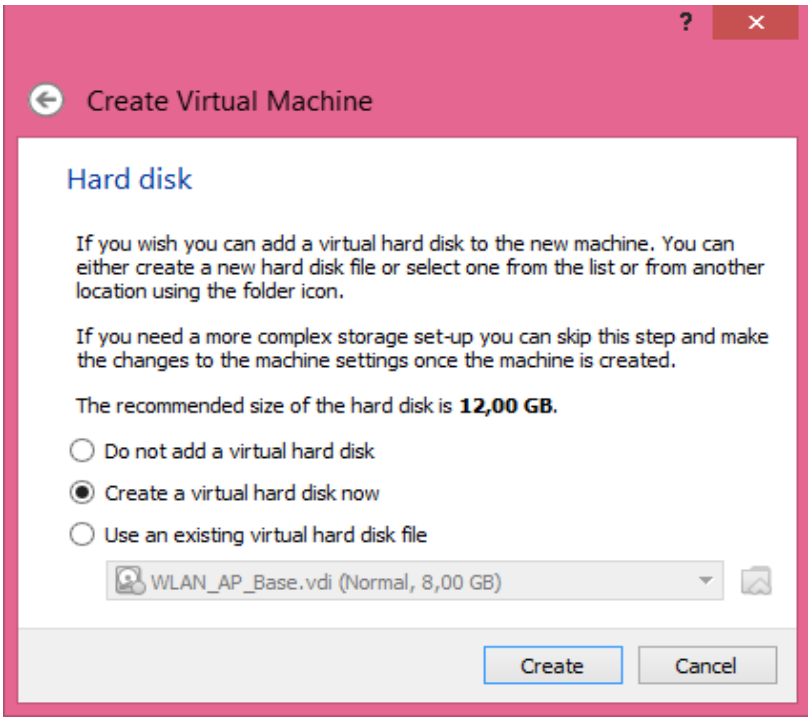


**Figure II.3** Disque dur

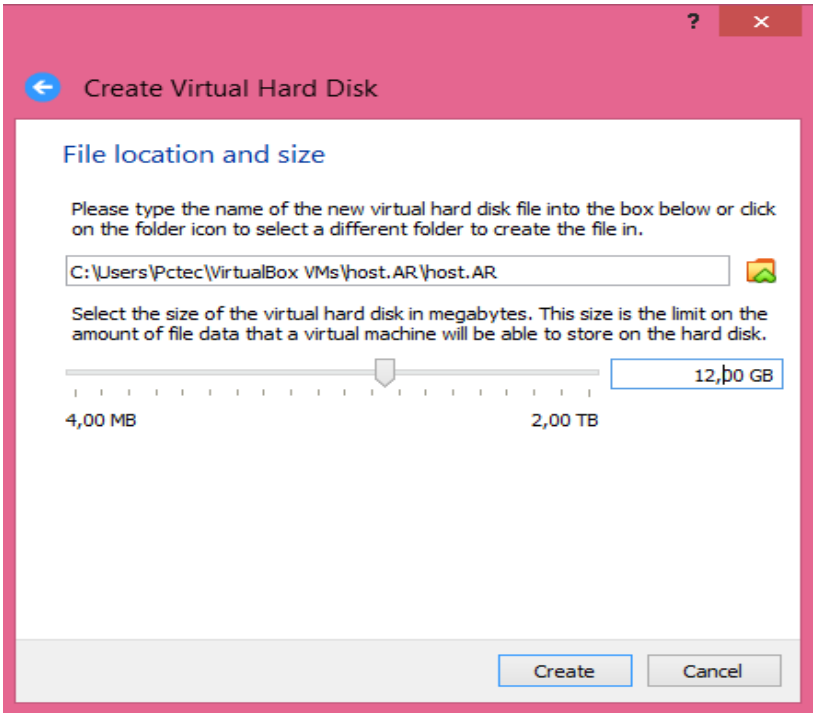


**Figure II.4** Emplacement du fichier et taille

Après cette étape, la machine est ajoutée à la liste dans le gestionnaire de machine virtuelle VirtualBox.

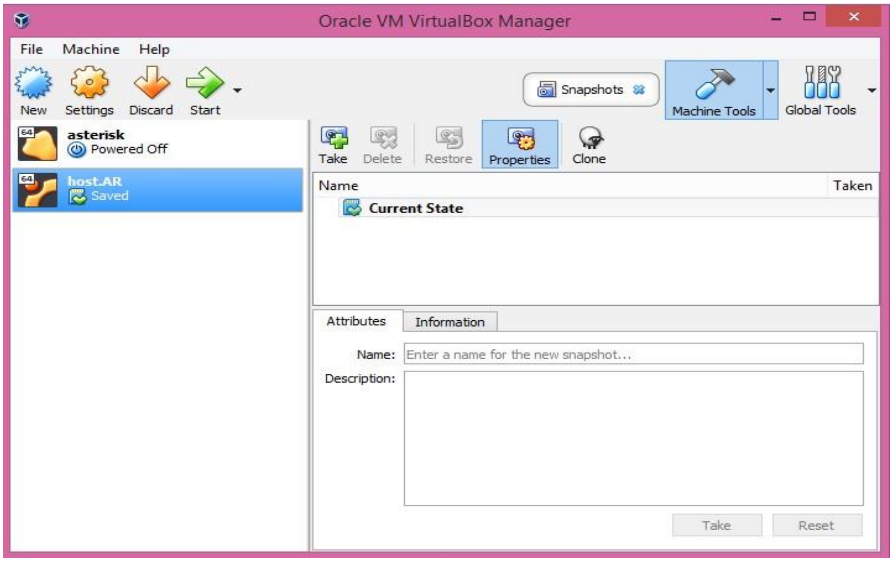


**Figure II.5** VM

## II.2.2. Installation

Pour lancer l'installation d'Ubuntu dans Virtualbox, il faut d'abord télécharger l'image ISO et la sauvegarder dans le disque dur.

>*image ISO:* Un fichier électronique unique qui contient le contenu identique d'un disque optique, y compris la hiérarchie des dossiers et des fichiers. À l'aide d'une extension de fichier .ISO, des images ISO sont créées pour distribuer les données du disque sur un réseau afin de graver un CD ou un DVD sur l'ordinateur de destination. Les fichiers de l'image ISO ne sont pas compressés ; cependant, un programme utilitaire ISO est requis pour les identifier et graver le disque avec la structure de fichier/dossier d'origine.

- Sélectionnez-la VirtualBox Ubuntu et cliquez sur **configuration** (settings),appuyer sur **Storage,** puis sélectionnez l'image ISO précédemment téléchargée.
  Laisser les autres paramètre de préférence par default. Cliquez sur **ok** pour enregistrer les modifications.

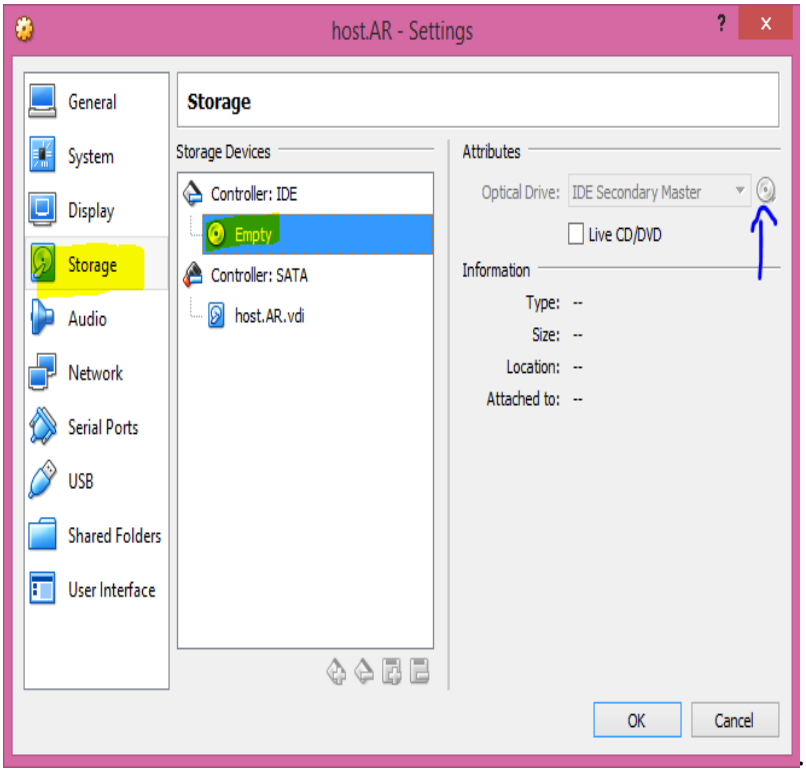


**Figure II.6.** Choisir le fichier ISO d'installation

- Cliquer sur **démarrer** (star) pour déclencher la vm,


**Figure II.7.**Lancement de la machine virtuelle

- Aprés avoir choisi la langue, on appuie sur "Essayer Ubuntu"

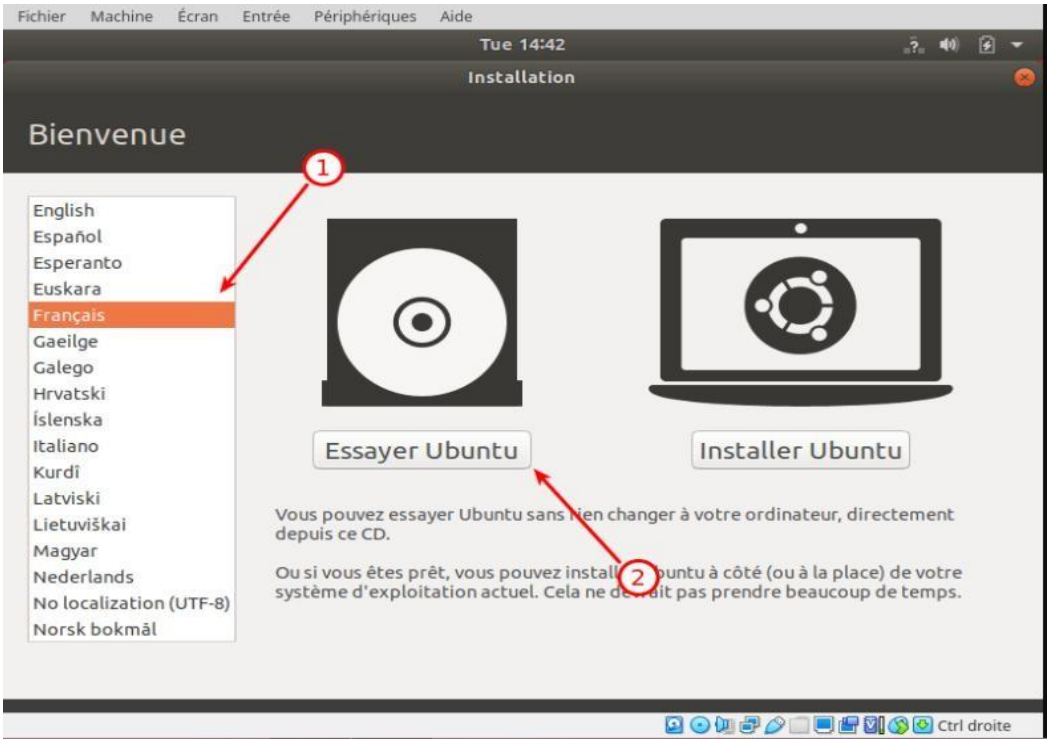


**Figure II.8.** Instalation

- Ouvrez les paramètre et modifier la résolution pour avoir une meilleure visibilité.

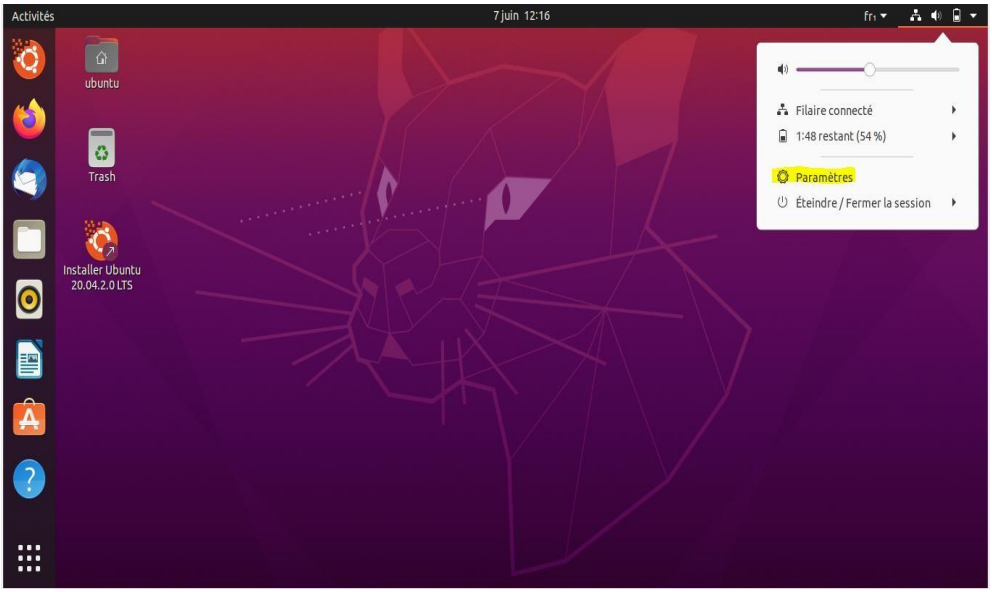


**Figure II.9.**La barre de paramètres

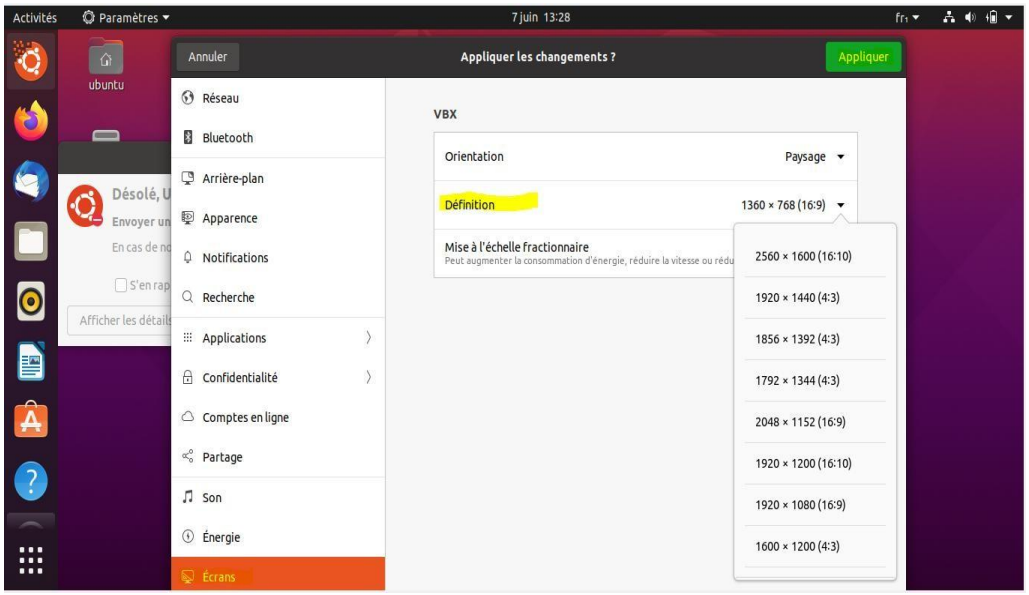


**Figure II.10.** Modification de la résolution

# II.3. Installation et configuration d'Asterisk

## II.3.1. Installation

On ouvre le terminal avec "Ctrl+Alt+T"

- Premièrement il faut mettre à jour la distribution en tapant :

```
arsriyad@arsriyad Vitua lBox:~S sudo apt update
arsriyad@arsriyad-Vitua Box:-$ sudo apt upgrad
```

- Nous passons ensuite, à l'installation de dépendance

```
arsriyad@arsriyad Vitua lBox:~S Sudo apt-get install build-essential libxml2-dev libncurses5-dev linux-headers-`uname -r` libsqlite3-dev libssl-dev
```

- Créer un dossier pour contenir les source d'Asterisk

```
sudo mkdir /usr/src/asterisk
cd /usr/src/asterisk
```

- Le téléchargement de la dernière version d'asterisk, et l'installation se fait par la commande ci-dessous :

```
sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/releases/asterisk-16.18.0.tar.gz tar xvzf asterisk-16.18.0.tar.gz
cd asterik- 16.18.0
```

```
sudo ./configure
```

- Puis taper cette commande pour personnaliser les paramètres:

```
sudo make menuselect
```

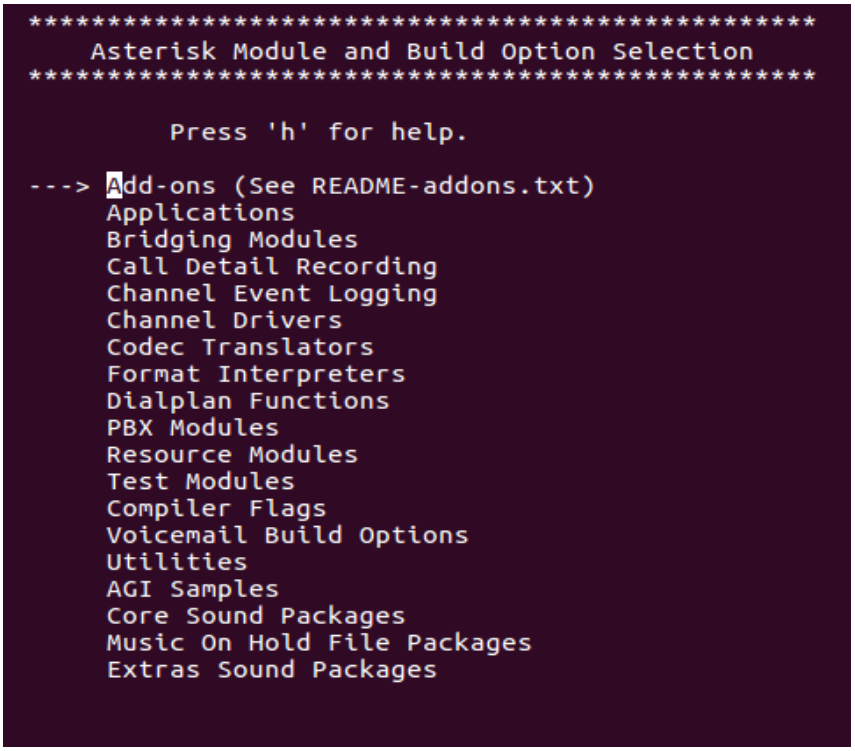


**Figure II.11**.Paramètre d'Asterisk

Le menu qui s'affiche nous permet de personnaliser l'installation d'Asterisk

=>Core Sound Package et cochez CORE-SOUNDS-FR-ULAW à l'aide de la touche Espace. Quittez en pressant la touche Echap.

=>Music On Hold File Packages,décochez MOH-OPSOUND-WAV et cochez MOH-OPSOUND-ULAW.

=>Extras Sound Packages et cochez EXTRA-SOUNDS-FR-ULAW.

- Et pour terminer l'installation il faut taper les commandes suivantes

```
sudo make
sudo make install
sudo make samples
```

```
sudo make config
```

- Enfin, lancer Asterisk à l'aide de la commande suivante

```
sudo /etc/init.d/asterisk start
```

- afficher la console d'Asterisk avec la commandes:

```
asterisk -cvvvvvvvvvvr
```

## II.3.2. .Configuration

### *II.3.2.1. La création des comptes utilisateurs*

Elle se fait dans le fichier **sip.conf**

```
cd /etc/asterisk/
sudo nano sip.conf
```

Nous allons éditer ce fichier et y créer les utilisateurs 800 et 801 avec comme numéro respectif 800 et 801

```
[800]
type = friend
secret = 800
username = 800
callerid="800"
context = CLIENT_IN
qualify = yes
nat = yes
host = dynamic
disallow=all
allow=all
allow=ulaw
allow=alaw
allow=g729
call-limit=1
```

**Figure II.12.**Utilisateur 1

```
[801]
type = friend
secret = 801
username = 801
callerid="801"
context = CLIENT_IN
qualify = yes
nat = yes
host = dynamic
disallow=all
allow=all
allow=ulaw
allow=alaw
allow=g729
call-limit=1
```

**Figure II.13.** Utilisateur 2

**Explication des options:**

**[**800**]=>** Numéro SIP

type = friend =>Type d'objet SIP,il existe 3 types d'utilisateurs:peer, user,friend

>Le type "friend" permet à l'utilisateur d'émettre et de recevoir les appels

secret = 800 =>Mot de pass de compte Sip (utilisateur)

username =>Nom d'utilisateur

context =>Utiliser dans le fichier extension.conf

host =dynamic => l'utilisateur peut se connecter a ce compte à partir de n'importe quelle adresse IP

disallow = all =>Désactivation de tous les codecs

allow=ulaw => Activation du codec µlaw

call-limit = 1=>

### *II.3.2.2. Configuration du Dialplan (plan d'appel)*

**cd /etc/asterisk/**

**sudo nano extension.conf**

```
[CLIENT_IN]
exten => 801,1,dial(SIP/801,20)
exten => 800,1,dial(SIP/800,20)
exten => 801,2,Hangup()
exten => 800,2,Hangup()
```

**Figure II.14.**Configuration du extension.conf

[CLIENT_IN] même contexte que celui définit lors de la création des utilisateurs.dans lequel les utilisateurs faisant partis de ce contexte pourrons communiquer entre eux.

exten => instruction pour déclarer un numéro.

800 => Numéro de l'utilisateur

1 => la priorité de l'instruction.

Dial => application pour lancer l'appel

SIP => protocole utilisé

20 => Durée en seconde de l'application avant de passer à la priorité 2

Hangup =>application pour raccrocher

# II.4. Grandstream Wave Lite (GS Wave)

## II.4.1. Présentation

Grandstream Wave est une application de téléphone logiciel gratuite qui permet aux utilisateurs de passer et de recevoir des appels vocaux/vidéo via leurs comptes SIP professionnels ou résidentiels sur n'importe quel appareil Android™ (version 4.1+) de n'importe où dans le monde, via des données cellulaires ou WiFi. Cette application prend en charge l'intégration de jusqu'à 6 comptes SIP, la conférence vocale à 6 voies. Grandstream Wave prend également en charge les fonctionnalités avancées de téléphonie SIP, notamment le transfert d'appels, l'intégration du répertoire LDAP et plus encore. Avec Grandstream Wave, les utilisateurs professionnels et résidentiels ont toujours accès à leurs lignes SIP et peuvent facilement rester en contact avec leurs contacts professionnels ou personnels sans utiliser de forfaits de données cellulaires coûteux.

## II.4.2. Configuration

Pour configurer GS Wave, il suffit d'ajouter un <compte SIP> et de renseigner le numéro d'utilisateur SIP et l'adresse du serveur SIP et le mot de passe .

Après avoir lancé l'application, veuillez appuyer sur l'icône Paramètres dans le coin inférieur droit de l'application, comme indiqué par la capture d'écran ci-dessous :

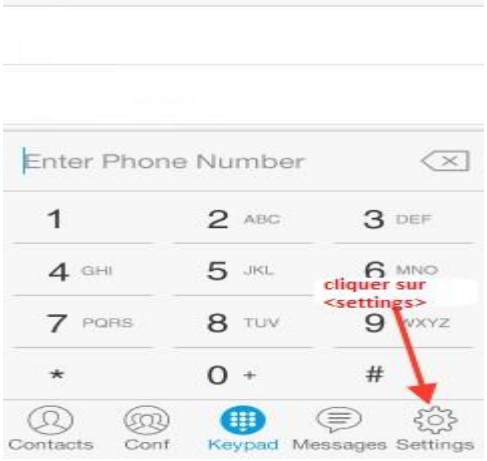


**Figure II.15.**Interface de l'application

Depuis l'écran Paramètres, appuyez sur l'option Paramètres du compte...

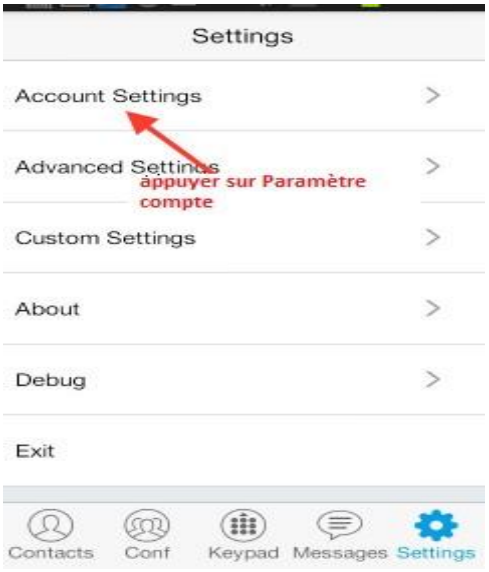


**Figure II.16.**Paramètre de GS Wave

... suivi de l'option + dans le coin supérieur droit de l'interface Paramètres des comptes, et enfin de l'option Comptes SIP pour configurer un nouveau profil SIP dans le softphone :


**Figure II.17.**Paramètre du compte

L'étape suivante est la configuration du compte, et pour que l'authentification soit possible, il faut avoir trois paramètres de configuration importante (SIP server, SIP User ID, Password).

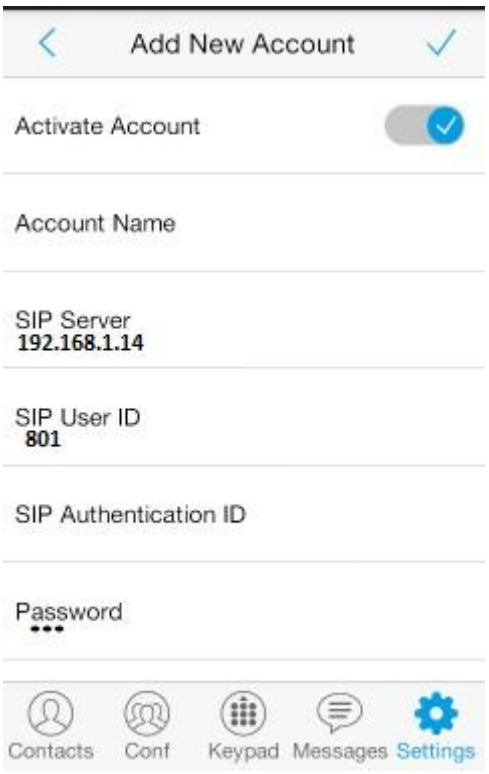


**Figure II.18**.Configuration du compte SIP

Pour vérifier si le compte d'utilisateur "801" est connecté avec le serveur SIP,

on utilise la commande SIP show peers :

```
arsriyad-VirtualBox*CLI> sip show peers
Name/username             Host                                  Dyn Forcerport Comedia    ACL Port     Status      Description
800/800                   (Unspecified)                          D  Yes        Yes           0        UNKNOWN
801/801                   192.168.1.5                            D  Yes        Yes           55767    OK (89 ms)
```

**Figure II.19.** Listes des comptes SIP

- **Résultat**: le compte SIP est enregistré sur le serveur SIP Asterisk

-**Test d'Appel :** Il nous faut 2 comptes SIP connectés avec le serveur Asterisk (utilisateur "800",utilisateur"801")

On lance un appel de l'utilisateur "801" vers l'utilisateur "800"


**Figure II.20** Lancement d'un appel

Finalement, l'appel a été effectué avec succès via le serveurs SIP Asterisk et c'est le but de ce chapitre .

## II.5. Test d'appel par l'application M-SIP

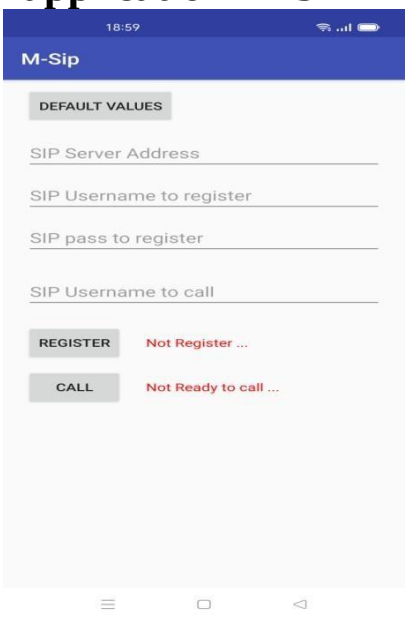


**Figure II.21.**Interface de M-SIP

Entrer manuellement les détails du compte SIP (SIP server adress, SIP user ,SIP pass) , ensuite cliquer sur "REGISTER" .


**Figure II.22**. Configuration de M-SIP

Quand l'authentification soit possible, entrer un numéro d'un autre utilisateur pour lancer l'appel

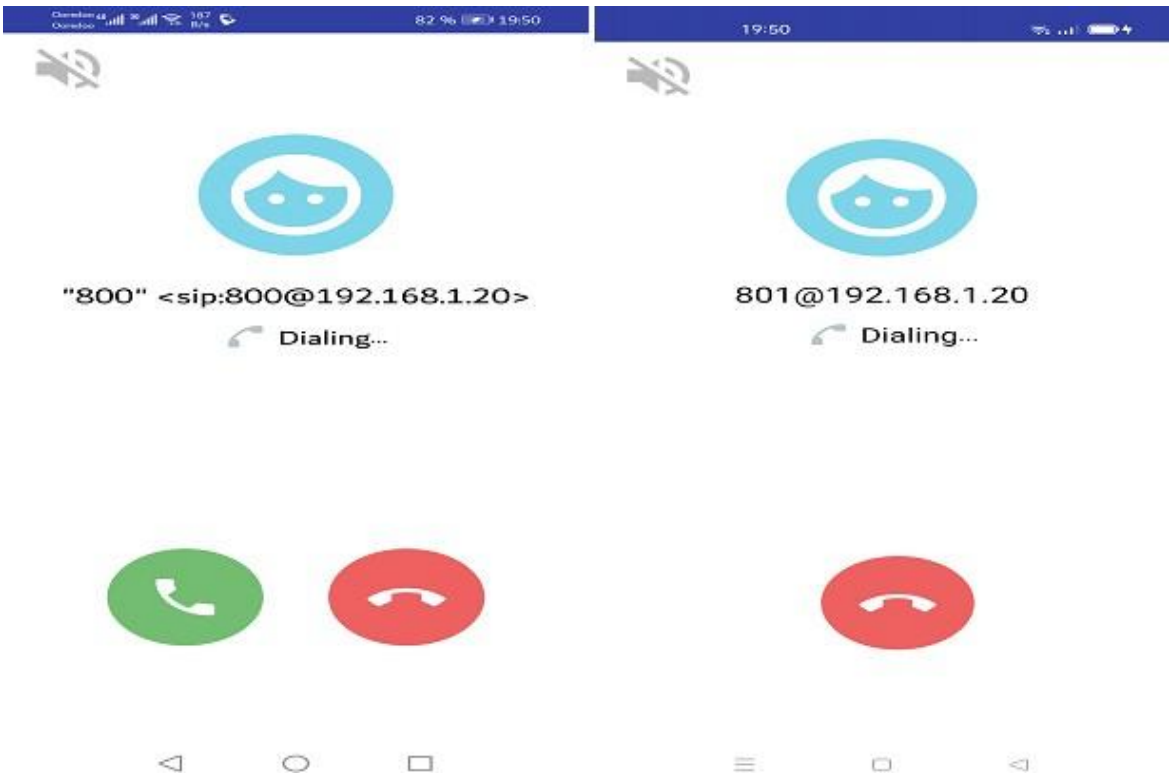


**Figure II.23**. Test d'appel

Le test d'appel est positif ,cela veut dire que toutes les applications SIP peuvent fonctionner sur le serveur SIP Asterisk .

## II.6. Quelques commandes utiles pour la console d'Asterisk

- sudo asterisk -rvvvvv => Pour se connecter à la console Asterisk
- reload => pour redémarer le serveur
- sip reload => pour relancer la configuration SIP
- sip show peers => Pour lister tous les comptes SIP
- sip show peer 801 => Pour lister les paramètres d'un compte SIP avec détails
- dialplan reload => Pour relancer la configuration du Dialplan (extensions.conf)
- dialplan show => pour visualiser le Dialplan
- core show channels => Pour voir les communications en cours
- core show channelstats => Pour observer la perte de paquets sur une communication

## II.7. Conclusion

Ce chapitre nous a permis d'enrichir nos connaissances dans différents domaines. Il nous a permis de nous familiariser avec la plate forme Linux, d'apprendre les configurations des outils Asterisk et de nous initier au domaine professionnel et aux nouvelles technologies du réseau internet . Cependant, en termes de sécurité, le créateur ou développeur doit faire attention à plusieurs types d'attaques contre ce type de serveurs. Dans le chapitre suivant, nous présenterons les principaux problèmes de sécurité liés à la VoIP.

# Chapitre III

# Vulnérabilités contre la voix sur IP et quelques moyens de sécurisation

# III.1. Introduction

Bien que la voix sur IP présente de nombreux avantages, elle présente également des inconvénients majeurs, dont la sécurité informatique. La téléphonie sur Internet étant basée sur un système informatique, les problèmes liés à la sécurité sont donc inévitables. Il existe deux principales classes de vulnérabilités sur un environnement VoIP. La première dépend des protocoles utilisés (SIP, H.323…) et la deuxième est reliée aux systèmes sur lesquels les éléments VoIP sont implémentés.

Dans ce chapitre, nous allons décrire quelques attaques majeures qui menacent cette technologie VoIP, et nous détaillerons quelques-unes.

# III.2. Les attaques protocolaires

Les attaques les plus fréquentes contre le système VoIP sont :

## III.2.1. Déni de service

Le déni de service, le nom anglais "Denial of Service" ou encore DOS, est une attaque conçue pour rendre les services ou les ressources d'une organisation indisponibles pendant une période de temps. Habituellement, ce type d'attaque est effectué sur les machines, les serveurs et les accès de l'entreprise, de sorte que les clients ne peuvent pas y accéder.

Cela touche 99% de la planète car la plupart des dénis de service exploitent des failles liées au protocole TCP/IP. Son principe est d'envoyer des paquets ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des équipements victimes et de les empêcher ainsi d'assurer les services réseau qu'elles sont censés offrir, Une attaque de type DoS peut s'effectuer à plusieurs niveaux, soit :

**A la couche réseau grâce à des fragmentations des paquets :** il est possible de rendre hors service de nombreux systèmes d'exploitation et dispositif VoIP par le biais de la consommation des ressources.

**A la couche transport**: on a plusieurs types d'attaques dans cette couche, par exemple, on a L'UDP flooding, son principe est d'envoyer un grand nombre de requêtes UDP vers une machine. Le trafic UDP étant prioritaire sur le trafic TCP, ce type d'attaque peut vite troubler et saturer le trafic transitant sur le réseau et donc permet de perturber la bande passante. Presque tous les dispositifs utilisant le protocole SIP fonctionnent au-dessus du protocole UDP, ce qui en fait d'elles des cibles.

## III.2.2. Le sniffer (sniffing)

Un sniffer est un programme qui permet de capturer tous les paquets circulant sur un réseau et qui permet d'éditer leurs contenus**.** Il peut capturer n'importe quelle information

envoyée à travers un réseau local**,** et donc afficher aussi bien l'identité des utilisateurs que leurs mots de passe transmis par tout service transportant des données claires (non chiffrées).

### III.2.3. Suivi des appels

Appelé aussi Call tracking, cette attaque se fait au niveau du réseau LAN/VPN et cible les terminaux (soft/hard phone). Elle a pour but de connaître l'appelant qui est entrain de communiquer et quelle est la période de la communication. Pour réaliser cette attaque, l'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE.

### III.2.4. Compromission de serveurs

Les serveurs jouent un rôle important dans une solution de voix sur IP, et même s'il n'est pas forcement possible d'intercepter un appel si un serveur est compromis, il est souvent possible de récupérer des CDRs (Call Detail Records) qui contiennent toutes les traces des appels effectués. En revanche la compromission d'une passerelle entre le réseau VoIP et le réseau téléphonique classique permet d'écouter de manière transparente les appels, même s'ils sont chiffrés du côté VoIP (SRTP).

## III.3. Les attaques sur les couches basses

### III.3.1. Arp redirect (ou spoofing)

L'attaque ARP redirect vise les réseaux locaux Ethernet, qu'ils soient partitionnés ou non en sous-réseaux (switchés).

D'abord , pour rappel, le protocole ARP utilise l'adresse IP d'un hôte connu pour lui demander quelle est son adresse MAC. Ainsi ARP utilise une série de requêtes en broadcast puis écrit le résultat obtenu dans son cache ARP.

Cette technique de spoofing consiste à s'attribuer l'adresse IP de la machine cible, c'est-à-dire à faire correspondre son adresse IP à l'adresse MAC de la machine pirate dans les tables ARP des machines du réseau. Pour cela il suffit en fait d'envoyer régulièrement des paquets ARP_reply en broadcast, contenant l'adresse IP cible et la fausse adresse MAC. Cela a pour effet de modifier les tables dynamiques de toutes les machines du réseau (routeurs compris). Celles-ci enverront donc leur trames Ethernet à la machine pirate tout en croyant

communiqueré avec la cible, et ce de façon transparente pour les switches d'où la notion de redirection grâce au protocole ARP (ARP redirect).

### III.3.2. Attaque de l'homme du milieu

Les attaques du type "l'homme du milieu" est la traduction "man in the middle attack" en anglais , L'objectif du pirate dans ce type d'attaque consiste à se faire passer pour le client auprès du serveur et à usurper l'identité du serveur auprès du client. Devenant ainsi "l'homme du milieu", le pirate espionne les communications entre le client et le serveur dans le but de collecter des données en les modifiant ou non durant leur transmission.

Pour instaurer une attaque "man in the middle" via Internet, le pirate doit être en mesure d'observer les deux parties en présence. Il lui faut pour cela connaître les adresses IP du client (l'internaute) et du serveur (le site Internet) [21].

## III.4. Les vulnérabilités de l'infrastructure

### III.4.1. INFRASTRUCTURE HARDWARE

#### *III.4.1.1. les téléphone IP*

Un attaquant peut pirater un appareil téléphonique VoIP, tel qu'un téléphone IP, un Smartphone ou tout autre logiciel ou appareil client.

Habituellement, il obtient les privilèges qui lui permettent d'avoir un contrôle total sur les fonctions de l'appareil.

Un point de terminaison (téléphone IP) peut être piraté à distance ou via un accès physique à l'appareil.

Un hacker peut modifier les aspects opérationnels d'un tel appareil :

- La pile du système d'exploitation peut être modifiée pour masquer la présence de l'attaquant .
- Un Firmeware modifié de manière malveillante peut avoir été téléchargé et installé. Les modifications apportées faites à la configuration des logiciels de téléphonie IP peuvent permettre :

  - ✓ De renvoyer les appels entrants vers un autre terminal à l'insu de l'utilisateur ;
  - ✓ De surveiller les appels ;

- ✓ A l'information de la signalisation et les paquets contenant de la voix d'être acheminés vers un autre dispositif et également d'être enregistrés et modifiés.

#### III.4.1.2. LE SERVEUR VoIP

Un autre élément de réseau vulnérable est le serveur du fournisseur de réseau de téléphonie IP, qui peut être la cible d'attaques visant à compromettre l'ensemble du réseau.

Si un serveur de signalisation est compromis par un attaquant, il peut contrôler entièrement l'information de signalisation pour différents appels, ce qui permettra à l'attaquant de modifier tout paramètre lié à l'appel. Il est à noter que le serveur de téléphonie VoIP est installé sur un système d'exploitation, il peut donc être la cible de virus, de vers ou de tout code malveillant.

### III.4.2. INFRASTRUCTURE SOFTWARE

L'une des faiblesses majeures du système d'exploitation est un débordement de tampon qui permet aux attaquants de prendre le contrôle partiel ou total de l'appareil.

Ce n'est pas la seule vulnérabilité et elle varie selon le fabricant et la version du système d'exploitation. Ces attaques ciblant le système d'exploitation sont souvent liées à un manque de sécurité au stade initial de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit. Les appareils VoIP comme les téléphones IP, les gestionnaires d'appels, les passerelles, les serveurs proxy... héritent des mêmes vulnérabilités du système d'exploitation ou du micrologiciel sur lequel ils s'exécutent.

On en conclura que l'application VoIP est faible une fois que le système d'exploitation sur lequel elle s'exécute est piraté.

## III.5. Les dispositifs de sécurité

- Développer des procédures de sécurité et installer des dispositifs contre le phishing.
- Activer toutes les fonctions disponibles sur le réseau VoIP pour crypter et authentifier les appels afin d'empêcher les accès illégaux et de maintenir la confidentialité des conversations.

- Pour assurer la sécurité des équipements, utilisez une architecture conforme aux normes liées aux technologies sans fil de dernière génération : WPA ou WPA2 par exemple.
- Le pare-feu doit être suffisamment puissant pour défendre le réseau VoIP contre les attaques et analyses externes. Choisir le bon appareil pour le trafic peut rapidement détecter les appels suspects et identifier les signes d'une menace. La configuration peut être effectuée de manière à ce que les administrateurs réseau soient immédiatement alertés lorsqu'une demande de connexion suspecte arrive sur le réseau.
- N'utilisez jamais les mots de passe "par défaut" proposés par le système de téléphonie IP et changez-les toujours.
- Mettez régulièrement à jour les technologies antivirus et anti-spam pour tous les équipements de réseau VoIP.
- Découvrez les méthodes couramment utilisées par les hackers.
- Gardez un œil attentif sur tous les événements inhabituels sur le réseau VoIP

## III.6. Les protocoles de sécurité

Sans cryptage des appels, toutes les informations sensibles sont susceptibles d'être dévoilées. Aujourd'hui, il est très important de crypter les données et les voix des appels VoIP.

### III.6.1. IPsec

IP Security est un protocole qui vise à sécuriser les échanges de données au niveau de la couche réseau. Il repose sur deux mécanismes. Le premier, AH, est pour l'authentification d'en-tête visant à Assurer l'intégrité et la fiabilité des datagrammes IP. En revanche, il n'offre aucune Confidentialité : les données fournies et transmises par ce « protocole » ne sont pas cryptées. Le second, Esp, pour encapsuler la Security Payload peut également permettre l'authentification, mais, il est principalement utilisé pour crypter des informations.
Que ces deux mécanismes indépendants sont toujours utilisés ensemble.

## III.6.2. TLS

### *III.6.2.1. Présentation du TLS*

Transport Layer Security (TLS) est un protocole standard de l'Internet Engineering Task Force (IETF) qui assure l'authentification, la confidentialité et l'intégrité des données entre deux applications informatiques communicantes. Il s'agit du protocole de sécurité le plus largement utilisé actuellement et il est le mieux adapté aux navigateurs Web et autres applications qui nécessitent l'échange sécurisé de données sur un réseau. Cela inclut les sessions de navigation Web, les transferts de fichiers, les connexions de réseau privé virtuel (VPN), les sessions de bureau à distance et la voix sur IP (VoIP). Le protocole TLS est subdivisé en quatre sous protocoles Handshake protocol, Change Cipher Spec Protocol, Alarm Protocol, Record Protocol.

### *III.6.2.2. Handshake protocol*

Il permet au serveur et au client de s'authentifier entre eux, puis de négocier un algorithme de chiffrement et une clé cryptographique avant que l'application ne transmette les données.

- **Fonctionnement**

**-Etablissement de la liaison**

Le client lance la communication avec le serveur en envoyant un message SYN (Synchronize). Le serveur accepte la communication en envoyant un message SYN-ACK (synchronize-acknowledgment). Enfin, le client informe le serveur de la bonne réception du message reçu en envoyant un ACK (acknowledgment).

**-La négociation**

Le client envoie le message HELLO_CLIENT en clair au serveur contenant la version de TLS, un message aléatoire pour la signature des données, un identifiant de session, une liste des suites d'algorithmes cryptographiques supportés par le client par ordre décroissant de préférence .

Le serveur répond au client avec un message HELLO_SERVER. Si les information envoyé par le client ne sont pas disponibles côté serveur, la communication s'interrompt.

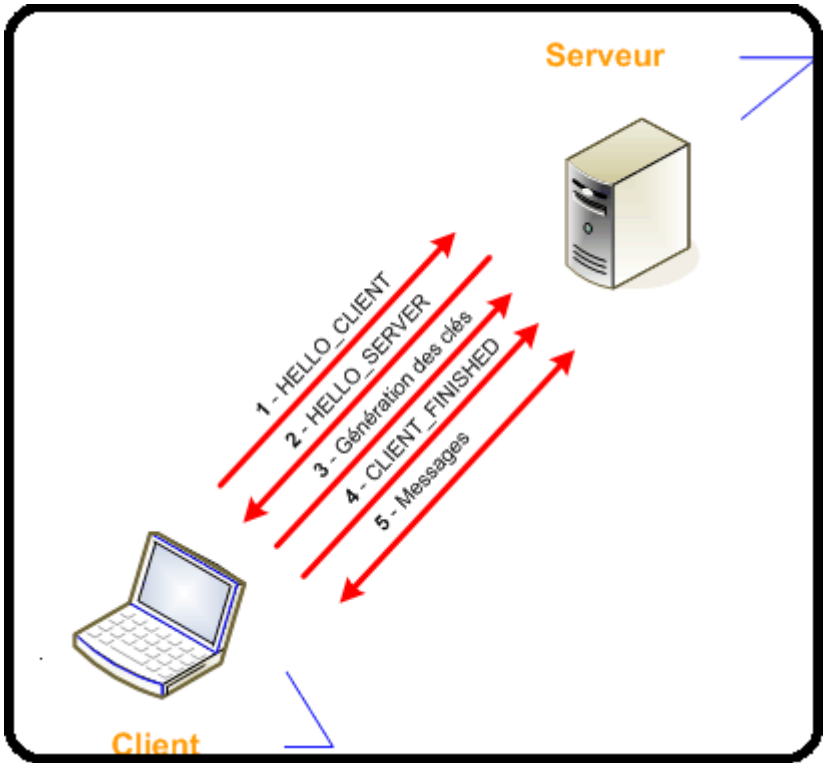


Figure III.1. :Négociation client/serveur

**-Authentification du serveur**:

Une fois les algorithmes négociés, le serveur s'authentifie auprès du client en envoyant son certificat X.509 (message certificate).En option, le serveur envoie également sa clé publique (différente de la clé publique du certificat serveur) au client pour chiffrer la clé de session (Server Key Exchange). En fonction de la configuration du serveur, il envoie le message Client Certificate Request afin de demander au client son propre certificat.Le client vérifie le format du certificat, sa date d'expiration, son statut révoqué ou non et si le certificat est de confiance. La chaine d'autorité du certificat serveur doit pour cela être embarquée dans le magasin de confiance du client. Si au moins une de ces vérifications échoue, la transaction est abandonnée.Enfin, le serveur envoie le message Server Hello Done pour indiquer qu'il a terminé.

-Authentification du client et génération de la clé de session

Le client envoie son propre certificat au serveur (Client Certificate), si demandé. Le serveur procède aux mêmes vérifications que celles faites par le client (voir point 3) sur le certificat serveur.Le client produit un secret pré-maître (pre-master key) qu'il chiffre avec la

clé publique du certificat serveur. Si le serveur a envoyé Server Key Exchange, cette clé chiffrée est chiffrée à nouveau avec la clé publique du serveur. Le message Client Key Exchange envoie le résultat au serveur. Ce secret permet par la suite au client et au serveur de générer des clés de sessions non échangées.Si le client a envoyé son certificat, il envoie aussi le message Certificate Verify, contenant l'empreinte de tous les messages précédents signés avec la clé privée du client. Ce message permet de prouver que le client possède bien la clé privée associée à son certificat.

**-Fin du Handshake TLS**

Le client envoie deux messages Change Cipher Spec et Finished chiffrés et signés avec les clés vues précédemment pour indiquer que le tunnel TLS s'est établi. Le serveur fait de même, c'est la fin du Handshake.

A partir de ce moment, le client et le serveur communiquent en suivant les spécifications du protocole Record, en garantissant la confidentialité et l'intégrité de tous les messages échangés.

### *III.6.2.3. Change Cipher Spec Protocol*

Ce protocole contient un seul message : change_cipher_spec. Il est envoyé par les deux parties à la fin du protocole de négociation. Ce message transite chiffré par l'algorithme symétrique précédemment négocié.

### *III.6.2.4. Alarm protocol*

Ce protocole spécifie les messages d'erreur que peuvent s'envoyer clients et serveurs. Les messages sont composés de deux octets. Le premier est soit warning soit fatal. Si le niveau est fatal, la connexion est abandonnée. Les autres connexions sur la même session ne sont pas coupées mais on ne peut pas en établir de nouvelles. Le deuxième octet donne le code d'erreur.

**-Les erreurs fatales sont** :

Unexpected_message – indique que le message n'a pas été reconnu

Bad_record_mac – signale une signature MAC incorrecte

Decompression_failure – indique que la fonction de décompression a reçu une mauvaise entrée

Handshake_failure – impossible de négocier les bons paramètres

Illegal_parameter – indique un champ mal formaté ou ne correspondant à rien.

**-Les warnings sont :**

Close_notify – annonce la fin d'une connexion

No_certificate – répond une demande de certificat s'il n'y en a pas

Bad_certificate – le certificat reçu n'est pas bon (par exemple, sa signature n'est pas valide)

Unsupported_certificate – le certificat reçu n'est pas reconnu

Certificate_revoked – certificat révoqué par l'émetteur

Certificate_expired – certificat expiré

Certificate_unknown – pour tout problème concernant les certificats et non listé ci-dessus[22].

## III.7. Conclusion

La voix sur IP est de plus en plus ciblée jour après jour. Il existe plusieurs d'autres attaques qui menacent la sécurité de la VoIP. Les attaques citées dans ce chapitre sont les plus connues et les plus courantes dans les réseaux VoIP, Donc, les entreprises qui décident d'adopter cette technologie doivent le faire prudemment, en mettant le facteur sécurité au premier plan.En suivant certaines mesures parmi celles mentionnées dans ce chapitre, on peut créer un réseau fiable et sécurisé.

# Conclusion générale

En bref, la VoIP est une technologie révolutionnaire qui défie les règles établies par la téléphonie RTC. Elle est plus flexible, simple d'utilisation, ne nécessite pas d'investissement important, coûte moins cher, offre de nouveaux services et bien d'autres avantages pour que toute entreprise qui se veut compétitive et moderne aujourd'hui ait le cap sur la téléphonie sur IP pour gérer les connexions internes et externes. Elle vise principalement à améliorer l'environnement de travail des employés de l'entreprise en libérant l'utilisateur de la localisation de l'appareil téléphonique.

Notre objectif de ce projet c'est d'apprendre comment installer et configurer la solution voIP basé sur Asterisk ,avec l'étude des failles de sécurité existant et leurs solution.

Nous avons constaté que la sécurité complète de notre solution est presque impossible. La sécurité VoIP est un sujet très important qui présente des problèmes difficiles pour qu'elle résoudre. Avec l'intégration de la téléphonie dans les systèmes d'information et dans le monde des réseaux IP, la sécurisation de cette application devient particulièrement compliquée.

La question n'est donc pas de savoir si la sécurité est nécessaire, mais comment créer une solution robuste et interopérable avec les infrastructures existantes. Chaque jour, la cybercriminalité nous rappelle que la sécurité n'est plus une option mais une obligation.

Comme perspectif il reste encore des défis à surmonter nous envisageons de considérer d'autres solutions de sécurité, et nous devons apprendre comment les appliquer pour sécuriser encore plus notre serveur, et aussi de prendre en compte la technologie IAX qui permet l'interconnexion entre serveurs Asterisk. Et aussi nous devons assimiler la création d'une interface graphique d'Asterisk qui permet à l'utilisateur de configurer le serveur plus simplement.

# Référence bibliographique

[1] MICOLINI, Orlando et HERRERA, Augusto. Traffic analysis over a VoIP server. IEEE Latin America Transactions, 2013.

**[2]** MAHLER, Paul. VoIP Telephony with Asterisk. Signate, 2005, **consulter le 01/05/2021.**

**[3]** Wazo, IPBX et PABX, https://wazo.io/guide-voip-webrtc/ipbx/pabx-definition/ **consulter le 03/05/2021**

[4] Yani KalombaYannick. *Etude et mise au point d'un systeme de communication VOIP,*Mémoire de Master 2 en réseaux et télécoms, Université protestante de Lubumbashi, Congo, 2009.

[5] BASSIROU KASSE. *Etude et mise en place d'un système de communication de VOIP,* Mémoire de Master II professionnel, Système d'informations réparties, Université Cheikh Anta Diop de Dakar, 2011.

[6] aircal.io, Les avantage de la téléphonieVoIP, **Clémentine Robine** 22 octobre 2019,

https://aircall.io/fr/blog/centre-dappels/les-avantages-de-la-telephonie-voip-pour-votre-entreprise/.

[7] Frameip.com, VoIP ,https://www.frameip.com/voip/#4-8211-les-avantages-de-la-voip, **consulter le 10/05/2021.**

[8] MONTORO, Pablo et CASILARI, Eduardo. A comparative study of VoIP standards with asterisk. In : 2009 Fourth International Conference on Digital Telecommunications. IEEE, 2009.

**[9]** programmerworld.net, QUE SONT LES AVANTAGES ET INCONVÉNIENTS DE VOIP ?, https://faq.programmerworld.net/lang/fr/voip/voip-advantages-disadvantages.htm, **consulter le 11/05/2021.**

**[10]** www.slideshare.net, Presentation VoIP, https://www.slideshare.net/Cynapsys/formation-voip?next_slideshow=1 **consulter le 11/05/2021**

[11] https://www.slideshare.net/jouhaaa/architecture-voip-protocol-h323-

[12] François Goffinet, Architecture SIP, [En ligne], https://sip.goffinet.org/sip/architecture/ , **consulter le 20/05/2021.**

**[13]** http://www.efort.com/r_tutoriels/SIP_EFORT.pdf?fbclid=IwAR3W1rnw7_o5GOd4HE0QIdU8thS3rpM2TdpPvFhm0jlw0FuEuWt9vtb0dec **consulter le 20/05/2021**

[14] https://www.beip.be/wp-content/uploads/2020/02/01189-rostom-white-paper-WEB.pdf

[15] EL ALLIA, Moourad , Developpement d'un environnement de communication multimedia sur internet, Ecole de technologie superieure université de Québec, Montréal, 22 octobre 2002.

**[16]** WIKI, Protocole de transport en temp réel, [En ligne] https://fr.xcv.wiki/wiki/Real-time_Transport_Protocol. **consulter le 26/05/2021**

**[17]** CLOUDFLARE, qu'est ce que l'ICMP, https://www.cloudflare.com/fr-fr/learning/ddos/glossary/internet-control-message-protocol-icmp/ , **consulter le 17/05/2021.**

**[18]** igm,Xposé système 2005, http://igm.univ-mlv.fr/~dr/XPOSE2005/mmancel/asterisk.html, **consulter le 17/05/2021**

[19] BENISSE, Mohamed Taib, *TRANSMISSION MÉDIA SUR LES RÉSEAUX IP EN UTILISANT LES PROTOCOLES SIP ET IAX* , Mémoire en RÉSEAUX DE TÉLÉCOMMUNICATION, ÉCOLE DE TECHNOLOGIE SUPÉRIEURE UNIVERSITÉ DU QUÉBEC, MONTRÉAL,2009.

[20] IMRAN, Ale, QADEER, Mohammed A., et KHAN, M. J. R. Asterisk VoIP private branch exchange. In : 2009 International Multimedia, Signal Processing and Communication Technologies. IEEE, 2009. p. 217-220.

[21] Sécurité info , L'attaque ARP redirect ,https://www.securiteinfo.com/attaques/hacking/arpredirect.shtml , **consulter le 18/05/2021.**

**[22]** Frameip, PROTOCOLE SSL ET TLS , https://www.frameip.com/ssl-tls/ , **consulter le 19/05/2021.**