République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri de Tizi-Ouzou

Faculté De Génie Electrique et d'Informatique
Département de Télécommunications

Mémoire de Fin d'Etudes de

MASTER ACADEMIQUE

Spécialité :

Réseaux & Télécommunications

Filière :

Télécommunications

Par
BAILECHE Amine
ABROUS Malha

Thème

MISE EN PLACE D'UNE INFRASTRUCTURE VoIP AVEC ASTERISK

Soutenu le : 30/09/2024

Devant le jury :

Président :	Mme. ABBA Faiza	Grade	MCB	UMMTO
Promoteur :	Mr. AMIR Mounir	Grade	MCA	UMMTO
Co-promoteur :	Mr. OUADAH Mohammed Chamse Eddine	Grade	MCA	UMMTO
Examinateurs :	Mr. HEDIR Abdellah	Grade	MCA	UMMTO

Remerciements

À la fin de ce mémoire, on souhaiterait exprimer notre reconnaissance et gratitude à Dieu le tout-puissant, pour nous avoir accorder la santé, la force, et la capacité de mener à bien ce travail.

الحمد لله On tient à remercier, tout particulièrement notre encadrant **Mr. Amir Mounir**, **Mohammed Chamse Eddine** pour nous avoir suivi et bien conseillé tout au long de la réalisation de ce mémoire. On le remercie pour la qualité de son encadrement exceptionnel. Son enthousiasme et son engagement envers notre réussite ont été une source d'inspiration tout au long de ce processus. Nos remerciements les plus sincères vont à tous nos professeurs pour leur générosité et la grande patience dont ils ont fait preuve. Nos vifs remerciements s'adressent aussi aux membres du jury, pour avoir pris le temps d'écouter notre présentation, et d'avoir accepté de juger notre présent travail.

Dédicace

Je dédie ce travail, signe de mon immense gratitude et mon plus grand respect aux deux personnes les plus importantes de ma vie : Mes très chers parents. Je souhaiterais remercier mes parents du fond du cœur pour leur amour inconditionnel, leur soutien infaillible, leur encouragement durant ces longues années d'études, leur confiance et patience, et leur sacrifice infini. Je souhaiterais vous dire papa, maman, que ma réussite aujourd'hui et pour vous et, surtout grâce à vous.

À mes très chers sœurs, ALECIA, DALIA, DJOUHER, LYDIA et ma tata ATHENIA Qui ont toujours été là pour moi, qui m'ont soutenu dans les hauts et les bas, et sur qui je sais que je pourrai toujours compter.

À la mémoire de ma chère grand-mère JIDA Dahbia et mon oncle d'amour DADA Moh paix à leurs âmes. Même s'ils ne sont plus parmi nous, je tiens à dire qu'ils vivront à jamais dans mon cœur et que c'est aussi grâce à leurs prières et bénédictions que je suis arrivée là où je suis aujourd'hui. À tous les membres de ma famille, À tous mes amis, Et tous ceux qui m'aiment.

MALHA

Dedicace

Avec l'expression de ma reconnaissance, Je dédie ce travail marquant de ma vie a ceux qui, quel que soient les termes embrassés, je n'arriverai jamais a leur exprimer mon amour et ma gratitude les plus sincères.

A la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non âmes et exigences, et qui n'a epargner aucun effort pour me sentir heureux et en toute securité : mon adorable mère

A l'homme, qui doit ma vie,celui qui a combattu toute sa vie pour me procurer tout ce d'ont j'avais besoin, celui qui m'a soutenu tout au long de mon parcours et qui était toujours un très bon exemple pour moi : Mon cher Père.

A mes sœurs katia et tinhinane.

A mon grand-père mahammed.

A mes amis : hakim chikhi, ferhat lebir, samir laziz, massinissa haddad, aissa difellah, yidir yamouten.

A mes amies : tafat challal, tannina challal.

A toutes les personnes qui, de près ou de loin, m'ont aidé à la réalisation de ce travail.

A tous mes enseignants de l'université Mouloud Mammeri de Tizi-Ouzou.

AMINE

Table des Matières

CHAPITRE II : Attaques contre la VoIP et bonnes pratiques de sécurisation

Chapitre III : installation et configuration d'asterisk pour la voip

Liste des abréviations

AGI: Asterisk Gateway Interface

AMI: Asterisk Manager Interface

API :Application Programming Interface

GPL: General Public Licence

HTTP: Hyper Text Transfer Protocol

IP: Internet Protocol

IPBX: Internet Protocol Private Branch eXchange

MCU: Multipoint control unité

PABX: Private Automatic Branch eXchange

RTC: Réseau Téléphonique Commuté

RTP: Real Time Transport Protocol

RTCP:Réseau Téléphonique Commuté Protocol

SIP: Session Initial Protocol

TCP: Transmission Control Protocol

UDP: Utilisateur Datagramme Protocol.

VOIP: Voice Over IP

WAN: Wide Aera Network

Liste des figures

Liste des tableaux

Résumé

La VoIP (Voice over IP) transforme les télécommunications en offrant une alternative moderne et économique aux systèmes traditionnels. S'appuyant sur les reseaux IP via internet et des protocole- IP comme SIP et RTP, elle favorise l'intégration de services numériques tels que la visioconférenc- Bien que flexible, la VoIP présente des vulnérabilités, nécessitant des mesures de sécuri appropriées. L'utilisation d'Asterisk sur Linux Ubuntu, associée au softphone Linphone, perm aux entreprises de déployer un système VoIP personnalisé et sécurisé. Une configuration adéquate d'Asterisk est essentielle pour garantir la qualité et la sécurité des communications, facilitant ainsi la collaboration dans un environnement numérique dynamique.
MOTS CLES: [**VIOP, PROTOCOLE IP, SIP, RTP, authentication asterisk, Codec Audio]**

Abstract

VoIP (Voice over IP) is transforming telecommunications by offering a modern and cost-effective alternative to traditional systems. Based on IP networks via the Internet and IP protocols such as SIP and RTP, it promotes the integration of digital services such as videoconferencing. Although flexible, VoIP has vulnerabilities, requiring appropriate security measures. The use of Asterisk on Linux Ubuntu, combined with the Linphone softphone, allows companies to deploy a personalized and secure VoIP system. Proper configuration of Asterisk is essential to ensure the quality and security of communications, facilitating collaboration in a dynamic digital environment.
KEYWORDS: [**VIOP, PROTOCOL IP, SIP, RTP, authentication, asterisk, Audio Codec].**

على إحداث تحول في الاتصالات من خلال تقديم بديل حديث واقتصادي للأنظمة VoIP (Voice over IP) تعمل تقنية ، فإنه يعزز تكامل الخدمات الرقمية مثل RTPو SIP مثل IP عبر الإنترنت وبروتوكولات IP التقليدية. بالاعتماد على شبكات بها نقاط ضعف، مما يتطلب اتخاذ تدابير أمنية مناسبة. يتيح استخدام VoIP مؤتمرات الفيديو. على الرغم من مرونتها، فإن مخصص VoIP الإلكتروني، للشركات نشر نظام Linphone ، جنبًا إلى جنب مع هاتفLinux Ubuntu على Asterisk .أمرًا ضروريًا لضمان جودة وأمن الاتصالات، وتسهيل التعاون في بيئة رقمية ديناميكية Asterisk وآمن. يعد التكوين الصحيح لـ
مفاتيح الكلمات : [، المصادقة، العلامة النجمية، برنامج ترميز الصوتRTP، SIP، IP PROTOCOL، VIOP]

Depuis quelques années, les entreprises, en particulier celles de service telles que les centres d'appels, commencent à être attirées par la technologie VoIP. Il n'est pas inutile que les entreprises migrent vers ce type de technologie. Le principal objectif est de réduire les dépenses liées aux communications, d'utiliser le même réseau pour proposer des services de données, de voix et d'images, et d'améliorer les coûts de configuration et d'assistance **[1].**

Différents fournisseurs proposent différentes solutions qui facilitent la transition des entreprises vers le domaine IP.Selon Nortel, Siemens et Alcatel, certains fabricants de PABX privilégient l'intégration progressive de la VoIP en intégrant des cartes extensions IP.

Cette méthode simplifie l'adoption du téléphone IP, en particulier dans les grandes entreprises qui utilisent une plateforme traditionnelle et souhaitent profiter de la voix sur IP. Cependant, cela ne vous donne pas accès à tous les services et à une intégration optimale dans le domaine des données [2].

La solution proposée par des fournisseurs tels que Asterisk consiste à développer des logiciels PABX. Cette méthode offre une grande souplesse, une excellente intégration dans le domaine des données et de la voix, et surtout un prix beaucoup plus attractif **[3].**

Les vulnérabilités de cette solution, qui repose entièrement sur la technologie IP, mettent ainsi en péril la sécurité de ce protocole et de l'infrastructure réseau sur laquelle elle est déployée. Le problème principal pour les entreprises et un défi majeur pour les développeurs réside dans cette dernière. Les entreprises peuvent subir des pertes catastrophiques et énormes en raison de certaines attaques sur les réseaux VoIP, telles que les attaques de déni de service et les vols d'identité **[4].**

Ainsi, la sécurité du réseau VoIP ne se limite pas à une nécessité, mais devient une obligation, afin de minimiser au maximum le risque d'attaques sur les réseaux VoIP **[5].**

Toute l'infrastructure réseau doit être sécurisée pour une solution de VoIP, y compris les outils et les équipements de gestion des communications et des utilisateurs, le système d'exploitation sur lequel ces outils sont installés, **[6]**

Ainsi que les protocoles de signalisation et de communication. Le protocole H.323 offre un cadre pour les échanges audio, vidéo et de données sur les réseaux IP. L'ITU (International Telecommunications Union) l'a créé pour les réseaux qui ne veulent pas assurer une qualité de service (QoS), comme IP IPX sur Ethernet, Fast Ethernet et Token Ring. Il est disponible dans plus de 30 produits et couvre les domaines du contrôle des appels, de la gestion multimédia et de la gestion de la bande passante pour les conférences point-à-point et multipoints. L'interfaçage entre

le LAN et les autres réseaux est également abordé dans H.323. L'un des protocoles de signalisation les plus renommés est H.323.

Transport d'informations. Il est même nécessaire de se prémunir contre les individus malveillants. L'amélioration de la sécurité réduit les risques.

Ce mémoire est divisé en trois chapitres distincts.

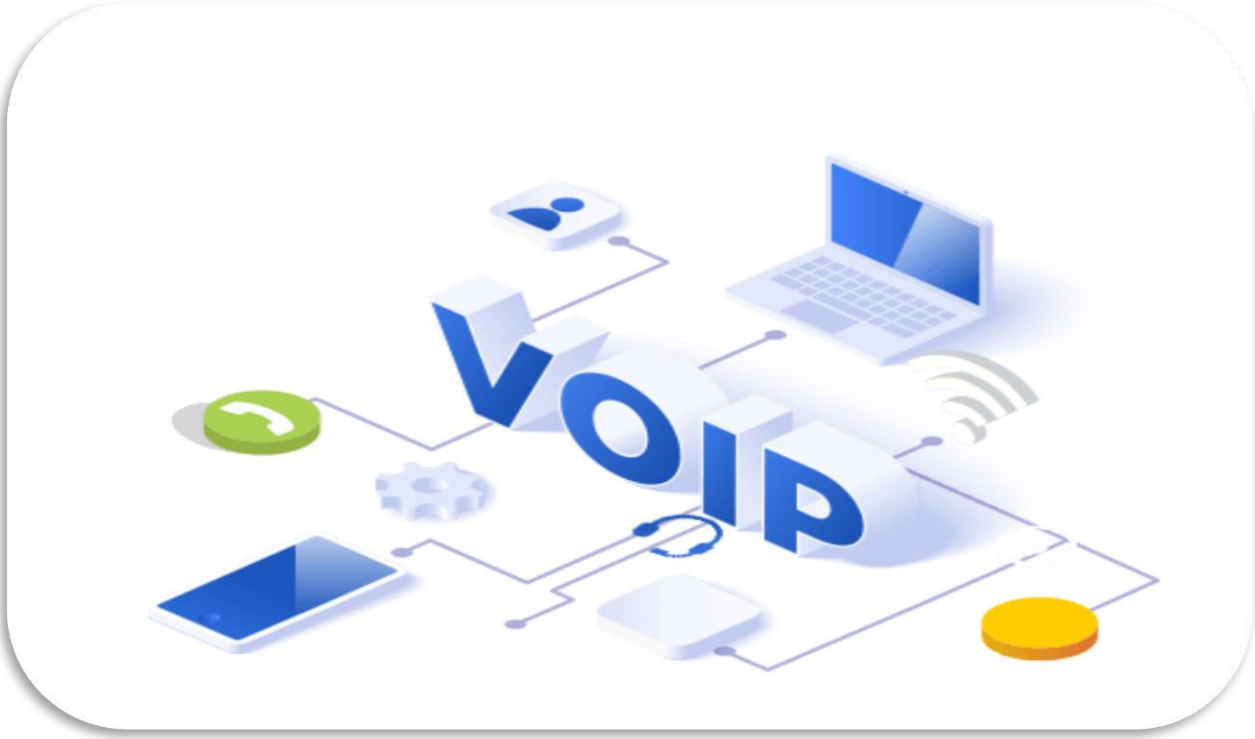
• Dans le chapitre initial, on présente la voix sur IP et ses composants, on décrit et explique son architecture et ses protocoles, et on énumére les principaux atouts de cette technologie ainsi que ses points faibles.

• Le chapitre suivant se concentre sur la protection des infrastructures de Voix sur IP. Il explique en détail les diverses catégories de vulnérabilités de sécurité On définit également les bonnes pratiques et les mesures de sécurité à mettre en œuvre pour guérir ces vulnérabilités.

• Chapitre Trois : Création d'une solution VoIP sécurisée.

L'objectif de ce chapitre est d'expliquer comment installer et configurer une solution VoIP en utilisant le serveur Asterisk sur linux ubuntu et le client linphone. Il présente les conditions préalables, les outils requis et les étapes de configuration indispensables afin de mettre en place une plateforme VoIP sécurisée pour les entreprises.

Chapitre I
La Voix Sur IP



Généralités sur la Voix sur IP

Introduction

La voix sur le protocole Internet (IP) est un sujet très vaste et très enrichissant. Dans un premier temps, il est important de définir les concepts dissimulés derrière le terme générique « VoIP » (Voice Over IP).

La "VoIP", également connue sous le nom de "voix sur IP" en français, fait référence à toutes les technologies qui permettent de communiquer de manière orale à travers un réseau utilisant le protocole IP. En général, le mot "VoIP" est employé pour désigner des communications "Point à Point". On parle plutôt de streaming pour la diffusion de son sur IP en multipoints (comme les radios en ligne, par exemple) **[7].**

- IP (Internet Protocol)

Un protocole de communication de réseau informatique, appelé Internet Protocol, est un protocole de niveau 3 dans le modèle OSI et le modèle TCP/IP (Figure 1), qui offre un service d'adressage unique pour tous les terminaux connectés.

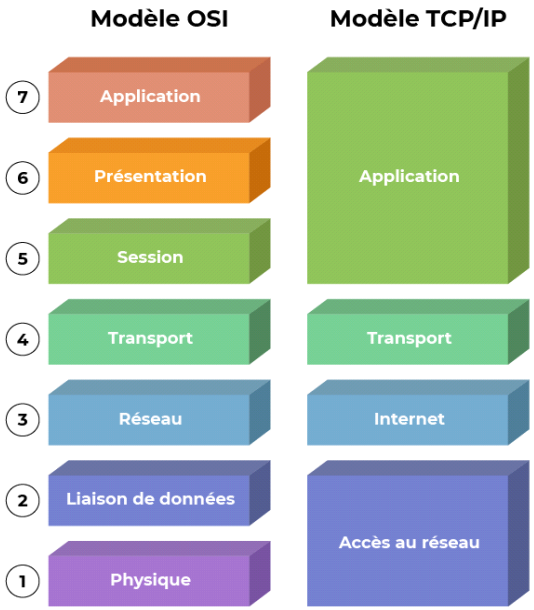


Figure I.1 : Modèle OSI (Open Systems Interconnection) et du modèle TCP/IP **[8].**

I.1.Historique

La VoIP (Voice over IP) est une technologie qui rend possible l'envoi de voix et de données vocales via des réseaux IP. Pour comprendre l'histoire de la VoIP, il est essentiel de revenir sur la conception de cette technologie et d'explorer son développement à travers le temps. Dès les années 1970, les premières expérimentations de transmission vocale ont été réalisées en utilisant des réseaux de données. À cette époque, les réseaux téléphoniques traditionnels reposaient sur des circuits commutés, une technologie à la fois coûteuse et peu efficace. Les chercheurs et ingénieurs se sont alors tournés vers des méthodes alternatives pour la transmission vocale, désireux de tirer parti des possibilités offertes par l'expansion rapide des réseaux informatiques. C'est dans ce contexte que la technologie de la vios sur IP a commencé à emerger.

Le concept consistait à convertir les signaux vocaux analogiques en formats numériques, permettant leur transmission via des réseaux IP. Dans les années 1980, les initiatives de recherche et de développement ont constitué le cadre principal pour l'émergence des premières applications VoIP. L'un des premiers succès mémorables de la VoIP fut la création du protocole H.323 par l'Union internationale des télécommunications (UIT) au cours des années 1990. Ce protocole a posé les jalons techniques de la VoIP en encadrant les normes de communication vocale sur les réseaux IP, comprenant la signalisation, le transport et la gestion. Il a permis de chiffrer les échanges de données vocales entre divers terminaux à travers différents réseaux, ouvrant ainsi la voie au lancement commercial de la VoIP.

Dans les années 1990, plusieurs sociétés et fournisseurs de services de télécommunications ont commencé à explorer et à adopter des systèmes de VoIP **[9] .**

Ces premières innovations offriraient une option moins onéreuse par rapport aux systèmes de télécommunication, visant principalement les échanges internes des entreprises. L'utilisation de techniques de compression sonore, comme le codec G.711, a diminué la bande passante nécessaire pour la transmission vocale tout en bonifiant la qualité du service **[10].** L'essor du haut débit a joué un rôle fondamental dans l'avancement de la VoIP. L'augmentation de la vitesse et de la fiabilité de la connexion Internet a permis d'optimiser considérablement la qualité des appels VoIP.

L'attrait croissant de la VoIP comme alternative aux services téléphoniques classiques séduit de plus en plus d'utilisateurs, notamment en raison de ses tarifs réduits et de ses fonctionnalités avancées telles que la messagerie vocale, les conversations en conférence, et la transcription automatique. Les services téléphoniques traditionnels ont vu leur popularité

augmenter, en partie grâce à leurs coûts moins élevés et leurs options avancées telles que la messagerie vocale, les conférences téléphoniques et la transcription automatique **[11]**. Par ailleurs, les réglementations et politiques entourant la VoIP ont évolué au fil du temps. De nombreux pays ont dû adapter leurs cadres juridiques pour intégrer la VoIP dans le secteur des télécommunications. Des questions touchant à la législation, à la protection des données, à la confidentialité et à la fiscalité ont été soulevées et ont suscité des débats passionnés. La fusion des systèmes informatiques et des réseaux de télécommunication a engendré de nouveaux défis réglementaires et économiques. Les réseaux de télécommunication ont engendré de nouveaux défis réglementaires et économiques.

Au début des années 2000, plusieurs entreprises renommées ont ouvert leur capital au public. Des entreprises de VoIP ont mis à disposition des services VoIP accessibles, entraînant une adoption massive de cette technologie. Des acteurs tels que Google, Vonage et Skype ont été essentiels dans l'expansion de la VoIP, en fournissant des solutions intuitives, économiques et innovantes **[12].** L'essor de la concurrence dans le domaine des télécommunications a également poussé divers opérateurs traditionnels à lancer leurs propres offres de services VoIP. Depuis lors, le secteur de la VoIP a poursuivi son développement et sa diversification. La transition vers des normes ouvertes a permis une meilleure interopérabilité entre les divers fournisseurs et plateformes de communication.

De plus en plus d'appareils sont désormais compatibles avec la VoIP, allant des smartphones aux téléphones de réseau, des télécommandes aux systèmes de contrôle à distance. Les technologies avancées ont également permis d'améliorer constamment la qualité des communications VoIP en intégrant de nouveaux codecs audios et des algorithmes de correction d'erreurs plus performants **[13].** Parallèlement, les développements des technologies 4G et 5G ont ouvert de nouvelles perspectives pour la VoIP mobile, facilitant les échanges vocaux d'une clarté exceptionnelle à l'échelle mondiale. La voix sur IP a fait un long chemin depuis ses débuts exploratoires. Ce qui était jadis une technologie prometteuse mais limitée est à présent devenue un standard incontournable dans le domaine des télécommunications.

A travers ce chapitre, nous allons faire une présentation générale de la Vip. Nous expliquerons ce qu'elle est et comment elle fonctionne. Nous explorerons en détail l'architecture de la Vop, ses composants et son mode de fonctionnement. Nous aborderons également les protocoles de signalisation et de transport de la VIP ainsi que leurs principes de fonctionnement,

leurs mécanismes, et que les codecs utilisés et Les modes d'accès.

Enfin, nous examinerons les avantages et les inconvénients que cette technologie offre.

I.2.Architecture VOIP

Étant donné que la Vop est une technologie de communication récente, elle n'a pas encore de standard particulier. Effectivement, chaque fabricant ajoute ses propres normes et fonctionnalités à ses solutions. Différentes méthodes peuvent être utilisées pour proposer des services de téléphonie et de visiophonie sur des réseaux IP.

L'architecture VIP est généralement décrite dans la figure ci-dessous, qui inclut toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux **[14].**

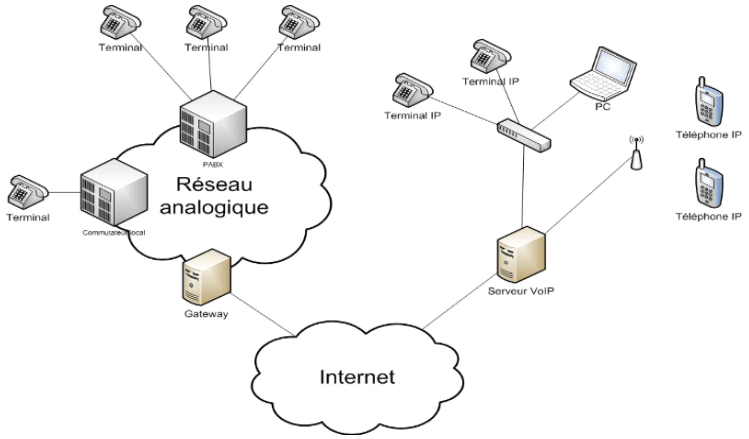


Figure I.1 : Architecture générale de la VIP. **[14]**

I.2.1 Les composants de l'architecture de la VIP sont les suivants :

- ✓ Le routeur est utilisé pour acheminer les données et distribuer les paquets entre deux réseaux. Il est possible de simuler un Gatekeeper sur certains routeurs en ajoutant des cartes spécialisées qui supportent les protocoles VIP.
- ✓ La passerelle (Gateway) est un dispositif qui permet de relier le réseau commuté au réseau IP.
- ✓ Le PABX est le dispositif de commutation du réseau téléphonique traditionnel. Il est utilisé pour relier la passerelle ou le routeur au réseau téléphonique commuté (RTC). Cependant, si l'intégralité du réseau passe en IP, ce matériel devient obsolète.
- ✓ Les terminaux, qu'ils soient logiciels (softphone) ou matériels (hardphone), sont

généralement installés sur l'ordinateur de l'utilisateur. Il est possible d'utiliser un microphone et des haut-parleurs connectés à la carte son pour l'interface audio, même si un casque est conseillé. Afin d'améliorer la clarté, il est possible d'utiliser un téléphone USB ou Bluetooth.

I.2.2 Les divers éléments qui peuvent constituer un réseau :

a. PABX

Les postes téléphoniques d'un établissement (lignes internes) sont principalement reliés au réseau téléphonique public (lignes externes) par PABX (signifie : Private Automatic Branch eXchange). De plus, il offre la possibilité de mettre en place plusieurs fonctions, telles que :

- Faciliter les échanges d'appels entre les postes internes sans utiliser le réseau public.
- Établir des autorisations d'accès au réseau public pour chaque membre du personnel.
- Offrir divers services téléphoniques tels que des conférences, des transferts d'appels, des renvois, des messageries, des appels par nom...
- Effectuer la répartition par service de la facture téléphonique totale (taxes).
- Offrir des services de connexion entre téléphonie et ordinateur (CTI).
- Assurer la gestion des appels d'urgence dans les hôpitaux, les maisons de retraite, etc.
- Assurer la gestion d'un portier interphone d'immeuble et faire fonctionner une gâchette électrique.

Il s'agit d'un Switch avec des caractéristiques spécifiques et peut être perçu comme le cœur d'un réseau privé de téléphonie (Figure I.2). IP-PABX est un PABX (ou PBX) qui utilise la technologie IP pour accéder à son réseau. **[14]**

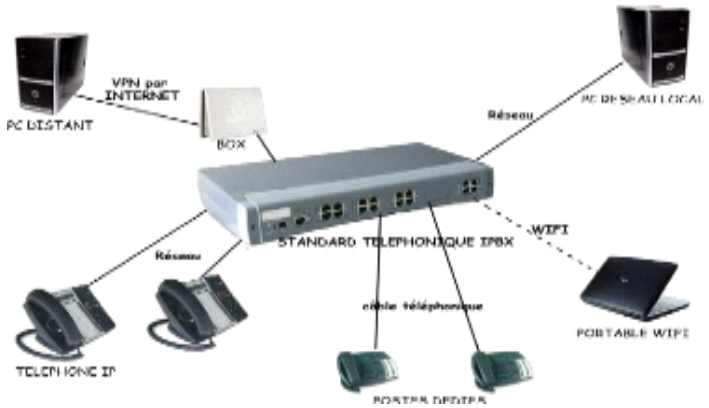


Figure I.2 : Standard Téléphonique IPBX. **[4]**

b.Le serveur de communications :

Il est responsable de la gestion des autorisations d'appel entre les terminaux IP ou les soft phones et les diverses signalisations du réseau. Il a la possibilité de disposer d'interfaces réseaux opérateurs (RTC-PSTN ou RNIS), sinon les appels externes seront transmis par la passerelle spécialement conçue pour cela (Gateway).

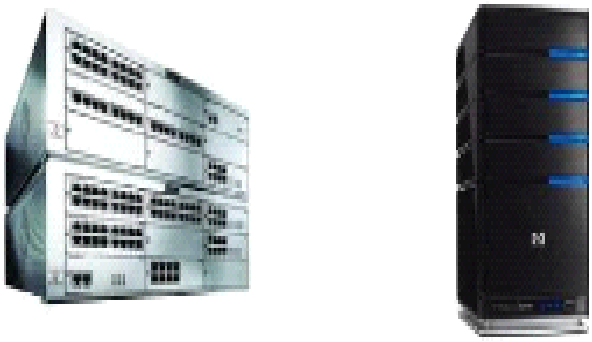


Figure I.3 : serveur de communication

c. La passerelle (Gateway)

Il s'agit d'un dispositif routier muni de cartes d'interface analogiques et/ou numériques qui peut être connecté soit à d'autres PABX (en QSIG, RNIS ou E&M), soit à des opérateurs de télécommunications locaux, nationaux ou internationaux. Il est possible d'avoir plusieurs passerelles dans un même réseau, ou bien une passerelle par réseau local (LAN). L'interface de la passerelle peut aussi être utilisée pour les postes analogiques traditionnels qui pourront exploiter

toutes les ressources du réseau téléphonique IP (appels internes et externes, entrants et sortants) **[14].**

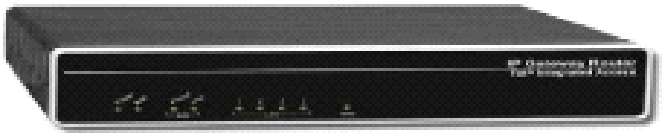


Figure I.4 : La passerelle (Gateway)

d. Le routeur

Un routeur joue un rôle essentiel dans un réseau informatique en gérant la route des paquets. Sa fonction consiste à faire passer des paquets d'une interface réseau à une autre, dans les meilleures conditions (sans diminution du signal ou perte de données), en respectant un ensemble de règles. La confusion entre routeur et relais est généralement présente, car dans les réseaux Ethernet, les routeurs fonctionnent au niveau de la couche 3 du modèle OSI.

Figure I.5 : Routeur Cisco

e. Un commutateur réseau (switch)

Il s'agit d'un dispositif qui permet de relier différents éléments dans un réseau informatique. Un switch se présente sous la forme d'un boîtier avec plusieurs ports Ethernet (de 4 à plusieurs dizaines), il peut intégrer la téléalimentation des ports Ethernet selon la norme 802.3af pour alimenter les IP-phones ou les bornes.

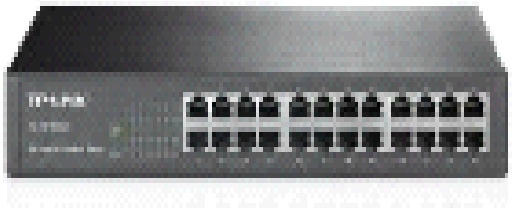


Figure I.6 : switch

f. Le Gatekeeper

Il réalise les transferts d'adresses (identifiant H323 et @ IP du référencement du terminal) et gère la bande passante et les autorisations d'accès. Il s'agit du point de passage indispensable pour tous les équipements de sa zone d'intervention.

Figure I.7 : Gatekeeper. **[3]**

g. L'IP-Phone

Il s'agit d'un téléphone portable qui fonctionne sur le réseau LAN IP à 10/100 avec une norme propriétaire, SIP ou H.323. Il est possible d'utiliser différents codecs audios, ainsi qu'un écran monochrome ou couleur, ainsi qu'une ou plusieurs touches programmables ou préprogrammées. Généralement, il est équipé d'un hub passif avec un seul port afin de pouvoir alimenter le PC de l'utilisateur (l'IP-PHONE est connecté à la seule prise Ethernet murale et le PC est connecté derrière l'IP-PHONE).

Figure I.8 : IP phone

h. Linphone

Un Soft Phone est un programme de communication en ligne. Il permet de communiquer d'un ordinateur à un autre ou d'un ordinateur à un autre téléphone. Il y a une multitude de softphones, dont l'un des plus connus est Linphone

Les interfaces de ces logiciels sont souvent conviviales et très exhaustives, car toutes les fonctionnalités présentes sur les téléphones classiques sont également disponibles sur ces logiciels.

Retrouve parfois d'autres fonctionnalités telles que la messagerie instantanée (IM ou chat), la visiophonie, l'échange de fichiers (par exemple pour partager des photos...), la conférence à plusieurs… **[14]**.

I.9 : Linphone **[14].**

I.3 Mode de fonctionnement de la VoIP

L'encapsulation d'un signal audio numérique (La voix) au sein du protocole IP est connue sous le nom de voix sur IP. Grâce à cette encapsulation, la voix peut être transportée sur n'importe quel réseau compatible TCP/IP. Pour transférer la voix sur un réseau IP, il est essentiel de la numériser

d'abord. Il est donc important de résumer les étapes requises pour numériser la voix avant de poursuivre.

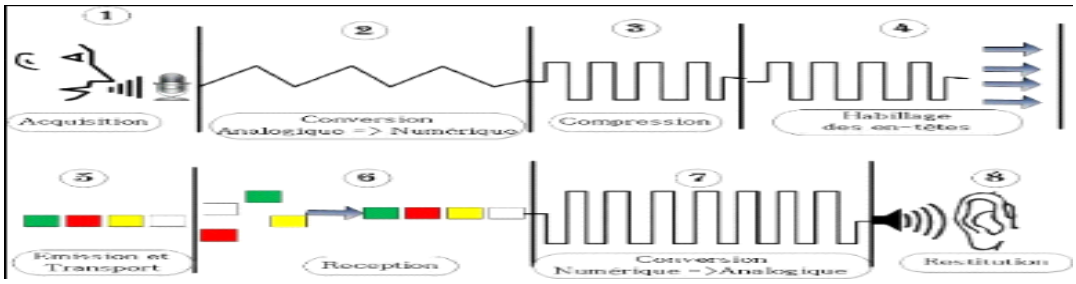


Figure I.10 : Processus de numérisation de la Voix **[7].**

I.3.a Numérisation

Si les signaux téléphoniques à envoyer sont analogiques, il est nécessaire de les convertir ensuite en format numérique en utilisant le format PCM (Pulse Code Modulation) à 64 Kbps. Lorsque l'interface téléphonique est numérique (comme l'accès RNIS, par exemple), on omet cette fonction.

I.3.b Compression

La compression du signal numérique PCM à 64 Kbps est effectuée en utilisant l'un des formats de codec (compression/décompression) avant d'être déposée dans des paquets IP. Le codec est généralement effectué par un DSP (Digital Signal Processor). La bande passante disponible permet également le transport du signal vocal dans son format initial à 64 Kbps.

I.3.c Décompression

En ce qui concerne la réception, les données reçues sont décompressées - Il est essentiel d'utiliser le même codec que pour la compression - puis converties dans le format adapté au destinataire (analogique, PCM 64Kbps, etc.…)**[7].**

I.4 Principaux protocoles de la VoIP

Un protocole est une liste de critères qui définissent les normes et les règles à respecter lors d'un échange de données. Il est primordial de respecter les contraintes temporelles lorsqu'on veut transporter la voix.

Il est donc nécessaire de considérer la mise en place d'un système de signalisation afin de garantir la connexion entre les utilisateurs.

Comme tout domaine en réseau, la VoIP utilise différents protocoles afin de garantir un fonctionnement optimal. Certains de ces protocoles sont consacrés à la signalisation des appels, d'autres au transport de la voix, d'autres encore à la configuration des postes.

Nous allons aborder dans cette partie les protocoles les plus fréquemment employés dans la VoIP : H.323 et SIP, que nous allons étudier en détail **[14].**

A/ Les Protocoles de Signalisation

I.4.1 Protocole H.323

H.323 est un protocole de la série H.32x qui aborde la vidéoconférence à travers divers réseaux.

Au-delà d'un protocole, H.323 établit une alliance de plusieurs protocoles distincts qui peuvent être classés en trois catégories : **la signalisation**, **la négociation de codec** et **le transport des données.**

Les messages d'alerte sont ceux qui sont envoyés afin de solliciter la mise en relation de deux clients, indiquant que la ligne est occupée ou que le téléphone sonne.

La signalisation en H.323 repose sur le protocole RAS pour l'enregistrement et l'authentification, tandis que le protocole Q.931 est utilisé pour l'initialisation et le contrôle des appels.Le protocole H.245 est employé pour la négociation de codec.

Le protocole RTP est utilisé pour le transport de l'information, permettant le transfert de la voix, de la vidéo ou des données numérisées par les codecs. Les messages RTCP peuvent servir à surveiller la qualité ou à renégocier les codecs en cas de baisse de la bande passante, par exemple.

Ce protocole est spécifié afin de traiter les données multimédia avec des contraintes temporelles élevées, telles que la voix ou la vidéo.

a) Composants d'un système H.323

L'architecture standard H.323 est constituée des composants suivants : Final.MCU (Unité de Contrôle Multipoint) - Passerelle (Gateway). - Gatekeepr (garderie).

• **Terminaux** (au minimum deux). Il s'agit des dispositifs de traitement utilisés par les utilisateurs, leur offrant la possibilité d'envoyer et de recevoir des appels. Il est nécessaire d'avoir au moins deux terminaux pour assurer la communication.

• **Gatekeepr**, ou gardien de barrière. Il s'agit de l'équipement qui permet de localiser les utilisateurs. Les différents utilisateurs peuvent être identifiés grâce à un nom auquel le gatekeeper attribue une adresse IP correspondante dans le réseau. En plus de ce rôle essentiel, un gardien de portes assure toute une série de fonctions supplémentaires de gestion et de contrôle des communications,

certaines étant nécessaires et d'autres facultatives.

- **Passerelle**, ou porte d'entrée. Il s'agit de l'appareil qui permet aux utilisateurs du réseau IP de connecter les utilisateurs actifs sur d'autres réseaux téléphoniques, tels que les réseaux RTC, RNIS ou ATM. Il est possible de disposer de plusieurs passerelles différentes selon la nature des réseaux non IP à interconnecter.

• **MCU** (Unité de Contrôle Multipoint), également connue sous le nom de pont multipoint. Il s'agit de l'équipement qui permet de gérer les conférences, c'est-à-dire les échanges multimédias impliquant plus de deux participants. Il est nécessaire que ces derniers se connectent d'abord à la MCU, où les demandes et les négociations des paramètres à utiliser lors de la conférence sont établies **[16].**

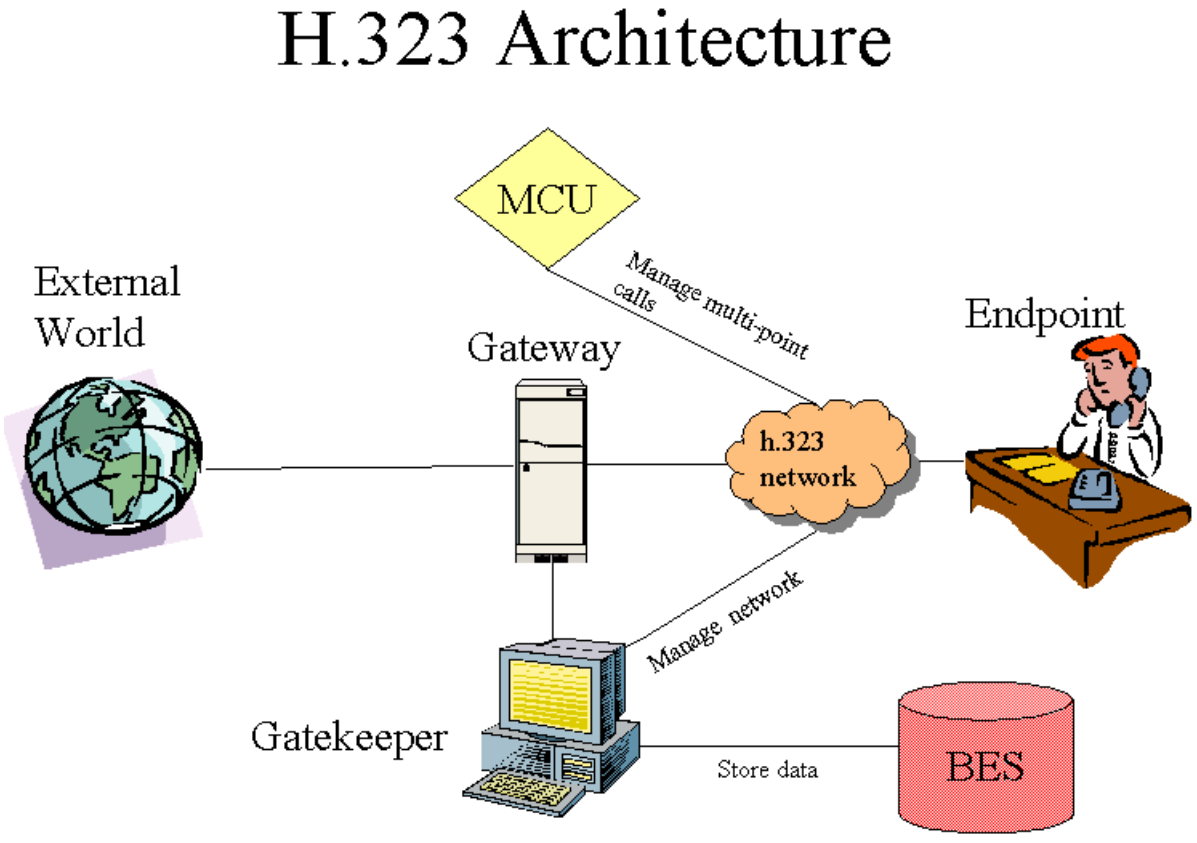


Figure I.11 : Les composants de l'architecture H.323**[17].**

b) Famille de protocole H.323

H.323 est divisé en trois grandes sections (Figure I.12). Effectivement, afin d'établir une communication audio ou vidéo sur IP, il est nécessaire d'encoder le signal en utilisant des codecs normalisés définis dans la norme 11.323, qui établit également la signalisation à utiliser pour établir une communication. Le transfert de la voix ou de la vidéo se fait par le protocole UDP, qui est joint aux protocoles RTP et RTCP pour le transfert de données en temps réel.

- Parmi les codecs envisageables, on peut citer pour le contrôle et la signalisation :

En ce qui concerne le contrôle et la signalisation : H.225, H.245, RTCP.
Pour la voix : G.711, G.722, G.723, G.726, G.728, G.729.
Pour la vidéo : H.261, H.263, H.263+, H.264
Dans le cas des données : T.123, T.124 et T.125 **[7].**

- Trois protocoles sont utilisés pour la signalisation de l'établissement des appels :
  - ✓ Le protocole H.245 est un élément essentiel de H.323 qui assure la gestion des appels. Quand une demande d'appel est acceptée, elle établit un canal de contrôle afin de discuter des paramètres de communication tels que le codeur utilisé et le contrôle de flux.
  - ✓ Le protocole H.225 (SIG) sert à la signalisation et à l'établissement d'appels. Il offre la possibilité de créer et d'étendre des liens entre les points H.323.
  - ✓ La signalisation RAS (Registration, Admission and Status) permet au Gatekeeper de surveiller les Endpoints situés dans sa zone, ce qui facilite la gestion du trafic entre le client et le serveur de communication.
  - ✓ Les procédures Protocole de contrôle RTCP (Real Time Protocol)
  - ✓ Les protocoles de diffusion en temps réel (RTP) pour les flux audios et vidéo **[7].**

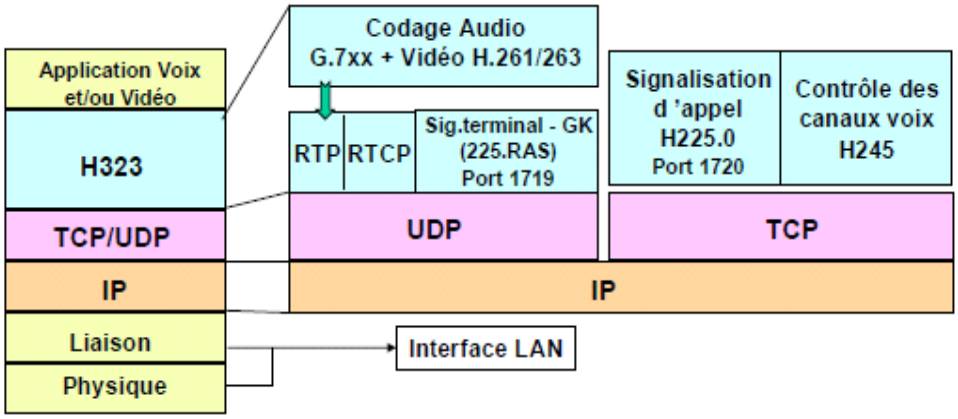


Figure I.12 : Architecture familles du clien H.323 **[18].**

c)Fonctionnalités de H.323

Il y a différentes façons de mettre en place une architecture H.323.Beaucoup de messages sont facultatifs et dans la réalité, il est possible de ne pas les utiliser tous. Par exemple, si la question de l'authentification n'est pas un souci, il est possible de se passer des messages RAS.

Il est également envisageable de suivre les messages de diverses façons. Par exemple, il est possible d'accéder aux canaux RTP sans attendre le message « connect » qui indique que la personne appelée a bien reçu le signal.

Il est possible de conclure que les messages H.225, H.245 et RTP sont envoyés de manière différente : Prenons l'exemple de la signalisation qui passera par plusieurs gardiens de portes qui sont responsables du contrôle et du routage de l'appel, tandis que le flux RTP passe directement d'un poste à l'autre.

Les architectures H.323 peuvent profiter de différentes mises en œuvre. L'architecte point à point et Gatekeeper, multipoint, seront visités **[16].**

- **Architecture point à point :**

Dans cette structure, chaque client gère la couche protocolaire et tout le trafic ne se déplace qu'entre l'émetteur et le destinataire.

Afin de débuter un appel, on appelle l'adresse IP du destinataire. Ainsi, la phase de signalisation commence et les protocoles liés envoyant un message au destinataire en lui suggérant de réaliser le rapport. On envoie également l'identifiant H.323 lors de la phase de signalisation. Le destinataire

vérifie son état et l'émetteur peut recevoir deux réponses : libre ou occupé.

La phase de négociation des codecs commence lorsque le destinataire est prêt à recevoir l'appel et chaque partie énumère les codecs disponibles pour s'entendre sur un standard.

Finalement, la communication commence et les flux sont généralement transmis en RTP. Lorsque la communication entre les deux parties est terminée, toutes les prises se referment. Le diagramme suivant illustre une structure point à point (Figure 1.13) :

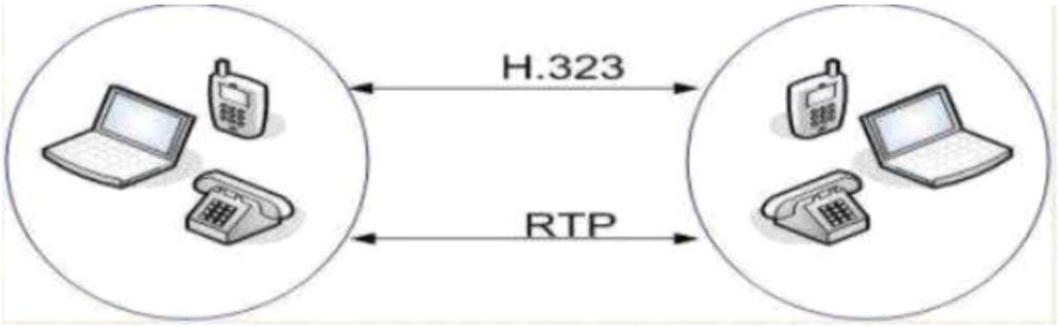


Figure I. 13 : Architecture point à point**. [19]**

- **Gatekeeper de l'architecture :**

« Point à point » entre deux clients enregistrés auprès d'un **gatekeeper**. Le portier est un nouvel élément qui joue un rôle dans le processus de signalisation dans cette architecture. Cet appareil garantit la traduction de l'adresse IP/numéro de téléphone ainsi que de toute la partie autorisée.

Les clients VoIP sont donc programmés pour s'inscrire auprès du gardien de portes. De cette manière, lors de leur connexion au réseau, ils communiquent leur adresse IP et leur identifiant H.323 au gardien de portes.

L'architecture gatekeeper est résumée dans le schéma ci-dessous (Figure 1.14).

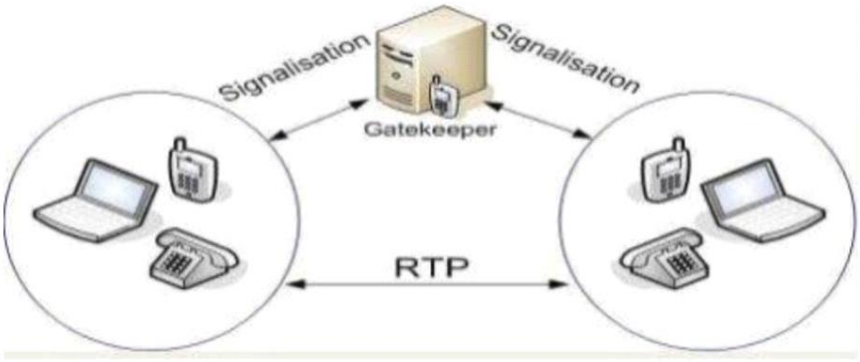


Figure I.14 : l'architecture Gatekeeper **[19].**

- **Architecture multipoints** : communication "Multipoints" entre différents clients (MCU requis)

Un nouvel élément est introduit dans cette architecture : l'unité de contrôle multipoint ou MCU.Ce système offre la possibilité de gérer différentes communications en même temps, ce qui est très pratique pour les conférences télécommunications. Il offre également des services tels que la transmission d'une tonalité.Lorsque le système VoIP est mis en service, la centrale multipoint informe le gatekeeper de sa présence et lui fournit diverses informations (nombre de clients simultanés, débits possibles et identifiant H.323). Ensuite, tout se déroule comme dans l'architecture de garde. Les clients VoIP doivent se connecter au gatekeeper.

Le schéma suivant illustre une structure à plusieurs points (figure 1.15)

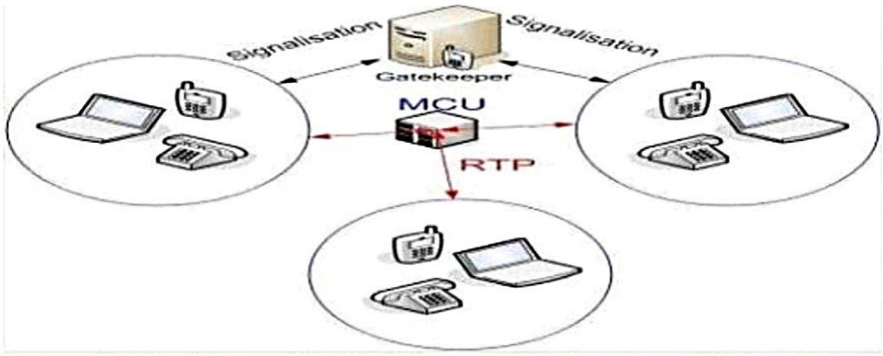


Figure I.15 : Architecture multipoints **[19].**

e) Avantages et inconvénients de la technologie H323

La technologie H.323 présente des points forts et des points faibles.

Parmi les bénéfices, nous mentionnons :

• Gestion de la bande passante : H.323 assure une gestion efficace de la bande passante en limitant les flux audio/vidéo pour garantir le bon déroulement des applications essentielles sur le réseau local. La bande passante et le débit peuvent être ajustés en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue) par chaque terminal H.323.

• H.323 offre la possibilité de réaliser des conférences multipoint en utilisant une structure centralisée de type MCU (Unité de Contrôle Multipoint) ou en mode ad-hoc.

• H.323 offre également la possibilité de transmettre des données en multicast.

• La compatibilité : H.323 permet aux utilisateurs de ne pas avoir à se soucier de la connexion.

• Flexibilité : une conférence H.323 peut englober différents appareils (studio de visioconférence, ordinateur, téléphone...) qui peuvent entrer en communication, en fonction des circonstances, de la voix, de la vidéo et même des données grâce aux spécifications T.120 **[16].**

I.4.2 Protocole SIP

Le protocole SIP - Protocole de démarrage de session est un protocole de gestion de session de communication en multimédia. C'est un protocole ouvert et standard qui est principalement utilisé pour la signalisation en VoIP.

En VoIP, ce protocole est donc utilisé pour gérer les appels. À titre d'exemple, SIP permet au poste de s'enregistrer auprès de l'IPBX.

Grâce à SIP, le poste peut également transmettre des informations à l'IPBX lorsque l'utilisateur appuie sur les touches du clavier. Il offre également la possibilité à l'IPBX de faire sonner un poste, de connecter deux téléphones, etc.

Il occupe donc une place centrale dans nos infrastructures de VoIP. Si un protocole est à conserver pour les applications et les systèmes VoIP, c'est celui-ci. Le protocole utilisé dans la solution de téléphonie de notre organisme d'accueil est d'ailleurs celui suivant.

Le protocole SIP est le standard ouvert de VoIP, qui est interopérable et le plus largement utilisé, et a pour objectif de devenir le standard des télécommunications multimédia (son, image, etc.). Par exemple, Skype, qui adopte un format exclusif, ne permet pas d'interagir avec un autre réseau de voix sur IP et ne propose que des passerelles payantes vers la téléphonie standard.

Ainsi, SIP ne se limite pas à la VoIP, mais peut être utilisé pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo.

a) L'architecture SIP

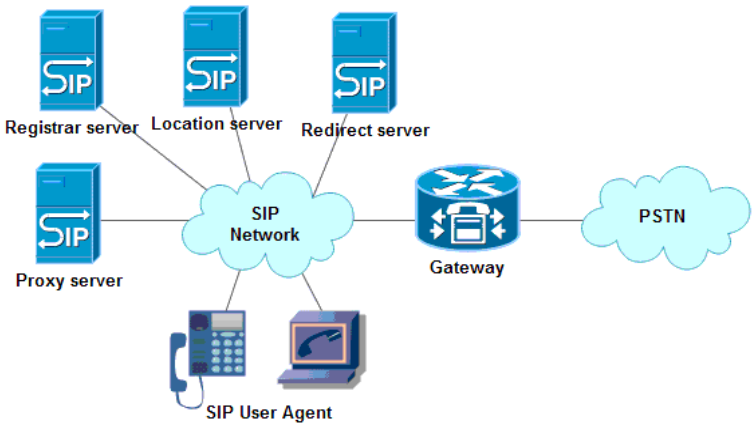


Figure I.16 : Architecture SIP **[20].**

L'User Agent est l'application de l'utilisateur final (terminal téléphonique, softphone...), composée de deux parties distinctes : la partie client et la partie serveur. La partie client est connue sous le nom d'User Agent Client (UAC) qui envoie les requêtes SIP, tandis que la partie serveur est appelée User Agent Server (UAS) qui les reçoit.

• **Serveur Registrar** :

Facilite la synchronisation des adresses IP avec les adresses SIP.

• **Serveur Redirect :**

Donne au client les renseignements sur le prochain saut qui doit être atteint par un message, puis le client contacte le serveur du prochain saut ou UAS.

• **Serveur Proxy :**

Transmet les demandes d'un client à un autre, il peut également rendre possible des opérations telles que l'authentification, l'autorisation ou le contrôle d'accès au réseau.

• **Serveur de localisation :**

La localisation de l'abonné en utilisant sa base de données alimentée par le serveur d'inscription. Il est fréquent que le serveur de localisation et le serveur Registrar soient mis en place au sein d'une

même organisation.

b) Principe de fonctionnement

Comme nous opterons pour le protocole SIP pour notre travail, nous examinerons en détail les différents aspects et caractéristiques qui font du protocole SIP une excellente option pour établir une session, ainsi que les principales caractéristiques du protocole qui sont :

Mise en place d'un compte SIP Il est primordial de veiller à ce que la personne appelée soit constamment accessible. Si vous le versez, un compte SIP sera lié à un nom unique. Par exemple, si un utilisateur d'un service de voix sur IP possède un compte SIP et que son adresse IP change à chaque redémarrage de son ordinateur, il doit néanmoins être toujours accessible. Il est donc nécessaire d'associer son compte SIP à un serveur SIP (proxy SIP) dont l'adresse IP est définitive. Il recevra un compte de ce serveur qui lui permettra d'effectuer ou de recevoir des appels, quel que soit son emplacement. Ce compte pourra être repéré à travers son nom (ou pseudonyme).

- Modification des caractéristiques au cours d'une session

Il est nécessaire qu'un utilisateur puisse modifier les paramètres d'un appel en cours. Par exemple, il est possible de modifier un appel initialement configuré en (voix uniquement) en (voix + vidéo).

b) Différents modes de communication

Grâce à SIP, les utilisateurs qui commencent une session ont la possibilité de communiquer en mode point à point, diffusif ou combiné.

• État Point par point : dans cette situation, on évoque l'« unicast », qui désigne la communication entre deux machines.

• Dans ce cas, on parle de « multicast » (plusieurs utilisateurs via une unité de contrôle MCU - Unité de contrôle multipoint) dans le mode diffusif.

Organiser les participants.

Lors d'une session d'appel, de nouveaux participants peut rejoindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente (cette fonctionnalité rejoint les caractéristiques d'un PABX, par exemple, où l'appelant peut être transféré vers un numéro spécifique ou être mis en attente).

Adressement

Les personnes ayant un compte SIP avec une adresse similaire à une adresse e-mail (sip: numéro@serveursip.com). Les utilisateurs ont un numéro SIP unique.

SIP : identifiant [: mot_de_passe] @serveur [? paramètres] On distingue dans cette adresse

On distingue également 3 modes précis

- ✓ Communication entre deux postes
- ✓ Plusieurs postes membre d'un serveur
- ✓ Communication entre deux postes

Le serveur Registrar assure la gestion des demandes REGISTER envoyées par les utilisateurs Agents afin de signaler leur emplacement actuel. Ainsi, ces demandes incluent une adresse IP, liée à une URI, qui seront enregistrées dans une base de données (figure I.17). La structure des URI SIP est très proche de celle des adresses email **: sip : utilisateur@domaine.com.** En règle générale, des dispositifs d'authentification empêchent toute personne de s'enregistrer avec n'importe quelle adresse URI **[16].**

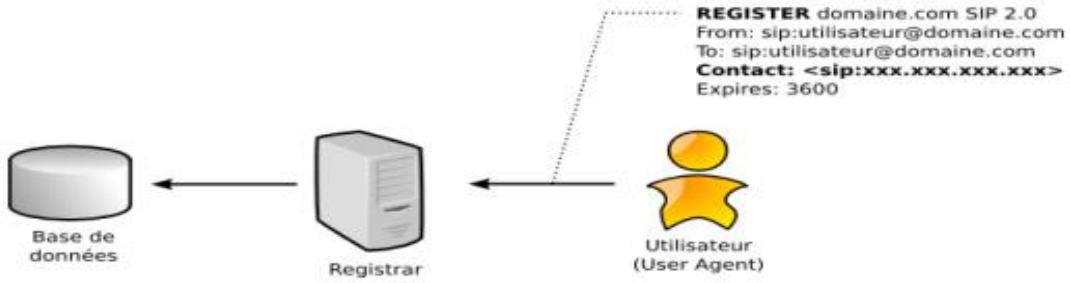


Figure I.17 : Enregistrement d'un utilisateur **[21].**

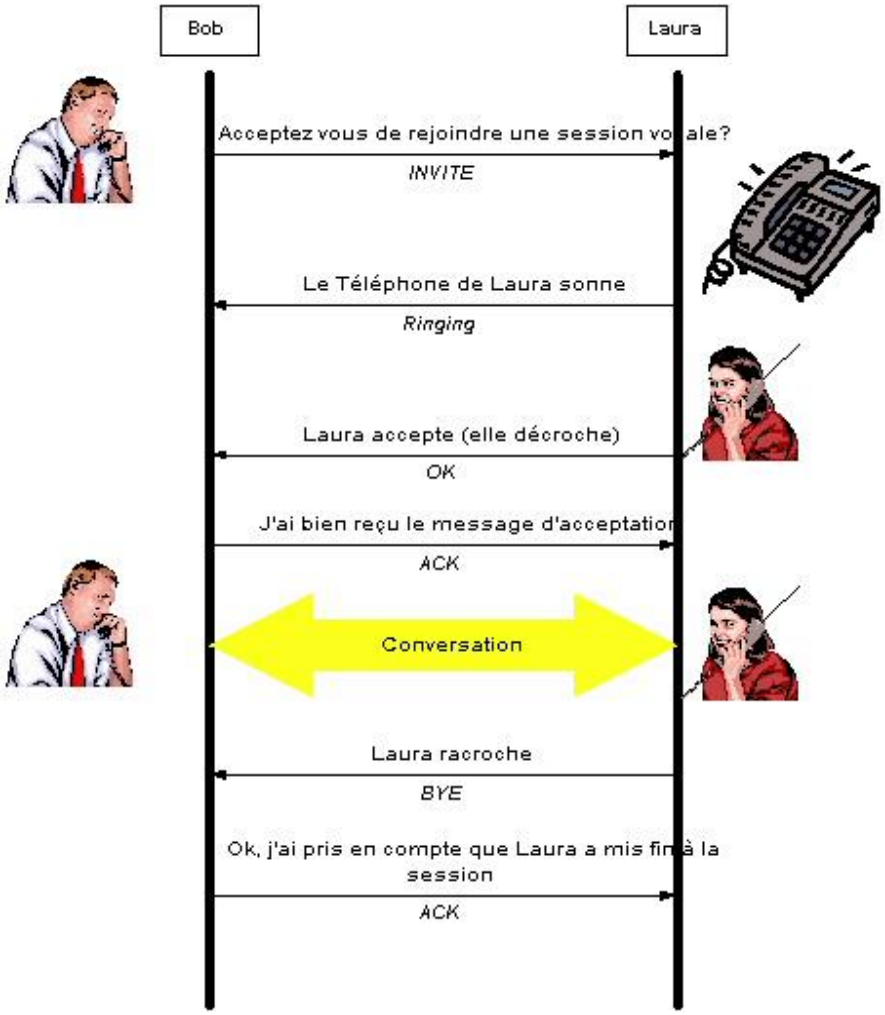


Figure I. 18 : Représente les échanges qui ont lieu entre deux UA pour l'établissement d'une connexion **[22].**

Ce cas est le plus simple car les deux UA connaissent l'adresse IP de leur interlocuteur c'est pourquoi ils peuvent se joindre directement

Mode diffusif : Plusieurs postes membre d'un serveur

L'objectif d'un Proxy SIP est de faciliter la communication entre deux utilisateurs qui ne sont pas conscients de leurs emplacements respectifs (adresse IP). Effectivement, un Registrar a préalablement stocké l'association URI-Adresse IP dans une base de données. Il est donc possible pour le Proxy d'interroger cette base de données afin de rediriger les messages vers le destinataire. Les étapes de l'interrogation du proxy de la base de données sont illustrées dans la figure I.19**[16].**

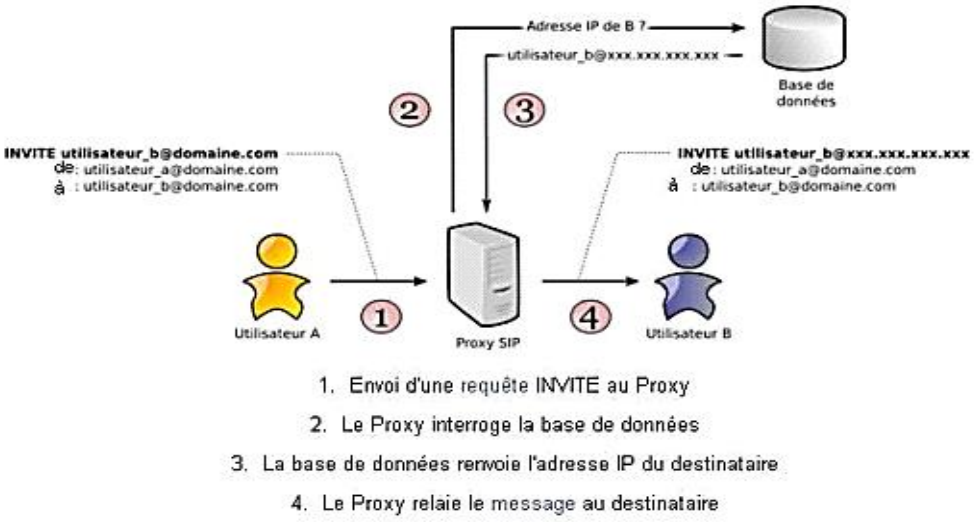


Figure I. 19 : Principe du protocole SIP [**23].**

Le Proxy ne transmet que les messages SIP afin de créer, superviser et achever la session (voir figure I.20). Après l'établissement de la session, les données, comme un flux RTP pour la VoIP, ne passent pas par le serveur Proxy. On les échange directement entre les utilisateurs **[16].**

Définit six messages SIP pour la négociation SIP :

- **INVITE** : Invite un autre terminal à participer à l'appel.
- **ACK** : accusé de réception, employé pour donner une réponse positive à une requête.
- **BYE** : met un terme à la session actuelle.
- **SIP** utilise différents types de messages, les plus importants étant les suivants :

Pour s'enregistrer, le client envoie ce message à son registrar afin de fournir son URI et son adresse IP.

- **INVITE** : Ce message donne l'opportunité à un client de solliciter la création d'une session supplémentaire. Il est également possible de l'utiliser pendant la communication pour modifier la session.
- **L'ACK** est un message qui confirme la création d'une session **SIP** après un message INVITE.
- **CANCEL** : Ce message annule une demande de session déjà faite avec un **INVITE**. **[1]**

BYE : met fin à une séance en cours. Contrairement au message de refus, il est nécessaire d'activer la session SIP afin d'envoyer un message de refus. Bien qu'il puisse sembler semblable à CANCEL, il y a une distinction essentielle :

Le message "BYE" est considéré comme un succès (la communication a eu lieu et est maintenant

terminée), tandis que **CANCEL** est considéré comme un échec par l'utilisateur. La personne appelée n'a pas répondu à temps, donc l'appelant a raccroché.

- Des codes de réponse **SIP** :

Une fois qu'une requête est reçue et traitée, un agent ou un serveur **SIP** émet un message de réponse indiquant le succès ou l'échec du traitement. Une séquence de trois chiffres est utilisée pour coder ces réponses. Le premier chiffre indique le type de réponse, tandis que le premier est un code de classe. Les deux chiffres suivants donnent une indication plus précise. Le tableau II.5 présente différentes réponses **SIP** envisageables.

• **Classe 1xx** - Réponse provisoire : la demande est en train d'être traitée.

• **Classe 2xx** - Réussite : la demande d'action a été bien reçue, comprise et acceptée.

• **Classe 3xx** - Redirection : il est essentiel d'effectuer une autre action auprès d'un autre équipement.

• **classe 4xx** : la demande est mal formulée.

• **Classe 5xx** - Erreur du serveur : le •serveur n'a pas réussi à répondre correctement à la requête.

• **Classe 6xx** - Autre erreur, problème global **[24].**

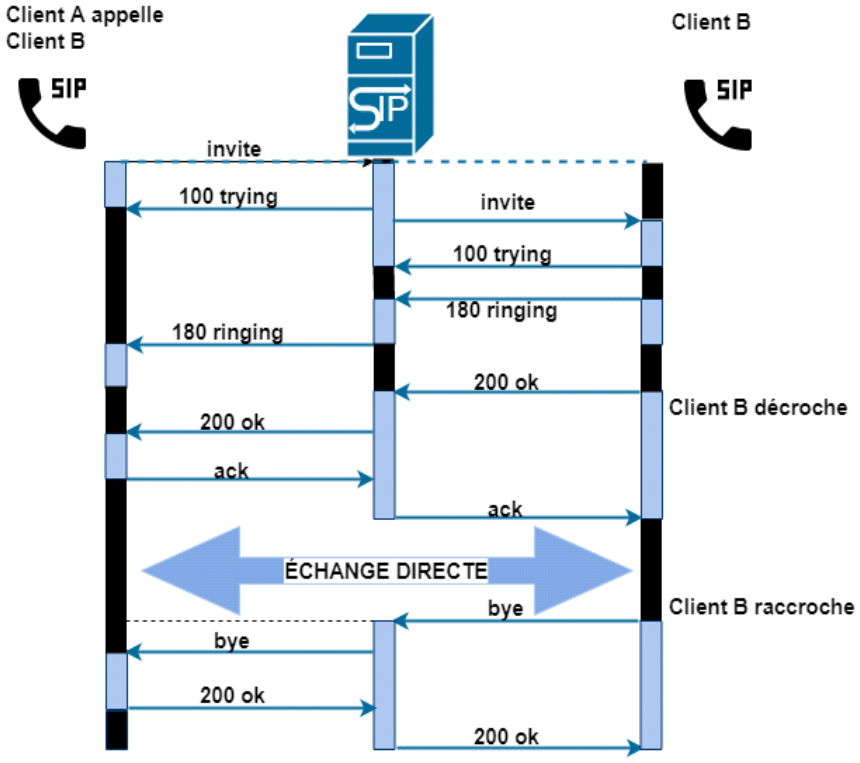


Figure I. 20 : Procédure d'établissement de session SIP**[24].**

c) Avantages et inconvénients

Les principaux atouts du protocole SIP sont l'ouverture, la conformité, la simplicité et la souplesse, voici en détail ces différents avantages :

• Ouvert : les protocoles et documents officiels sont expliqués et disponibles en téléchargement pour tous.

• Standard : le protocole a été standardisé par l'IETF et il continue d'évoluer en créant ou en développant d'autres protocoles qui fonctionnent avec SIP.

• Simple : Le SIP est facile et très proche de http.

• Adaptable : Le SIP peut également être employé pour toutes sortes de sessions multimédia (voix, vidéo, ainsi que musique, réalité virtuelle, etc.).

En revanche, une implémentation incorrecte ou incomplète du protocole SIP dans les User Agents peut occasionner des perturbations dans le fonctionnement ou générer du trafic inutile sur le réseau. Le nombre limité d'utilisateurs est un autre désavantage : SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne profite pas de l'effet réseau.

COMPARAISON ENTRE LE PROTOCOLE SIP ET H.323

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

Tableau I. 1 : Tableau de comparaison entre le protocole SIP et H.323 **[25] .**

	SIP	H.323
Nombre d'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
Fonction de conférence	Distribuée	Centralisée par l'unité MCU
Fonction de télé services	Oui, par défaut	H.323 v2 + H.450
Détection d'un appel en Boucle	Oui	Inexistante sur la version 1, un appel routé sur l'appelant provoque une infinité de requêtes
Signalisation multicast	Oui, par défaut	Non

B/ Protocoles de transport

Deux protocoles de transport supplémentaires utilisés dans la voix sur IP sont décrits, à savoir l'RTP et le RTCP.

I.4.3 Description générale de RTP (Real time Transport Protocol),

L'IETF a développé un protocole standardisé en 1996 pour faciliter le transport en temps réel de bout en bout des flux de données audio et vidéo sur les réseaux IP, c'est-à-dire sur les réseaux de paquets. Le protocole RTP se trouve au niveau de l'application et utilise les protocoles de transport TCP ou UDP sous-jacents. Cependant, l'utilisation de RTP est souvent utilisée au-dessus d'UDP, ce qui facilite l'accès au temps réel. Les applications en temps réel telles que la conversation en ligne ou la visioconférence représentent un véritable défi pour Internet. La mention d'une application en temps réel implique la présence d'une qualité de service (QoS) spécifique que RTP ne garantit pas en raison de son fonctionnement au niveau Applicatif **[25].**

Le protocole RTP se trouve au niveau de l'application et utilise les protocoles de transport CP ou UDP sous-jacents. Cependant, l'utilisation de RTP est souvent utilisée au-dessus d'UDP, ce qui facilite l'accès au temps réel. Les applications en temps réel telles que la conversation en ligne ou la visioconférence représentent un véritable défi pour Internet. L'utilisation d'une application en temps réel implique la présence d'une qualité de service (QoS) spécifique, que RTP ne garantit pas en raison de son fonctionnement au niveau Applicatif. En outre, RTP est un protocole situé dans un environnement multipoint, ce qui signifie qu'il a la responsabilité de gérer le temps réel et d'administrer la session multipoint.

I.4.3.1 Les fonctions de RTP

L'objectif principal du protocole RTP est de structurer les paquets à l'entrée du réseau et de les superviser à la sortie. Cela permet de reconstituer les flux avec leurs caractéristiques initiales. RTP est un protocole complet, intentionnellement incomplet et adaptable afin de répondre aux exigences des applications. Il sera inclus au sein du cœur de l'application. La supervision est confiée aux équipements d'extrémité **[19]** .Il s'agit également d'un protocole conçu pour les applications qui ont des caractéristiques en temps réel. Cela permet donc de :

• Instaurer une séquence de paquets en utilisant une numérotation, ce qui facilitera la détection des paquets perdus. Il s'agit d'un aspect essentiel dans la reconstruction des données. Il est important

de noter que la perte d'un paquet n'est pas une perte significative.

• Reconnaître la source, c'est-à-dire reconnaître l'expéditeur du paquet. Dans un multicast, il est nécessaire de connaître et de déterminer l'identité de la source.

• Déterminer le contenu des données afin de les relier à un transport sécurisé et reconstruire la base de temps des flux (horodatage des paquets : possibilité de resynchronisation)

I.4.3.2 Avantages et inconvénients

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.) ; de détecter les pertes de paquets ; et d'identifier le contenu des paquets pour leur transmission sécurisée.

Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garantit pas le délai de livraison.

I.4.4 Le protocole RTCP

I.4.4.1 Description générale de RTCP (Real time Transport Control Protocol)

Le protocole RTCP repose sur la diffusion régulière de paquets de contrôle à tous les membres d'une session. Le multiplexage des paquets de données RTP et des paquets de contrôle RTCP est possible grâce au protocole UDP (par exemple).

Le protocole RTP fait appel au protocole RTCP, qui est un protocole de contrôle du transport en temps réel, qui transmet les informations supplémentaires nécessaires à la gestion de la session.

I.4.4.2 Les fonctions principales du protocole RTCP sont les suivantes

Il est fréquent que les applications multimédias soient transportées par des flots différents, ce qui entraîne une synchronisation supplémentaire entre les médias. Prenons l'exemple de la voix, de l'image ou même des applications numérisées à différents niveaux hiérarchiques qui peuvent observer les flots gérés et suivre des chemins variés **[19].**

I.4.4.3 Point fort et limite du protocole RTCP

La transmission de données en temps réel est possible grâce au protocole de RTCP. Il offre la possibilité de surveiller de manière permanente une session et ses participants.

En revanche, il opère selon une stratégie complète. Et il est incapable de maîtriser l'élément essentiel de la communication, à savoir le réseau.

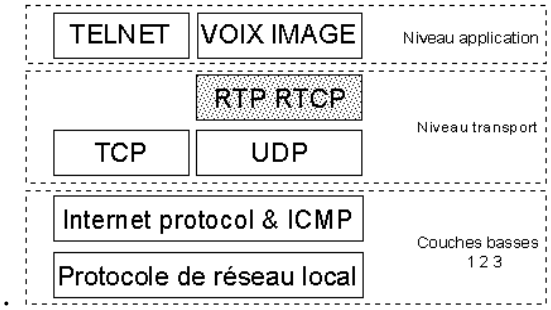


Figure I. 21 : RTP/RTCP dans de modèle OSI **[24].**

I.5 Les Codecs

L'abréviation Codec désigne le Codeur/Décodeur. Un codec repose sur un mécanisme qui permet de comprimer les informations qu'on lui transmet. C'est une méthode qui permet de compresser et de décompresser un signal, que ce soit de l'audio ou de la vidéo, généralement en temps réel, ce qui permet de diminuer la taille du fichier initial. La voix de l'émetteur est numérisée et compressée par le codec, ce qui permet d'encapsuler les données numériques dans des paquets IP et de les transmettre au destinataire. Lorsque le destinataire arrive, il décompose et restitue le son grâce au même codec. Il est. Les codecs à pertes et les codecs sans pertes sont différents. Un codec à pertes différencie les parties moins importantes des données et les élimine afin de gagner en importance.

I.5.1 Qualité de la voix

Dans le domaine de la téléphonie sur IP, les divers codecs sont plus ou moins efficaces dans la transmission du signal original. La qualité de la voix restituée est évaluée en utilisant le score MOS (Mean Opinion Score). Il s'agit d'une note de 1 à 5 attribuée par des auditeurs qui jugent de la qualité de l'écoute. Plusieurs codecs peuvent être utilisés pour la VoIP. Voici leur description :

- **G.711** : Ce codec a été le premier employé dans le domaine de la VoIP. Bien qu'il existe désormais des codecs bien plus intéressants, celui-ci est toujours utilisé dans les équipements afin de garantir la compatibilité entre différentes marques d'équipement
- **G.722** : Contrairement au G.711, ce codec permet une transformation du spectre jusqu'à 7kHz, ce qui permet une meilleure réalisation de la voix. Ce codec offre des débits de 48,56 ou 64kbit/s. L'une de ces caractéristiques est la possibilité de changer immédiatement de débit. Cela est extrêmement bénéfique lorsque la qualité de la transmission se détériore
- **G.723.1** : Le codec par défaut lors des communications à faible débit est G.723.1. On peut choisir entre deux modes. Le premier offre une vitesse de 6,4kbit/s tandis que le deuxième offre

une vitesse de 5,3kbit/s **[7].**

Tableau I. 2 : Liste des codecs avec leur débit correspondant **[25].**

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

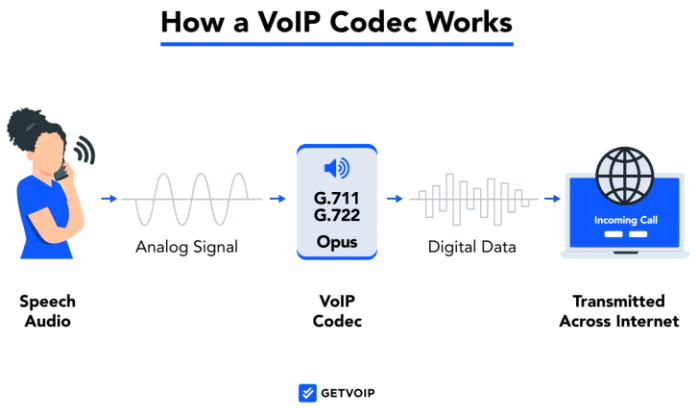


Figure I. 22 : fonctionnement du VoIP codec **[26].**

I.6 Les modes d'accès :

La voix sur IP englobe donc les échanges entre les ordinateurs. Pour ce genre de communication, il est nécessaire que chaque utilisateur possède un logiciel adéquat. En cas de connexion via le réseau Internet, on évoque alors la téléphonie en ligne.

Les communications de PC à téléphonie (PC to Phone) sont la deuxième catégorie de voix sur IP. Dans les deux cas, le téléphone portable est désigné sous le nom de soft phone, qui met l'accent sur l'imitation du téléphone portable par le biais d'un logiciel.

En fonction du terminal utilisé (ordinateur ou téléphone classique), on peut faire une distinction.

Trois options d'accès de voix sur IP sont envisageables :

• L'échange de voix sur IP entre deux machines.

La transmission de la voix sur IP entre un ordinateur et un téléphone.

La transmission de la voix sur IP entre deux appareils électroniques.

I.6.1 La voix sur IP entre deux ordinateurs

C'est le cas le plus simple. Il suffit de disposer d'une carte son, de haut-parleurs et de microphones pour chacun des interlocuteurs. Il faut également connaître l'adresse IP de chacun des terminaux pour établir la communication.

Dans ce premier type de voix sur IP, les utilisateurs communiquent à partir d'un logiciel de voix sur IP qu'on appelle soft phone.

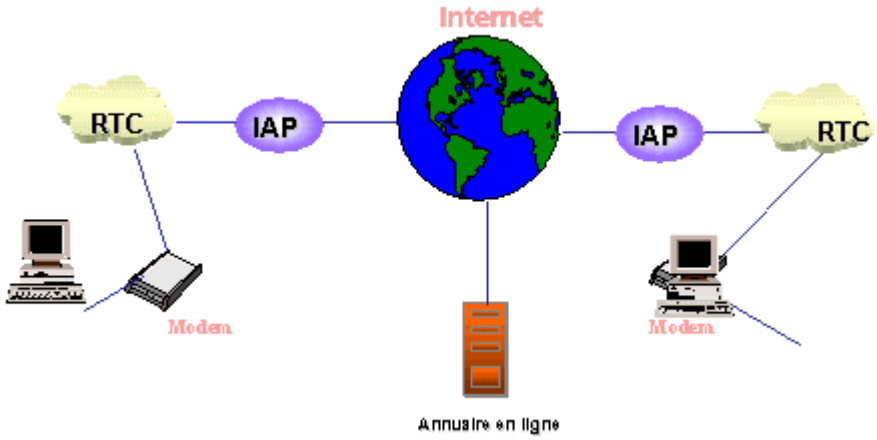


Figure I. 23 : Voix sur IP entre deux ordinateurs **[27].**

I.6.2 La voix sur IP entre un PC et un téléphone

Ce cas nécessite une conversion des signaux entre le RTC et le réseau IP. En effet, ces deux terminaux utilisant des technologies différentes (la commutation de circuits et la commutation de paquets). L'échange des informations nécessite une passerelle ainsi l'utilisateur possédant un ordinateur et désirant appeler l'autre sur son téléphone doit se connecter à un service spécial sur Internet, offert par un fournisseur de service (un ISP) ou par son fournisseur d'accès à Internet (son IAP) **[7].**

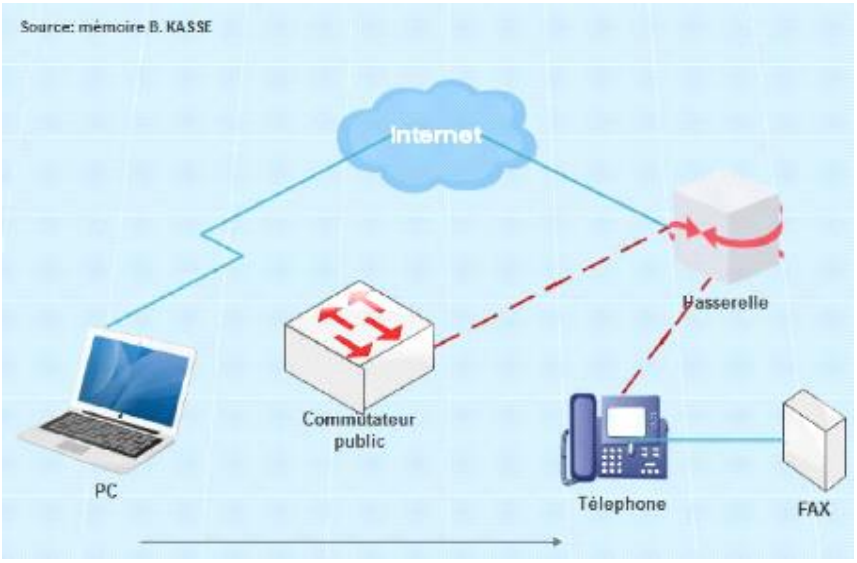


Figure I. 24: Voix sur IP entre un ordinateur et un téléphone **[7].**

I.6.3 La voix sur IP entre deux téléphones

Dans cette situation, il est requis de convertir les signaux entre le RTC et le réseau IP. Effectivement, ces deux appareils sont équipés de technologies distinctes (commutation de circuits et commutation de paquets). L'échange d'informations requiert une passerelle, ce qui signifie que l'utilisateur qui a un ordinateur et souhaite appeler l'autre sur son téléphone doit se connecter à un service spécifique sur Internet, proposé par un fournisseur de services (un ISP) ou par son fournisseur d'accès à Internet (son IAP) **[7].**

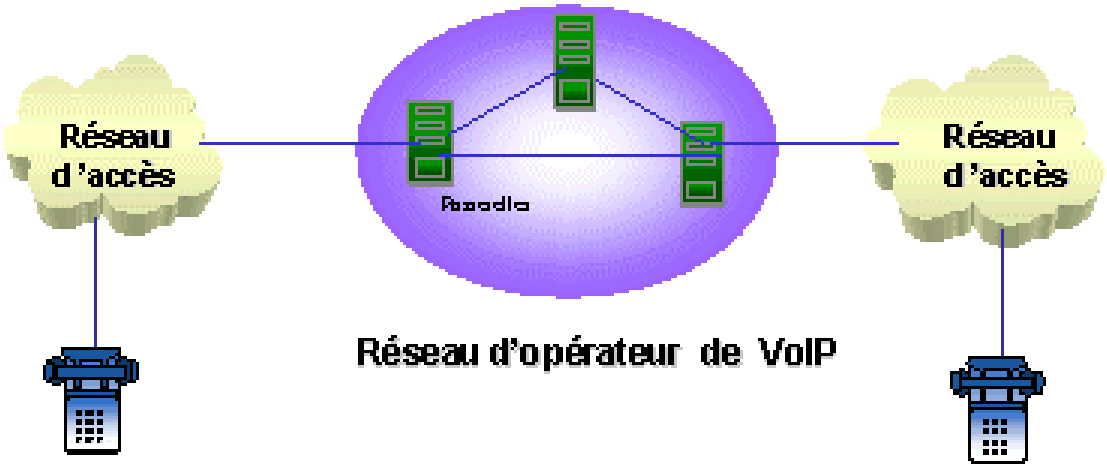


Figure I. 25: Voix sur IP entre deux téléphone **[27].**

I.7 Avantages Et Inconvénients De La Voix Sur IP

I.7.1 Les avantages de la VoIP

Étant donné que notre objectif est de mettre en œuvre un système de téléphonie par VoIP, il est essentiel de mettre en avant les atouts de cette technologie, ce qui pourrait inciter les entreprises à migrer vers cette nouvelle technologie de communication. Vous trouverez ci-dessous :

- **la flexibilité :**

Les solutions de téléphonie IP sont spécialement conçues pour prendre en charge une stratégie d'émigration à faible risque à partir de l'infrastructure déjà en place. Ainsi, il est possible de passer de la solution actuelle à la téléphonie sur IP de manière fluide.

• La diminution des dépenses : Effectivement, le trafic transmis par le réseau RTC est plus onéreux que sur un réseau IP. Les communications internationales en utilisant le VoIP connaissent des réductions significatives, ce qui les rend encore plus attrayantes dans la mutualisation de voix/données du réseau IP intersites (WAN). Dans cette situation, le bénéfice est directement lié au nombre de sites éloignés.

Un transfert de voix, de vidéos et de données (à la fois ou triple Play) ou multimédia : Lorsque l'entreprise considère la voix comme une application supplémentaire du réseau IP, elle ne se limite pas à remplacer un transport opérateur RTC par un transport IP, mais elle simplifie également la gestion des trois réseaux (voix, données et vidéo) grâce à ce seul transport.

• L'accès : Les utilisateurs ont la possibilité d'accéder à tous les services du réseau où qu'ils soient connectés, notamment en substituant les postes, ce qui permet d'optimiser les ressources et de mieux les gérer, ce qui permet de réaliser des économies importantes sur l'administration et l'infrastructure.

Les PABX en réseau ont accès à des services centralisés tels que la messagerie vocale et la taxation. On maintient cette même centralisation sur un réseau VoIP sans restreindre le nombre de canaux.

I.7.2 La vulnérabilité de la VoIP

-Attaque virus :

Lorsque le serveur VoIP est infecté par un virus, il est possible que les utilisateurs ne puissent plus accéder au réseau téléphonique. D'autres ordinateurs connectés au système peuvent également être infectés par le virus.

• Vol : Les pirates qui réussissent à pénétrer un serveur VoIP ont également la possibilité d'accéder

aux messages vocaux stockés et au service téléphonique, permettant ainsi d'écouter des conversations ou de passer des appels gratuits aux noms d'autres comptes.

fiabilit& et qualité sonore :Une des principales difficultés de la téléphonie sur IP réside dans la qualité de la retransmission, qui n'est pas encore optimale. Effectivement, des problèmes tels que la qualité de la reproduction de la voix du correspondant et le temps écoulé entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être très préoccupants. En outre, il est possible que des éléments de la conversation manquent (des paquets perdus lors du transfert) sans pouvoir être certains de leur perte et de leur moment **[14].**

I.8 Conclusion :

En résumé, la VoIP (Voice over IP) est un véritable changement dans le domaine des télécommunications en proposant une solution moderne et abordable aux systèmes de téléphonie classiques. L'architecture de la VoIP repose sur les protocoles IP, ce qui lui confère une grande souplesse et facilite son intégration avec d'autres services numériques, comme la visioconférence et la messagerie instantanée. Les protocoles de communication et de transport, tels que SIP et RTP, ainsi que les codecs audio employés, ont un impact essentiel sur l'efficacité et la qualité des communications VoIP.

L'objectif principal de cette initiative est d'améliorer le cadre de travail des employés de l'entreprise en permettant à l'utilisateur de se déplacer librement du lieu où se trouve le modem.

Chapitre II
Attaques contre la VoIP et bonnes pratiques de sécurisation

Introduction :

La VoIP, actuellement en plein développement, pouvant faire sujet d'attaque des pirates informatiques, au niveau spécifique des réseaux IP ou la VoIP proprement dite. Celle-ci présente un nombre de vulnérabilités en terme : de protocole, de logiciel, de système d'exploitation, d'infrastructure physique et d'erreur humaine.

Dans ce chapitre, nous dériverons des attaques qui menacent la VoIP, et nous détaillerons quelques-uns. Nous finirons par une description des bonnes pratiques pour sécuriser les communications de type voix sur IP **[15].**

II.1 Principaux risques

Figure II.1 : Illustration de Risque **[28].**

Cette étape permet de déterminer les menaces et d'identifier les sources de menaces. Une menace est une violation potentielle de la politique de service à cause d'une attaque ou d'une action involontaire ou négligente qui compromet la sécurité.

Les sources de menaces peuvent être classées en deux types : les attaques internes et les attaques externes.

Les attaques externes sont lancées par des personnes autres que celle qui participe à l'appel, et ils se produisent généralement quand les paquets VoIP traversent un réseau peu fiable ou l'appel passe par un réseau tiers durant le transfert des paquets.

Les attaques internes s'effectuent directement du réseau local dans lequel se trouve l'attaquant.

II.1.1 Sniffing

Un reniflage (Sniffing) peut avoir comme conséquence un vol d'identité et la révélation d'informations confidentielles. Il permet également aux utilisateurs malveillants perfectionnés de rassembler des informations sur les systèmes VoIP.

L'IP sniffing est une attaque passive, il est décrit comme le suivant,

1. L'intrus est placé sur un réseau.
2. L'intrus met sa station en mode écoute.
3. La station récupère l'ensemble du trafic échangé sur le réseau.
4. L'intrus utilise un analyseur de protocoles réseau à l'insu des administrateurs du réseau.[4]

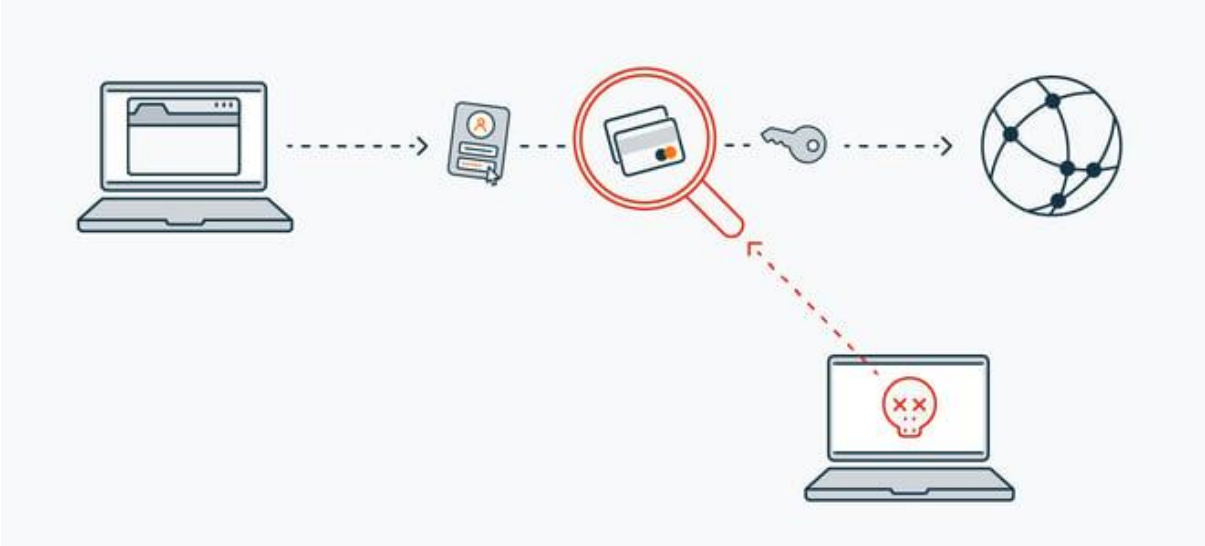


Figure II. 2 : Un renfilage (Sniffing) **[29].**

II.1.2 Suivie des appels

Appelé aussi Call tracking, cette attaque cible les terminaux (soft/hard phone). Elle a pour but de connaître qui est en train de communiquer et quelle est la période de la communication. L'attaquant doit récupérer les messages INVITE et BYE en écoutant le réseau et peut ainsi savoir qui communique, à quelle heure, et pendant combien de temps.

Pour réaliser cette attaque, L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE.

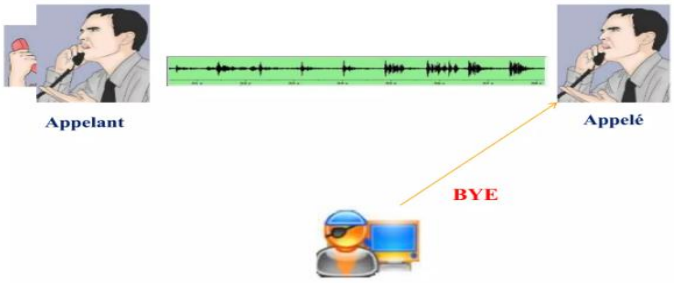


Figure II. 3 : Suivie des appels **[30].**

II.1.3 Injection de paquet RTP

Cette attaque pour but de perturber une communication en cours. L'attaquant devra tout d'abord écouter un flux RTP de l'appelant vers l'appelé, analyser son contenu et générer un paquet RTP contenant un en-tête similaire mais avec un plus grand numéro de séquence et timestamp afin que ce paquet soit reproduit avant les autres paquets (s'ils sont vraiment reproduits). Ainsi la communication sera perturbée et l'appel ne pourra pas se dérouler correctement.

Pour réaliser cette attaque, l'attaquant doit être capable d'écouter le réseau afin de repérer une communication et ainsi repérer les timestamps des paquets RTP.

Il doit aussi être capable d'insérer des messages RTP qu'il a généré ayant un timestamp modifié.

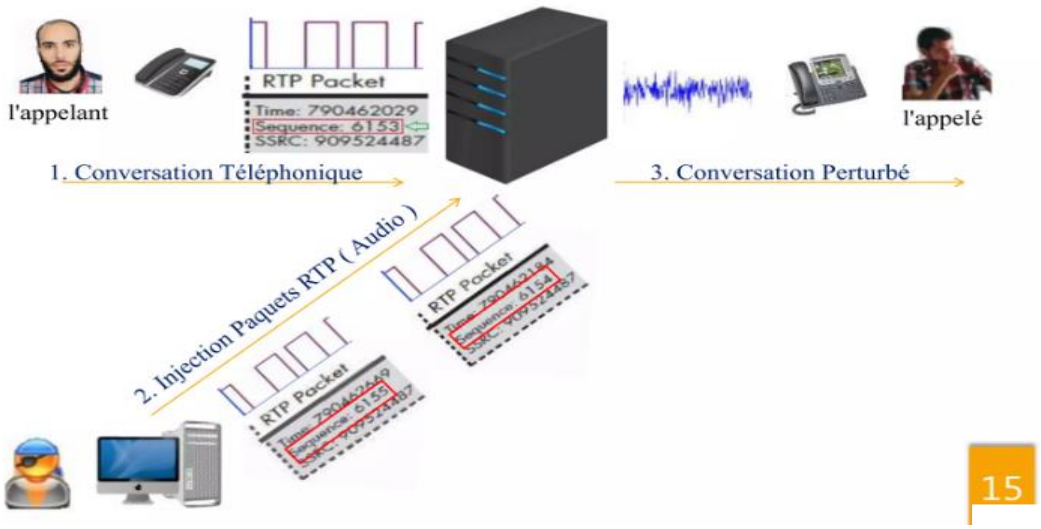


Figure II. 4 : Injection de paquet RTP **[30]**

II.1.4 Le déni de service (DOS : Denial of service)

L'attaque en déni de service consiste à surcharger le serveur Web de requêtes jusqu'à ce qu'il ne puisse plus suivre et s'arrête. Bloquant ainsi les communications internes, externes et aussi le système d'information.

Par exemple un nombre trop important de messages SIP INVITE ou de simples messages ICMP peuvent créer une situation de déni de service. Cette pratique vise à rendre un tel service sur un réseau indisponible, cette attaque peut être effectuée sur plusieurs couches du modèle OSI :

- **Attaque à travers la couche réseau**

*IP Flooding : consiste à envoyer des paquets IP vers une même destination de telle sorte que le traitement de ces paquets empêche une entité du réseau de traiter les paquets IP légitimes.

- **Attaque à travers la couche transport**

* L'UDP Flooding Attacks **:**

Le principe c'est l'envoie d'un grand nombre de requêtes UDP vers une machine pour saturer le trafic transitant sur le réseau.

. Attaque à travers la couche applications

* SIP Flooding : c'est une attaque qui touche les terminaux tels que les téléphones IP via les mécanismes du protocole SIP et les attaques DOS citant :

II.1.4.1 Attaque dos via la requête CANCEL

C'est un exemple de déni de service lancé contre l'utilisateur, l'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive à un utilisateur spécifique.

Une fois que l'utilisateur reçoit la requête INVITE par son dispositif, alors l'attaquant envoie immédiatement une requête CANCEL, cette requête provoque une erreur sur le dispositif de l'appelé et bloque l'appel. [4]

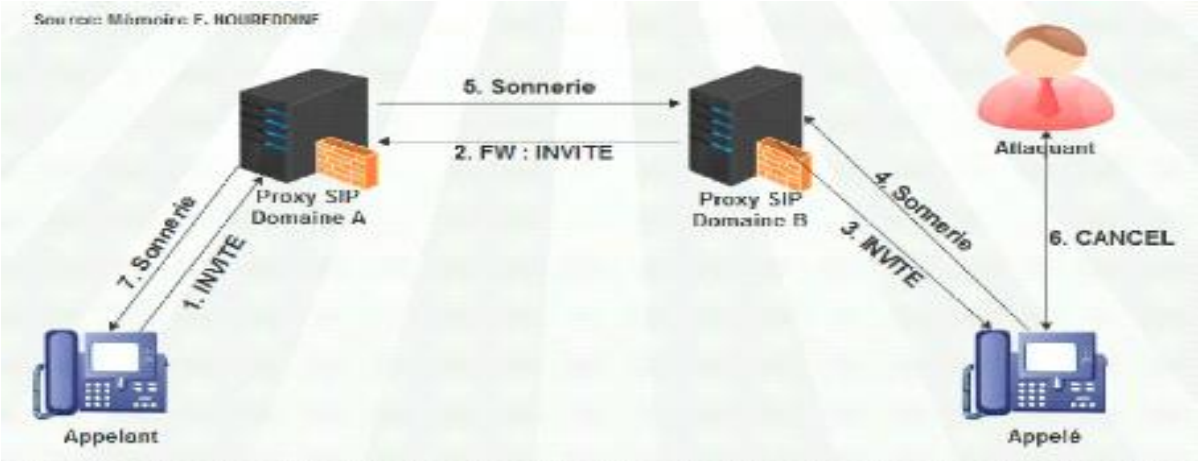


Figure II. 5 : Attaque Dos avec la méthode cancel **[31].**

II.1.5 L'écoute clandestine

L'écoute clandestine d'une conversation téléphonique. Un attaquant avec un accès au réseau VoIP peut sniffer le trafic et décoder la conversation vocale.

Le principe de l'écoute clandestine est montré dans la figure II.6 comme suit :

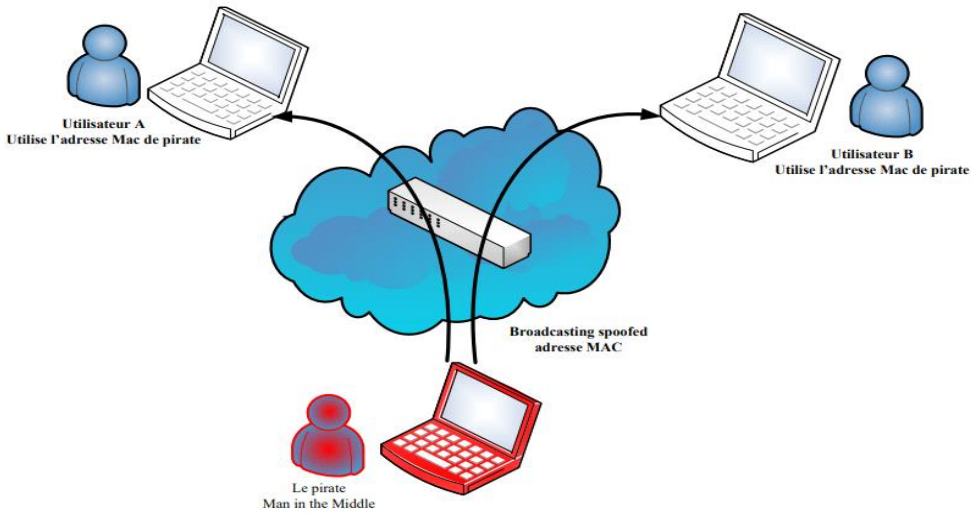


Figure II. 6 : Exemple de détournement d'appel " Man in the middle" **[15].**

1. Déterminer les adresses MAC des victimes (client-serveur) par l'attaquant
2. Envoi d'une requête ARP non sollicités au client, pour l'informer du changement de l'adresse MAC du serveur VoIP à l'adresse MAC.
3. Envoi d'une requête ARP non sollicités au serveur, pour l'informer du changement de l'adresse MAC du client à l'adresse MAC.
4. Désactiver la vérification des adresses MAC sur la machine d'attaque afin que le trafic puisse circuler entre les 2 victimes.

II.2 Eléments de sécurité

Figure II. 7 : Eléments de sécurité **[32].**

Pour éviter les attaques énumérées ci-haut, nous allons vous présenter dans ce point les bonnes pratiques de sécurités et les mesures de sécurités de la VoIP.

On a déjà vu que les vulnérabilités existent au niveau protocolaire, application et systèmes d'exploitation.

Pour cela, on a découpé la sécurisation aussi en trois niveaux : Sécurisation protocolaire, sécurisation de l'application.

II.2.1 Sécurisation protocolaire

La prévalence et la facilité de sniffer des paquets et d'autres techniques pour la capture des paquets IP sur un réseau pour la voix sur IP fait que le cryptage soit une nécessité. La sécurisation de la VoIP est à la protection des personnes qui sont interconnecté.

IP sec peut être utilisé pour réaliser deux objectifs. Garantir l'identité des deux points terminaux et protéger la voix. VOIPsec (VoIP utilisant IPsec) contribue à réduire les menaces, les sniffeurs de

paquets, et de nombreux types de trafic « vocal analyze ». Combiné avec un pare-feu, IPsec fait que la VOIP soit plus sûr qu'une ligne téléphonique classique.

Il est important de noter, toutefois, que IPsec n'est pas toujours un bon moyen pour certaines applications, et que certains protocoles doivent continuer à compter sur leurs propres dispositifs de sécurité.

II.2.1.1 VoIP VPN

Un VPN VoIP combine la voix sur IP et la technologie des réseaux virtuels privés pour offrir une méthode assurant la préservation de la prestation vocale. Puisque la VoIP transmet la voix numérisée en un flux de données, la solution VPN VoIP semble celle la plus approprié vu qu'elle offre le cryptage des données grâces a des mécanismes de cryptages, puisqu'elle permet d'offrir l'intégrité des paquets VoIP.

Cryptage aux points terminaux : Vu que notre objectif est d'assurer la confidentialité et l'intégrité des clients, la nécessité de concevoir des mécanismes d'authentifications et de chiffrement pour IP. Puisqu'il sécurise le paquet comme un tout (contrairement en mode transport qui ne sécurise que le Payload IP).

Le mode tunnel (réseau privé virtuel sécurisé), se base sur l'encapsulation de tout le paquet IP et ajoute un nouvel entête pour l'acheminement de ce dernier, et l'authenticité des paquets reçus assurée par l'utilisation d'IPSec (Internet Protocol Security) entre les machines concernées.

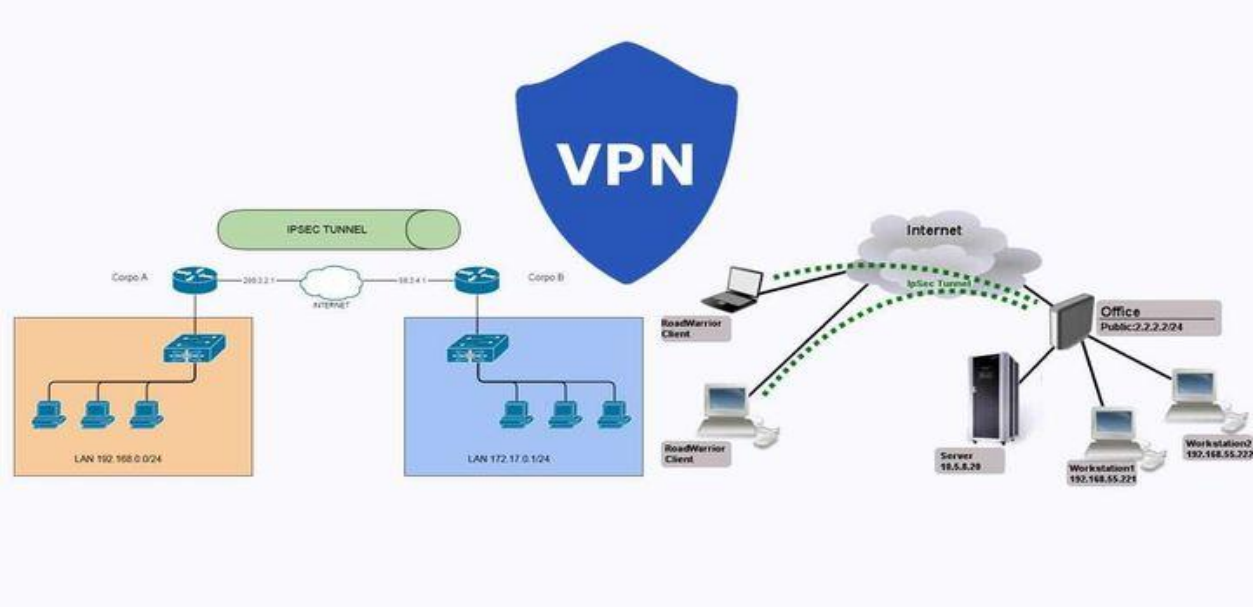


Figure II. 1 : VoIP VPN **[33].**

II.2.2 Protocole TLS.

C'est un protocole de sécurisation des échanges au niveau de la couche transport (TLS : Transport Layer Security). TLS, anciennement appelé Secure Sockets Layer (SSL), est un protocole de sécurisation des échanges sur Internet.

C'est un protocole modulaire dont le but est de sécuriser les échanges des données entre le client et le serveur indépendamment de tout type d'application. TLS agit comme une couche supplémentaire au-dessus de TCP **[15].**

Le protocole SSL et TLS est subdivisé en quatre sous protocoles (Figure II.9) :

- Le protocole Handshake : C'est un protocole qui permet au client et au serveur de s'authentifier mutuellement, de négocier les algorithmes de chiffrement, de négocier les algorithmes de MAC (Message Authentification Code) et enfin de négocier les clés symétriques qui vont servir au chiffrement.
- Le protocole Change Cipher Spec : Ce protocole contient un seul message : change_cipher_spec. Il est envoyé par les deux parties au protocole de négociation. Ce message transite chiffré par l'algorithme symétrique précédemment négocié.
- Le protocole Alert: 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.
- Le protocole Record : Ce protocole chapeaute les autres protocoles de SSL et TLS, en fournissant une interface unifiée pour la transmission des données.

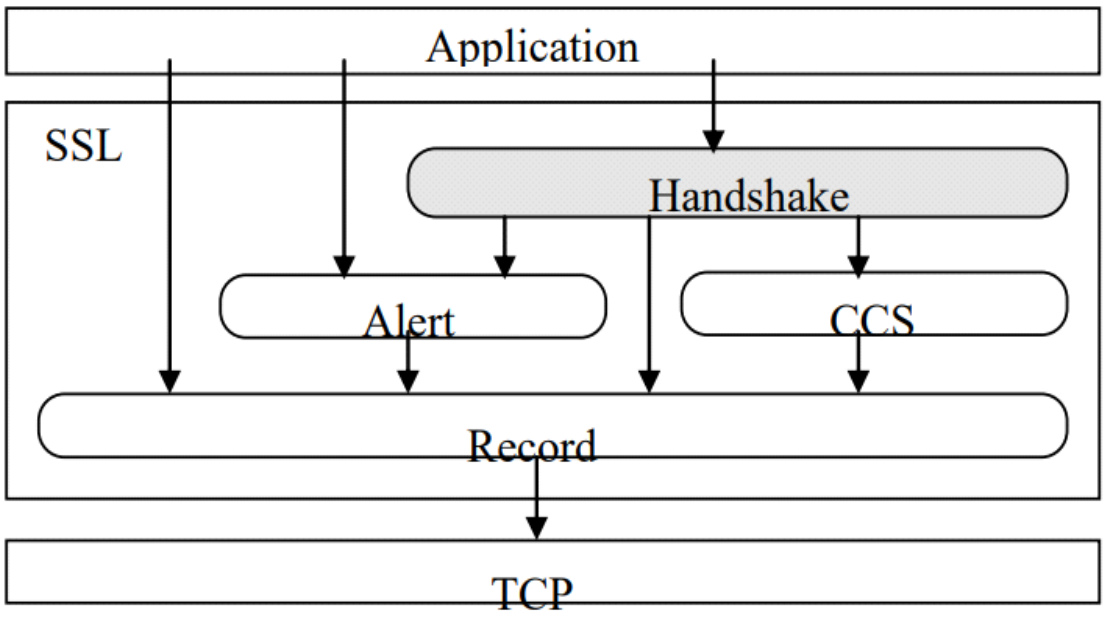


Figure II. 9 : Empilement des sous-couches protocolaires de SSL[**15].**

II.2.3 Secure RTP (SRTP)

SRTP est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPsec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il aussi est bâti sur le protocole temps réel RTP (Real Time Transport Protocol).

Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session on de voix sur IP tel que SIP (Session Initiation Protocol), ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP (Real Time Streaming Protocol). Mais, surtout, il s'adjoint les services du protocole de gestion de clé MIKEY (Multimedia Internet KEYing).

II.2.4 Service de sécurités offertes par SRT

Rendre confidentielles les données RTP, que ce soit l'en-tête et la charge utile ou seulement la charge utile.

Authentifier et vérifier l'intégrité des paquets RTP. L'émetteur calcule une empreinte du message à envoyer, puis l'envoie avec le message même.

La protection contre le rejeu des paquets.

Chaque récepteur tient à jour une liste de tous les indices des paquets reçus et bien authentifiés. Protocole de sécurisation des échanges sur Internet. C'est un protocole modulaire dont le but est de sécuriser les échanges des données entre le client et le serveur indépendamment de tout type d'application. TLS agit comme une couche supplémentaire au-dessus de TCP.

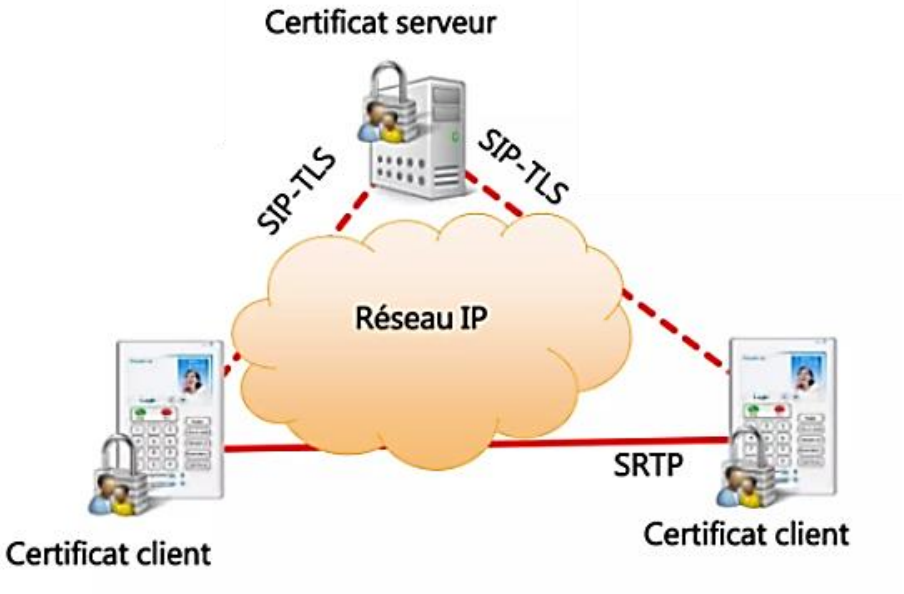


Figure II. 10 : Service de sécurités offertes par SRTP **[31].**

II.2.5 L'authentification :

L'une de méthode les plus importantes pour anticiper une attaque sur un système de téléphonie est de déterminer clairement l'identité des périphériques ou des personnes participant à la conversation.

Plusieurs solutions simples sont mises en œuvre pour cela, il est recommandé d'utiliser des mots de passe complexes lors de la configuration des clients SIP ; en effet, il faut savoir que certains hackers développent des robots en charge de sonder les réseaux informatiques et dès que l'un d'entre eux réponds au protocole SIP, un algorithme sophistiqué est engagé et teste toutes les combinaisons possibles de mots de passe **[7].**

Ainsi, il faut éviter

- Les mots de passes trop courts
- Les suites numériques (123456) ou alphabétiques (abcd)
- Les suites logiques tels prénoms ou dates

- Un mot de passe unique pour toutes les extensions SIP.

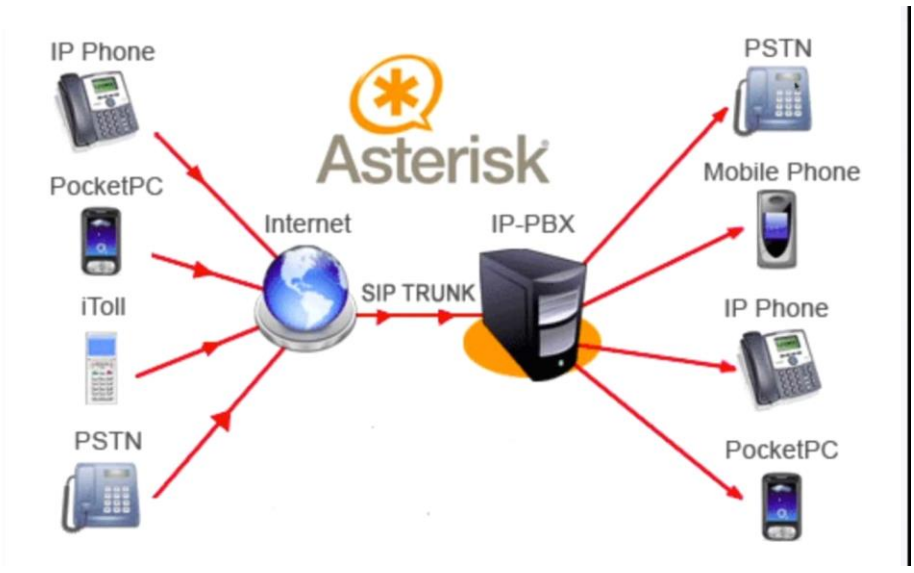
La confidentialité des mots de passes est primordiale : lors de la configuration des téléphones ou des softphones sur site, il est impératif d'être discret au moment de la saisie des mots de passe, et bien entendu de ne pas les communiquer aux utilisateurs **[15].**

II.3 Conclusion

Dans ce chapitre, nous avons présentés les vulnérabilités les plus importants et comment doit-on procéder pour y faire faces, tout en préconisant un certain nombre de mesures de sécurités devant être prises en compte dans le but de garantir la qualité de service du réseau ainsi que sa sécurité.

Chapitre III Installation et configuration

D'Asterisk pour la VoIP.



Introduction

Asterisk est un PABX open source pour systèmes UNIX originellement crée en 1999 par Mark Spencer fondateur de la société Digium. Asterisk est publié sous licence GPL. Asterisk permet, entre autres, la messagerie vocale, les conférences, les files d'attente, les agents d'appels, les musiques d'attente et les mises en garde d'appels ainsi que la distribution des appels. Toutes ces fonctionnalités standards sont intégrées directement au logiciel.

Asterisk implémente les protocoles H.320, H.323 et SIP, ainsi qu'un protocole spécifique nommé IAX (Inter-Asterisk eXchange). Ce protocole IAX permet la communication entre deux serveurs Asterisk ainsi qu'entre client et serveur Asterisk. Asterisk peut également jouer le rôle de registrar et passerelle avec les réseaux publics (RTC, GSM, etc.). Asterisk est extensible par des scripts ou des modules en Perl, en C, en Python, en PHP....**[34].**

III.1 Historique

Asterisk est né en 1999, créé par un étudiant de l'université d'Auburn (États-Unis - Alabama). À la recherche d'un commutateur téléphonique privé pour créer un centre de support technique sur Linux, il est dissuadé par les tarifs trop élevés des solutions existantes, et décide de se créer son propre routeur d'appels sous Linux : le PBX Asterisk. Quelques temps après, il crée la société Digium, fournisseur de cartes FXO et FXS compatibles avec Asterisk **[34] .**

III .2 L'architecture d'Asterisk

Asterisk est conçu pour un maximum de flexibilité. Pour cela des API (Application Programming Interface ou interface de programmation) spécifiques sont définis autour d'un noyau central de commutation. Le noyau s'occupe des interconnections internes du PABX IP sans tenir compte des protocoles, codecs et du matériel utilisés, ce qui autorise Asterisk à utiliser tous le matériel et les technologies appropriés déjà existants ou futurs

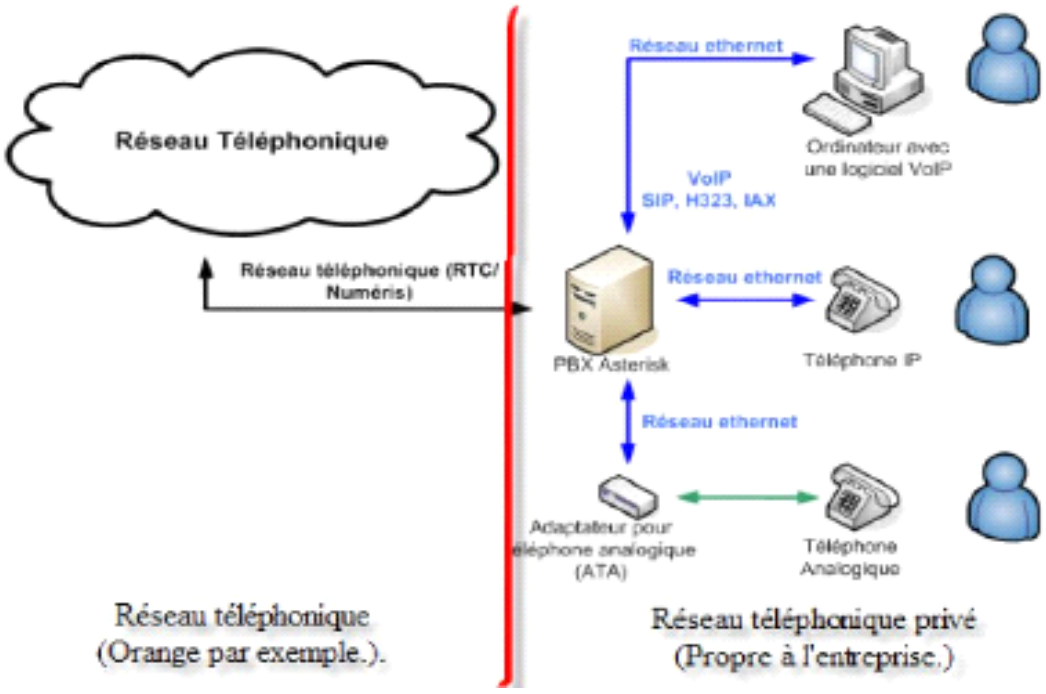


Figure III .1 L'architecture d'Asterisk **[35].**

III.3 Fonctionnalités Asterisk

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

Asterisk a le rôle d'un middleware entre les technologies de téléphonie VOIP (TDM, SIP …) et les applications (conférence, messagerie vocale, …). Ce PBX est base sur le protocole IP. Donc les communications et les paquets échanges sont transportés sous forme plusieurs protocoles de la voix qu'on veut (SIP, IAX, H.323, ADSI, MGCP). Au sein des grandes installations d'Asterisk, il est courant SEN-TR Asterisk de déployer les fonctionnalités sur plusieurs serveurs. Une unité centrale ou plus seront dédiées au traitement des appels et seront épaulées par des serveurs auxiliaires traitant les tâches secondaires (comme une base de données, les boîtes vocales, les conférences) **[35].**

Des modules tiers permettent de visualiser ou paramétrer le PBX via une interface Flash ou via un client léger. Enfin, notez qu'une distribution particulière d'Asterisk, Asterisk NOW, est dédiée au PBX léger sur un réseau domestique.

III.3.1 Caractéristiques ASTERISK

Offre toutes les fonctions d'un PBX et ses services associent :

- La conférence téléphonique.
- Les répondeurs interactifs.
- La mise en attente d'appels.
- La distribution des appels.
- Les mails vocaux.
- La musique d'attente.

La génération d'enregistrement d'appels pour l'intégration avec des systèmes de facturation. Asterisk fonctionne sur les principaux systèmes d'exploitation (Linux, BSD, Windows, Mac OS X).

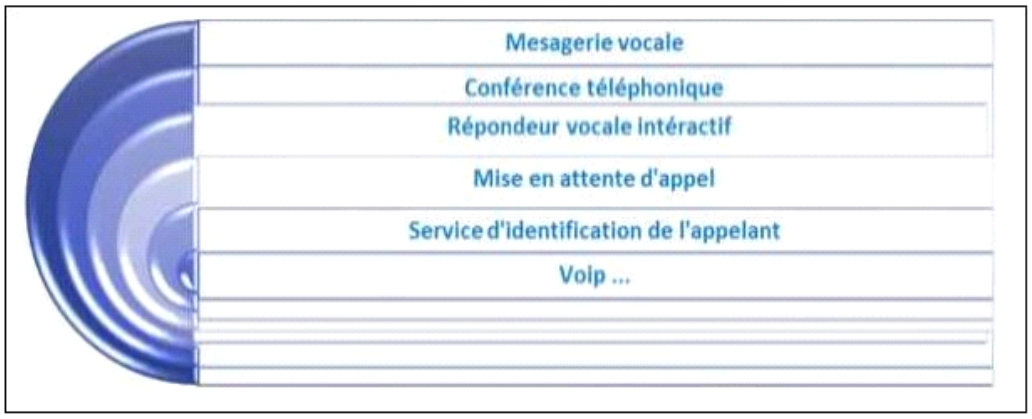


Figure III .*2* *Caractéristiques* ASTERISK**. [35]**

III .4 Architecture de la maquette de test

Figure III.3 : Architecture de la maquette locale VoIP avec un IPBX Asterisk

Cette architecture est composée d'un serveur Asterisk installé sous une distribution linux (Ubuntu) et des terminaux qui peuvent être des téléphones IP ou des softphone installer sur des PC et des téléphones portables.

A Mise en place d'un PABX-IP avec Asterisk

III .5 Installation du serveur ASTERISK

III.5.1: Les étapes d'installation :

a- La Workstation VMware Pro :

Figure III.4: VMware Workstation Pro.

- **Definition :**

VMware Workstation est un logiciel de virtualisation développé par VMware. Il permet de créer des machines virtuelles sur un seul ordinateur physique, ce qui est idéal pour tester de nouveaux logiciels ou des architectures complexes de systèmes d'exploitation avant de les déployer sur des machines physiques[36].

- **Système d'exploitation et processeur supportés :**

Nous pouvons installer VMware Workstation sur les systèmes d'exploitation hôtes Windows et Linux. Notre système hôte doit disposer d'un processeur x86 64 bits avec une fréquence de 1,3 GHz au minimum et assurer que les systèmes multiprocesseurs sont pris en charge.

Lorsque nous installons VMware Workstation, le programme d'installation effectue des contrôles pour vérifier que notre système hôte dispose d'un processeur pris en charge [36] .

- **Installation de la Workstation VMware pro :**

Pour faire nous allons suivre les étapes suivantes :

- **Téléchargement de VMware Workstation Player :**

Nous allons se connecter sur le site officiel de VMware et téléchargez la version idéale de VMware Workstation Pro pour notre système d'exploitation.

- **Exécution du fichier d'installation :**

Une fois le téléchargement terminé, nous allons ouvrir le fichier d'installation. Nous devons confirmer que vous souhaitons autoriser cette application à apporter des modifications à notre appareil.

- **Suivre l'assistant d'installation :**

- Accepter les termes du contrat de licence.
- Choisir les options d'installation par défaut.

- **Utilisation de VMware Workstation Pro :**

Une fois installé, nous allons exécuter le programme pour accéder a son interface, une fois ouvert, nous pouvons maintenant créer des nouvelles machine virtuelles en utilisant un fichier ISO de cette dernière.

b- Ubuntu :

Figure III.5 : La distribution LINUX (Ubuntu).

Pour l'installer nous devons suivre ces étapes :

1-Téléchargement du fichier ISO de Ubuntu :

Nous allons diriger vers le site officiel d'Ubuntu https://ubuntu.com

Puis vers la section téléchargement et nous allons sélectionner la version la plus récente d'Ubuntu server puisqu'elle est la plus fluide que celle du desktop.

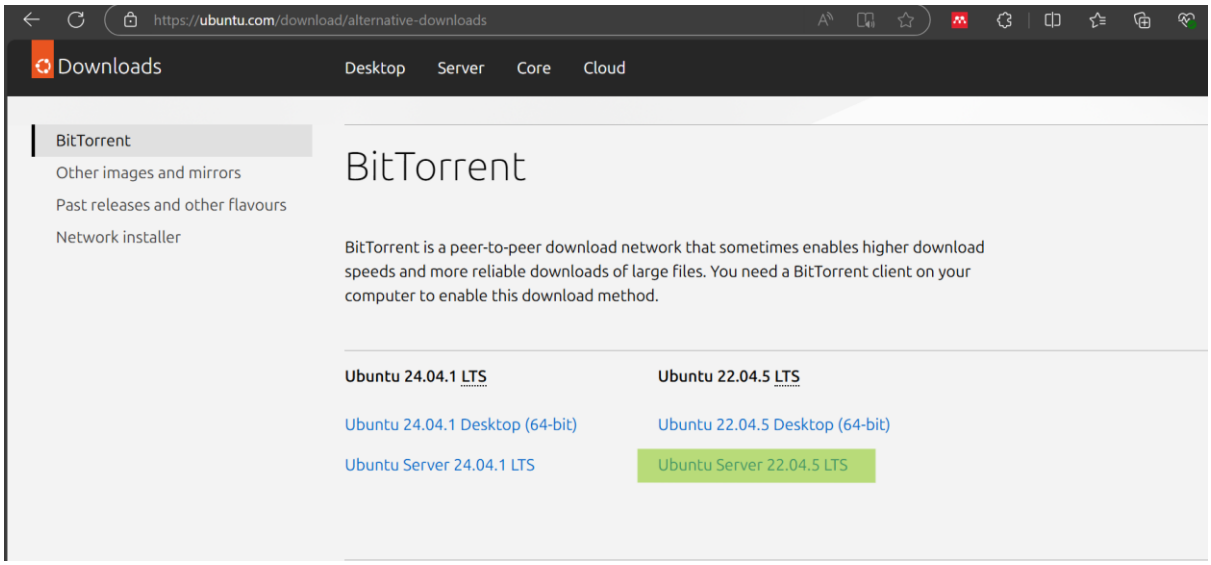


Figure III.6 : Le fichier iso d'Ubuntu à télécharger.

- **Installation d'Ubuntu sur VMware Pro :**

Pour faire cela nous suivrons ces étapes :

- **On lance VMware et on clique sur "créer une nouvelle machine virtuelle"**

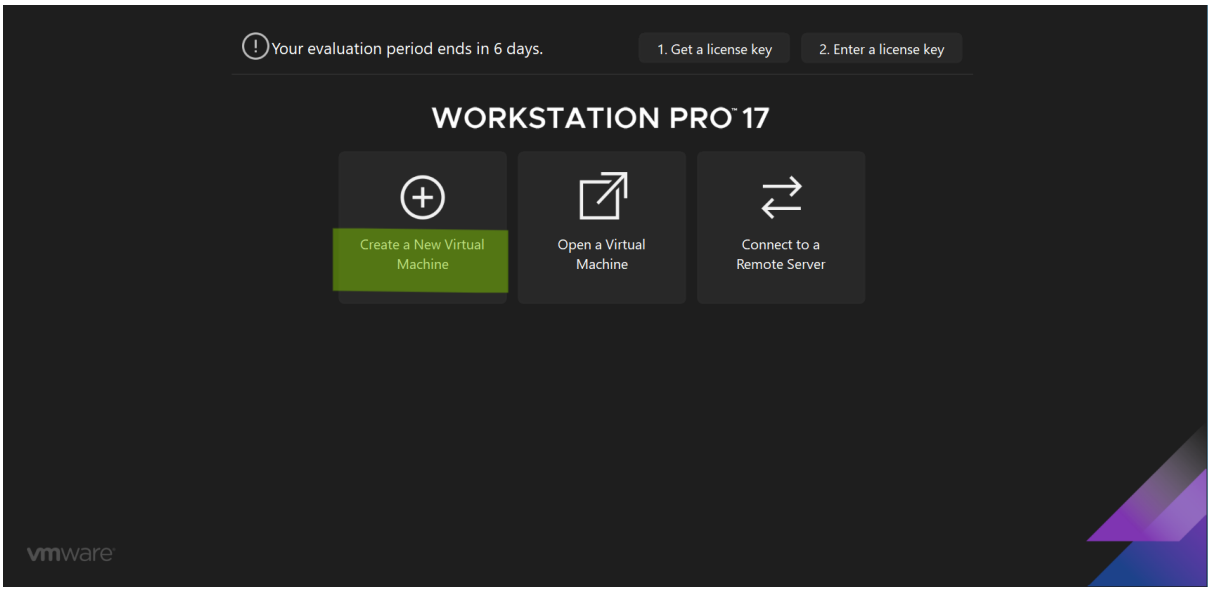


Figure III.7 Interface VMware

- **On choisi la configuration par défaut pour la création de la machine virtuelle, et la versions 17.5.x celle qui compatible avec notre système d'exploitation.**

Figure III.8 Choix de configuration par défaut

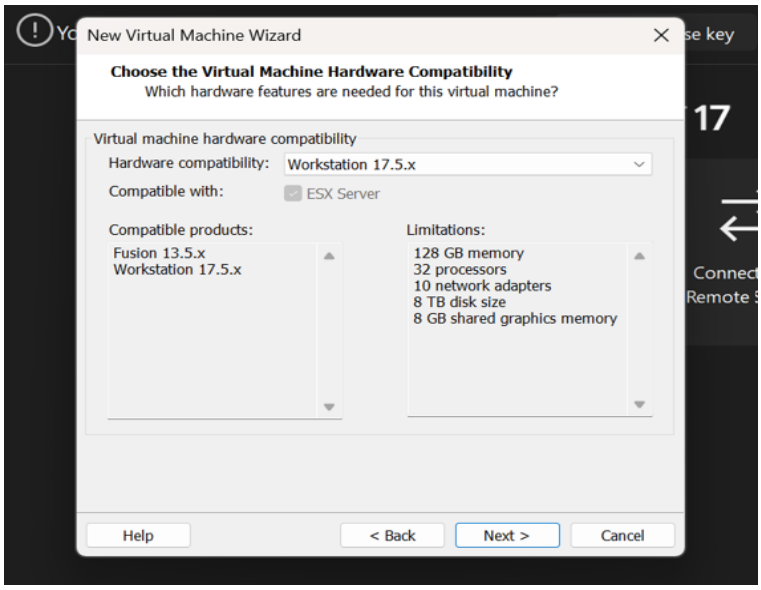


Figure III.9 Sélection de la version compatible

- **On va insérer le fichier ISO d'Ubuntu qu'on a télécharger dans notre machine puis on appuie sur suivant.**

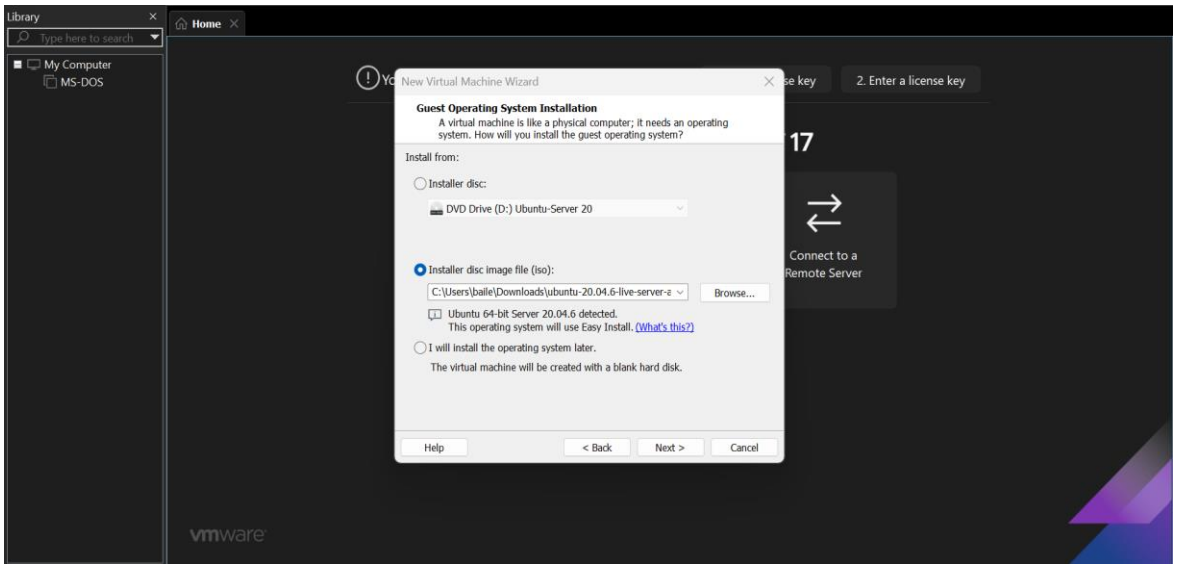


Figure III.10 Sélection du fichier ISO d'Ubuntu

- **Dans l'étape qui suit on va personnaliser notre LINUX en remplissant nos coordonnées :**

- **Fullname : ubuntu**
- **Username : ubuntu**
- **Password : ubuntu24**

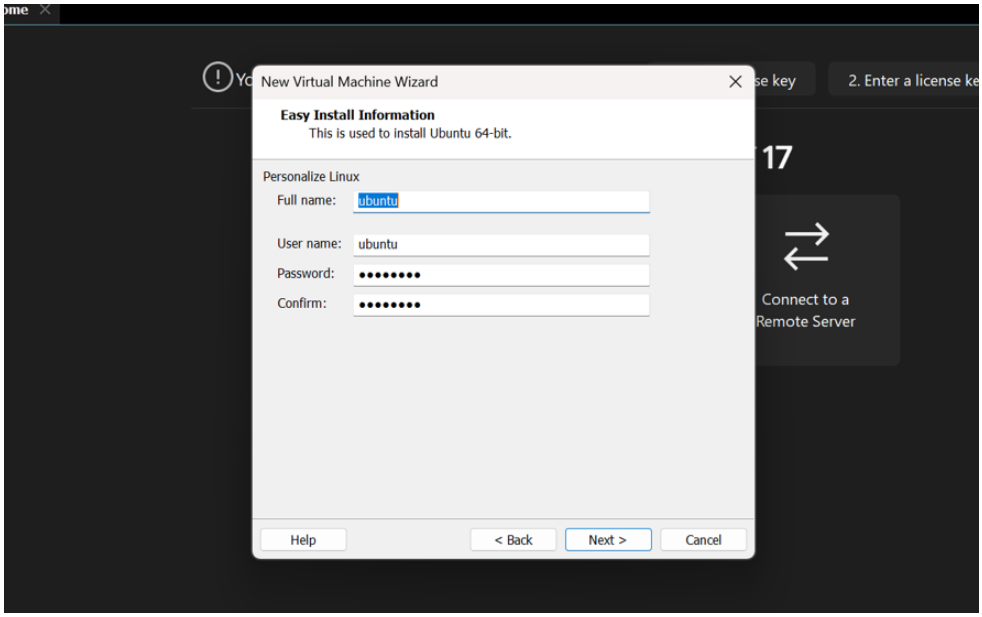


Figure III.11 Personnalisation de LINUX

- **Une fois fini, on passe à l'étape de donner à notre machine virtuelle la taille de mémoire quelle utilisera pour son bon fonctionnement.**

On a choisi 4GB.

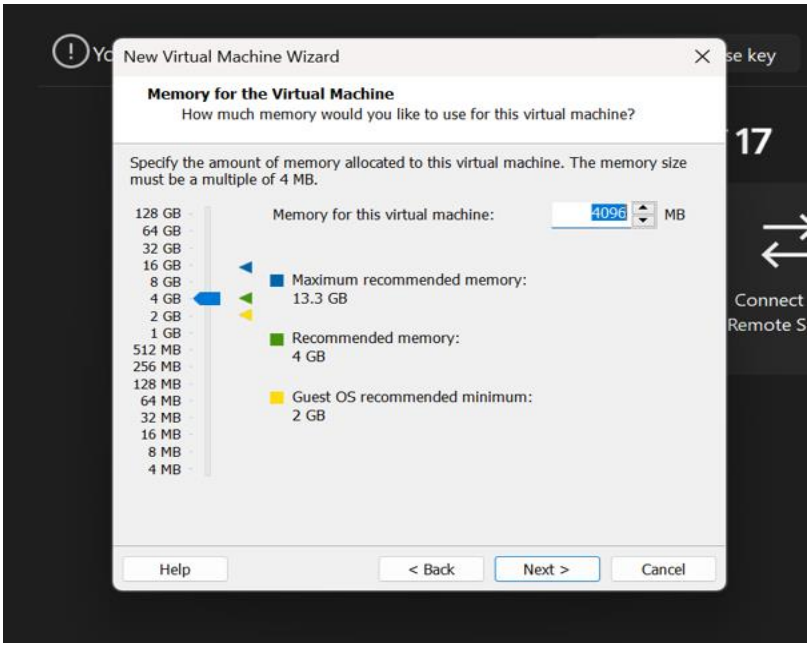


Figure III.12 Sélection de la taille de mémoire

- **Ensuite on sélection le type de connexion réseau que notre machine utilisera.**

On a choisi le (NAT) Network Address Translation.

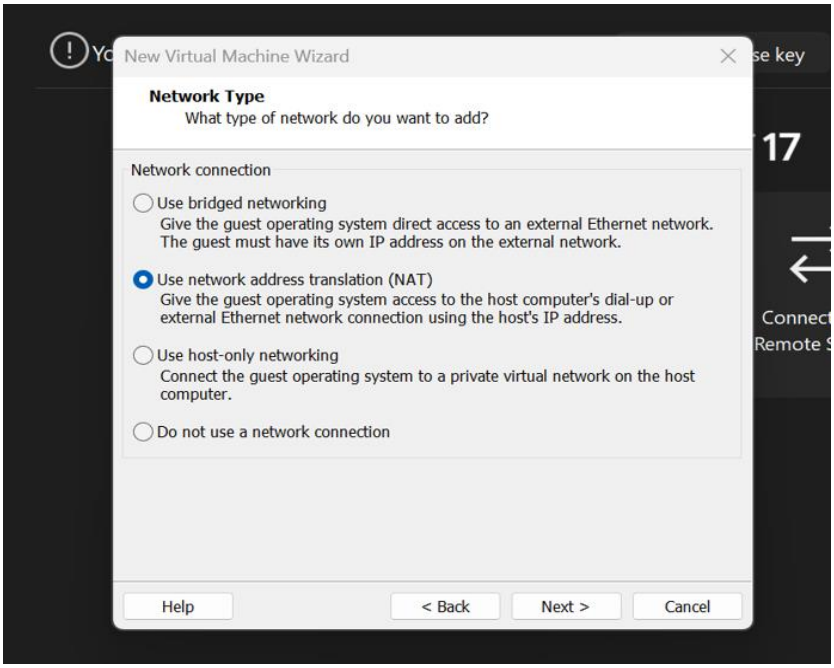


Figure III.13 Choix de connexion réseau

- **Ensuite on fait les étapes suivantes pour la création de notre disque virtuel :**

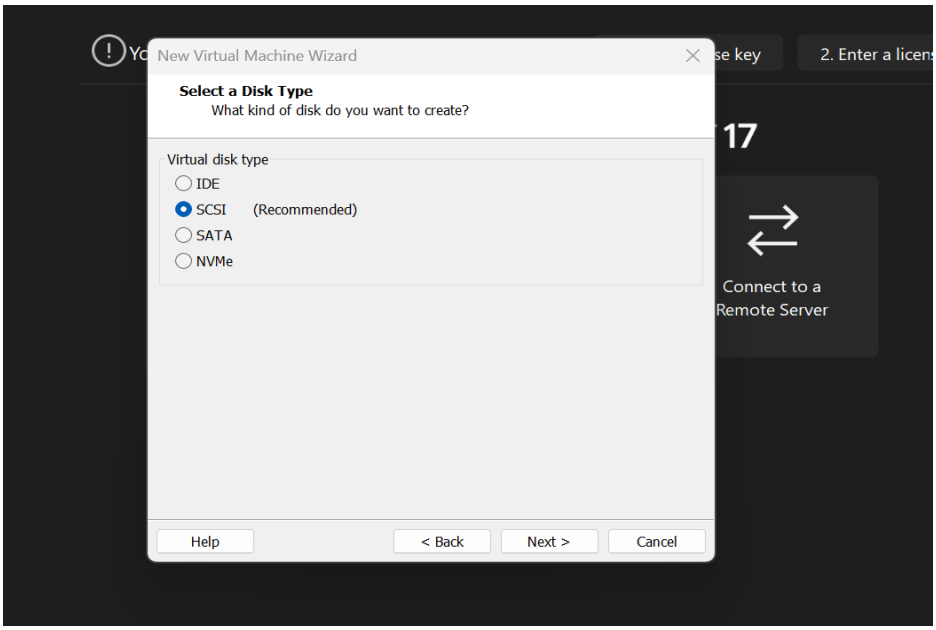


Figure III.14 Sélection du type de disque

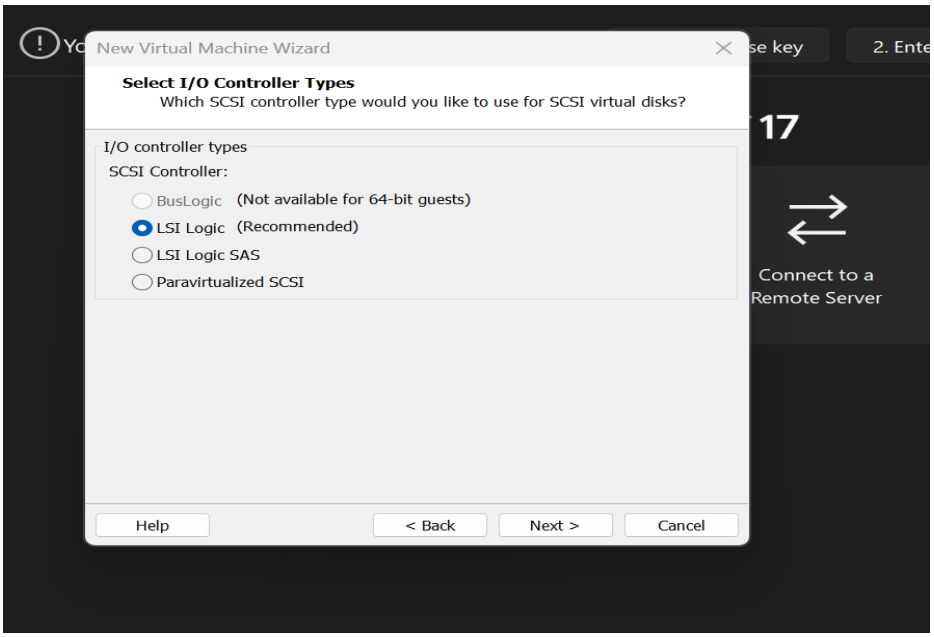


Figure III.15 Sélection du type de disque SCSI

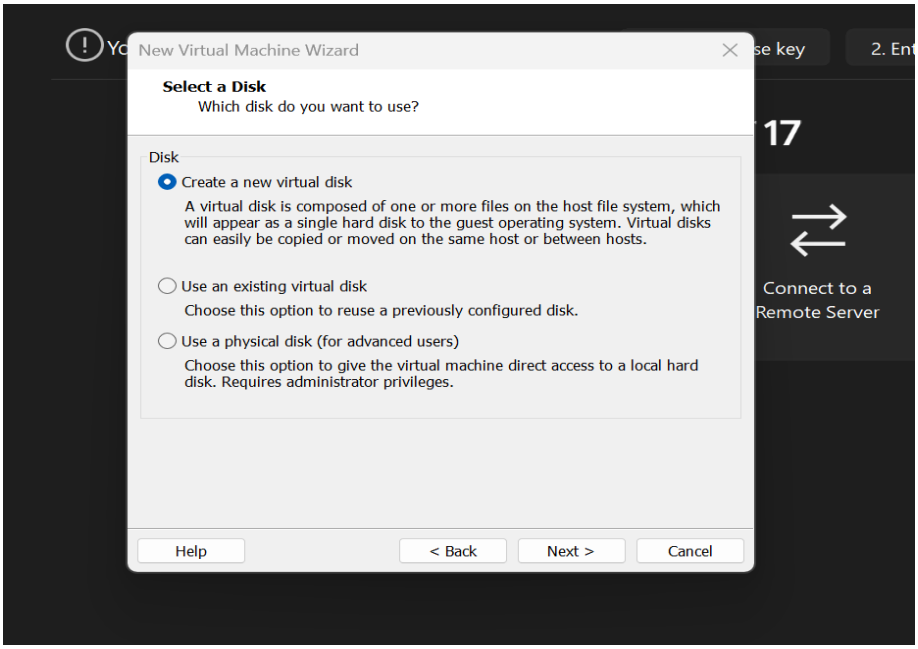


Figure III.16 Création d'un nouveau disque virtuel

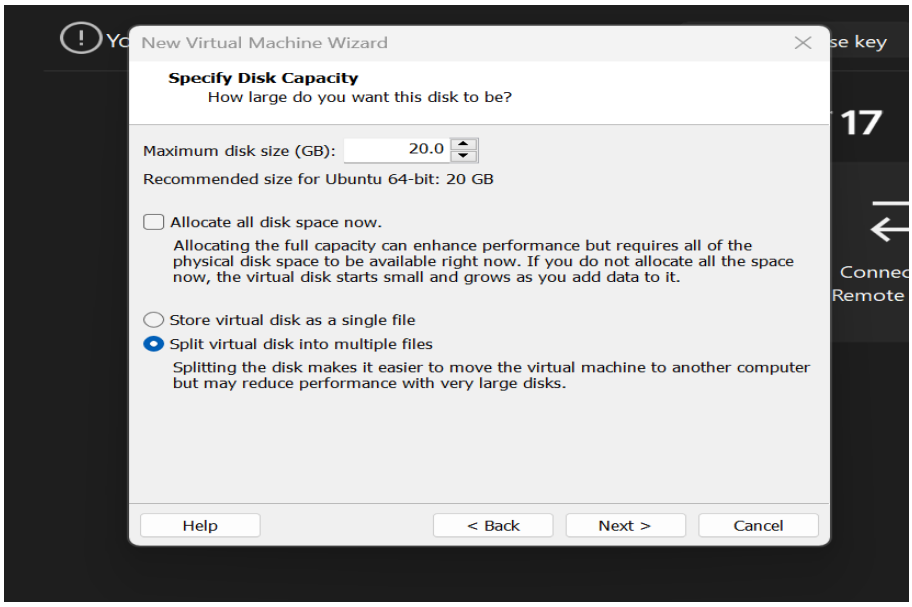


Figure III. 17 Choix de la capacité du disque virtuel

Dans cette étape on a donné un stockage de 20GB pour notre disque et on a choisi de le diviser en plusieurs fichiers, pour facilite son déplacement d'une machine à une autre.

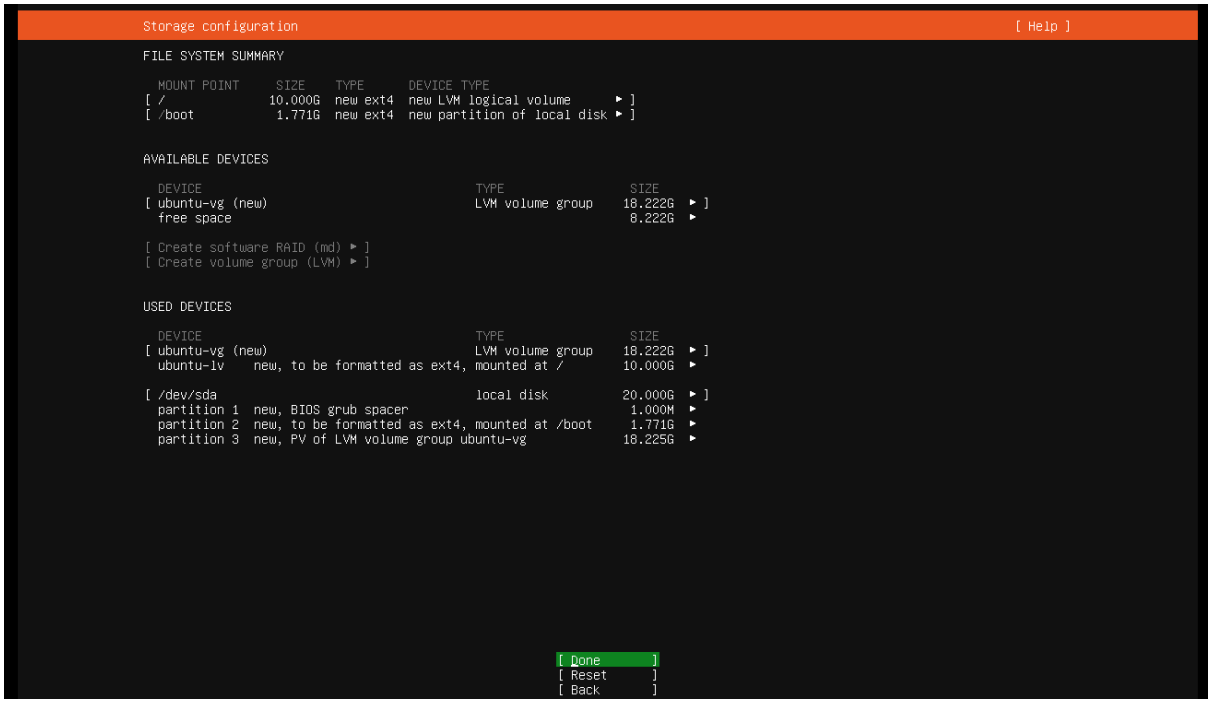


Figure III.18 L'aperçu de toutes les informations de notre système

Maintenant on est arrivé à l'étape finale on clique sur « done » pour lancer l'installation notre Ubuntu LINUX serveur.

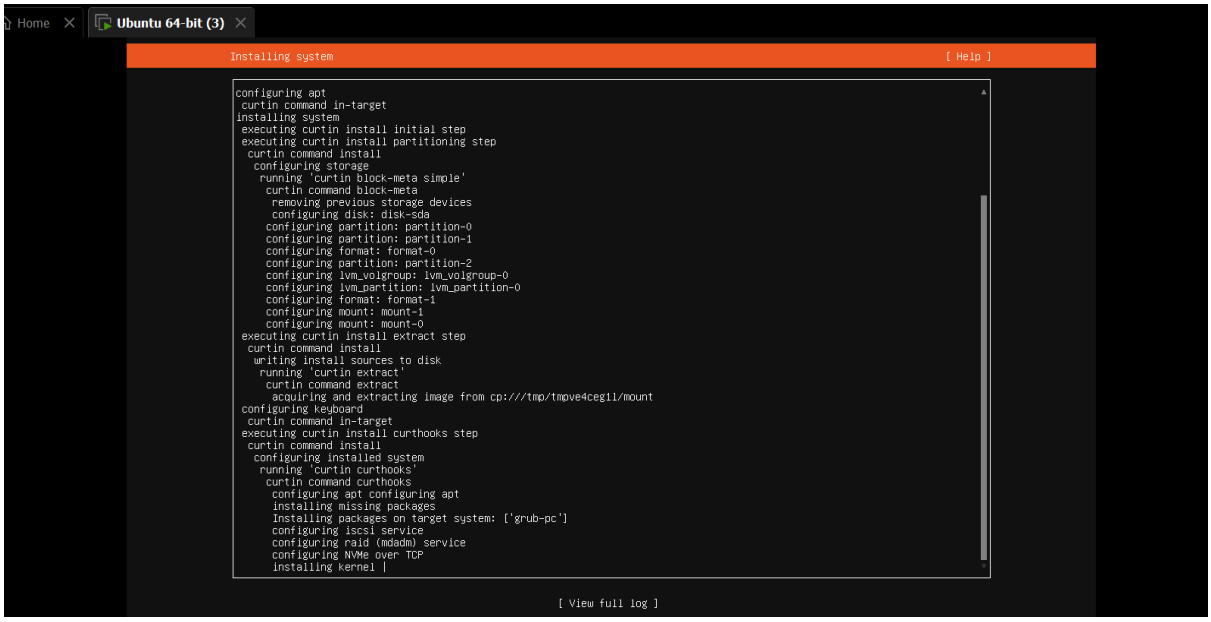


Figure III.19 Processus d'installation de Ubuntu

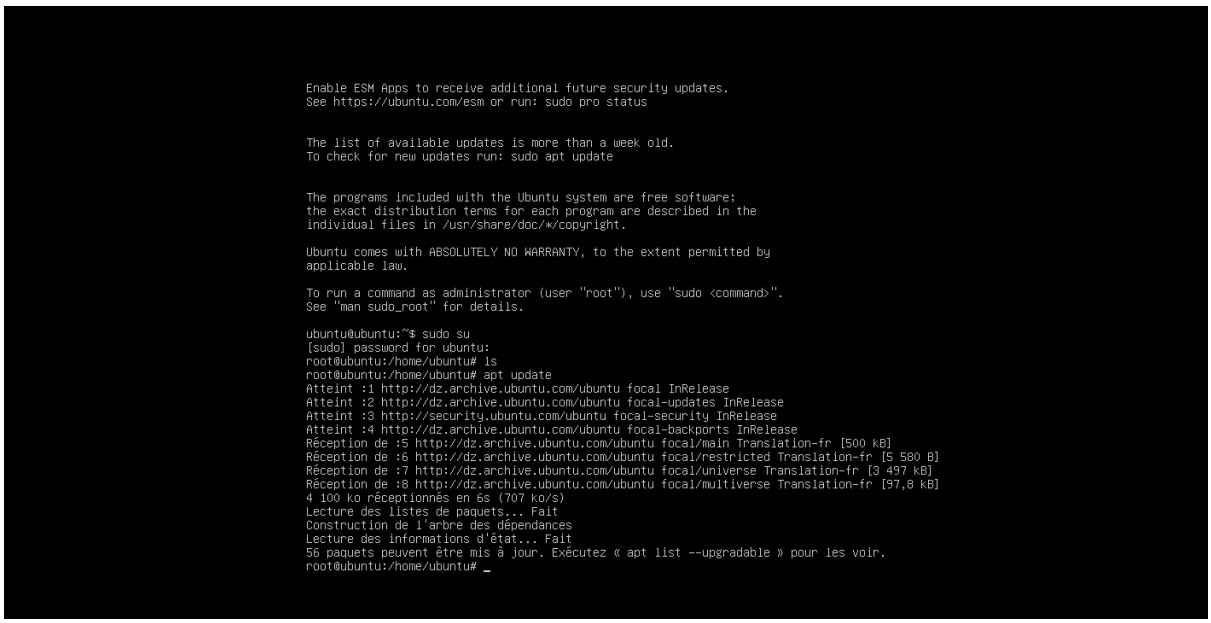


Figure III.20 Interface du serveur LINUX Ubuntu

c- Le Serveur Asterisk :

1.Compatibilité du système :

Le serveur qui héberge la plate-forme Asterisk est un serveur GNU/Linux fonctionnant avec un système d'exploitation Ubuntu

2.Préparation à l'installation :

On commence par mettre à jour notre distribution pour cela on utilisera les commandes suivantes

```
sudo apt-get update
sudo apt-get upgrade
```

3.Installation d'astiresk :

On tape la commande :

```
sudo apt-get install asterisk
```

```
root@hp-VMware-Virtual-Platform:/home/hp# apt install asterisk
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
asterisk est déjà la version la plus récente (1:20.6.0~dfsg+~cs6.13.40431414-2build5).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 3 non mis à jour.
```

Apres l'installation on modifie ces parametres pour que Asterisk démarre a l'allumage de l'ordinateur `sudo vim /etc/default/asterisk`

Ensuite on installe les paquets français d'asterisk avec la commande :

```
sudo apt-get install asterisk-prompt-fr
```

Rmq :

*- Il y a deux façons d'installer **Asterisk** sur une distribution à base de Debian, la première via le gestionnaire de paquet de Debian, la seconde en compilant directement la dernière version d'**ASTERISK**.*

*- Pour pouvoir disposer de la dernière version d'**ASTERISK**, il est recommandé de l'installer en compilant ses sources.*

III.6 Configuration du serveur ASTERISK

1 Sauvegarde des fichiers de configuration par défaut :

Apres installation, on se déplacera dans le répertoire « **/etc/asterisk** »

Pour configurer notre serveur Asterisk nous allons modifier les fichiers suivants :

- ✓ Le fichier **sip.conf**: pour la configuration générale d'Astérisque.
- ✓ Le fichier **extensions.conf**: pour la configuration du Plan de numérotation. **Dialplan (plan d'appel).**
- ✓ Le fichier **users.conf:** pour la configuration des utilisateurs.

C'est des fichiers se trouvent dansle dossier**/etc/astérisque**

III.6.1 Configuration générale d'Asterisk(Sip.conf) :

Nous allons commencer par éditer le fichier sip.conf qu va nous permettre pour l'instant de mettre les sons par défauts en Français.

Recherchez la ligne : langue=en Et remplacez la part : langue=fr

A chaque fois que vous modifiez un fichier deconfil faut recharger ce fichier de configuration dans Astérisque.

Dans la console d'Asterisk il vous suffit de taper la commande : recharger cette commande permet de recharger les fichiers de configurationsd'Astériksans redémarrer le serveur.

III.6.2Création des comptes utilisateurs

La création des utilisateurs se fait donc dans le fichier **users.conf**.

Voici le contenu de fichier **users.conf** avec deux utilisateurs **Amine** et **Malha** avec comme numéros respectifs le 1001 et le 1002.

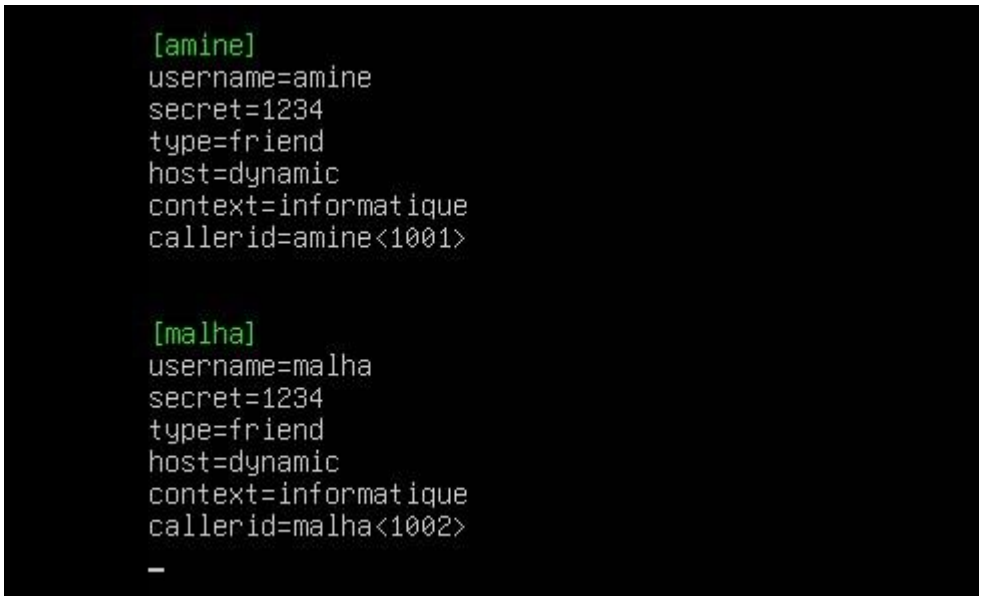


Figure III.21 Création des comptes utilisateurs

1 Explications sur la capture précédente :

- ✓ Username => Si Asterisk agit entre un client SIP et un serveur SIP distant, ce champ est utilisé pour authentifier le message INVITE envoyé par Asterisk au serveur (Identifiant de l'utilisateur)
- ✓ Type => il existe 3 types d'utilisateurs :
  - **- user** = peut appeler mais ne peut pas recevoir d'appel
  - **- peer** = peut recevoir des appels
  - **- friend** = peut appeler et recevoir des appels
- ✓ Secret => Mot de passe de l'utilisateur
- ✓ Host => - dynamic : Le client s'enregistre auprès du serveur
- ✓ Context => Contexte (Utiliser dans le fichier extensions.conf)

Une fois le fichier **users.conf** *enregistrée*

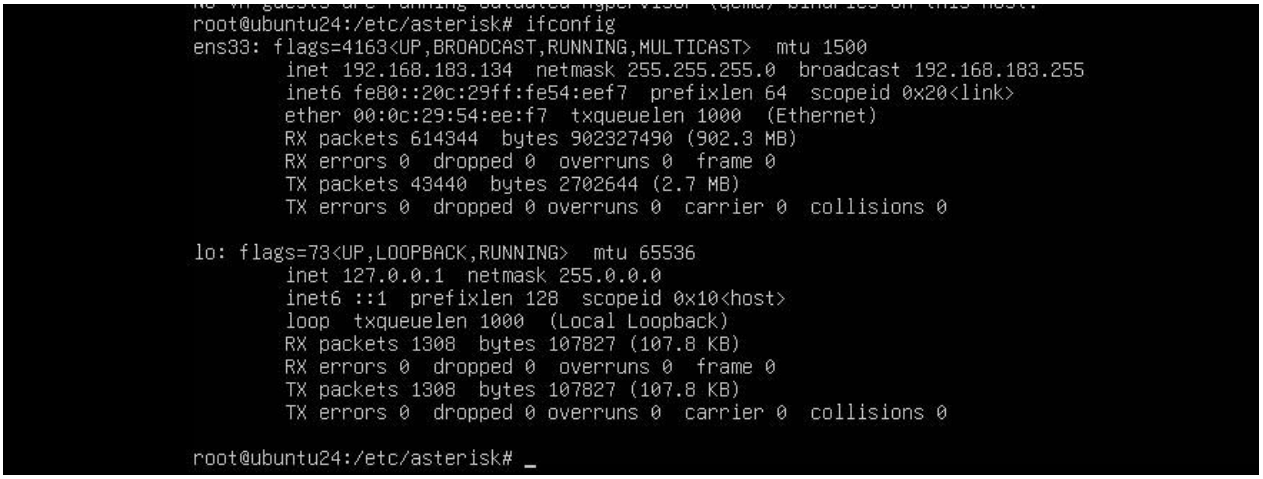


Figure III.22 Configuration ASTERISK

Nous allons maintenant éditer le fichier extensions.conf qui permet de configurer le Dialplan.

III.6.3 Configuration du Dialplan

Nous allons donc configurer Asterisk de telle sorte que l'utilisateur 1002 puisse appeler le numéro 1001.

Voici donc mon fichier **extensions.conf.**

Maintenant, vous pouvez enregistrer votre fichier **extensions.conf** et faire un reload dans la console d'Asterisk.

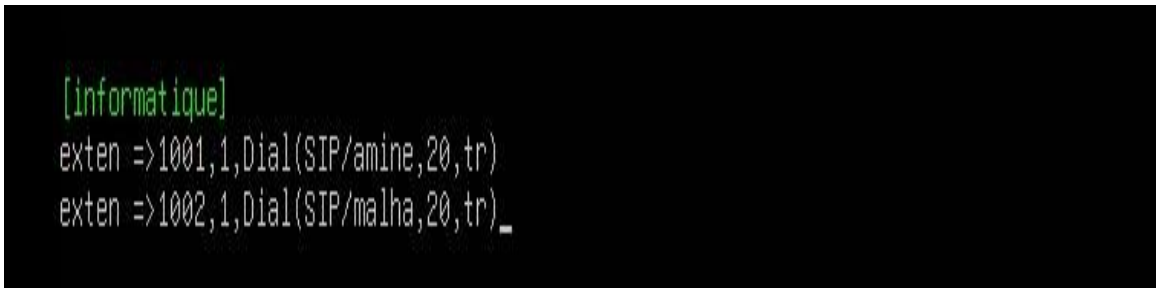


Figure III.23 C*onfigurer le Dialplan*

1 Explications sur la capture précédente

- **exten** => : déclare l'extension (on peut aussi simplement dire numéro).
- **1XXX** _ : Prend les extensions (ou numéros) de 1000 à 1999

- **1** : Ordre de l'extension
- **Dial** : application qui va être utilisé
- **SIP** : Protocol qui va être utilisé
- **${EXTEN}** : variable de l'extension composé, si on appelle le 1001 la Variable ${EXTEN} prendra comme valeur 1001
- **20** : temps d'attente avant de passer à l'étape suivante.

Maintenant, vous pouvez enregistrer votre fichier **extensions.conf** et faire un **reload** dans la console d'Asterisk

Donc la **ligne exten ⇒**

_1XXX,1, Dial(SIP/${EXTEN},20) se traduit par: Quand on compose le numéro (par exemple) 1001, on appelle le numéro 1001 et si au bout de 20 secondes il n'y a pas de réponses on passe à la ligne du dessous.

La seconde ligne : **exten ⇒ _1XXX,2, Hangup()** permet de raccrocher si il n'y a pas de réponses au bout des 20 secondes.

- ❖ Lancez la console Asterisk avec la commande suivante :

```
sudo asterisk -rrrrvvvvvvv
```

```
root@ubuntu24:/etc/asterisk# asterisk -rrrrvvvvvvv
Asterisk 20.6.0~dfsg+~cs6.13.40431414-2build5, Copyright (C) 1999 - 2022, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 20.6.0~dfsg+~cs6.13.40431414-2build5 currently running on ubuntu24 (pid = 1792)
ubuntu24*CLI>
```

Figure III.24 Lancez la console Asterisk

III.7 Configuration de Linphone

LINPHONE est un freeware, son utilisation est simple, il est disponible pourles différents systèmesd'exploitation Windows, Mac et Linux.

Pour configurer le client l'utilisateur « 1001 » et aussi « 1002 »

***Première étape et de crée le* compte SIP**

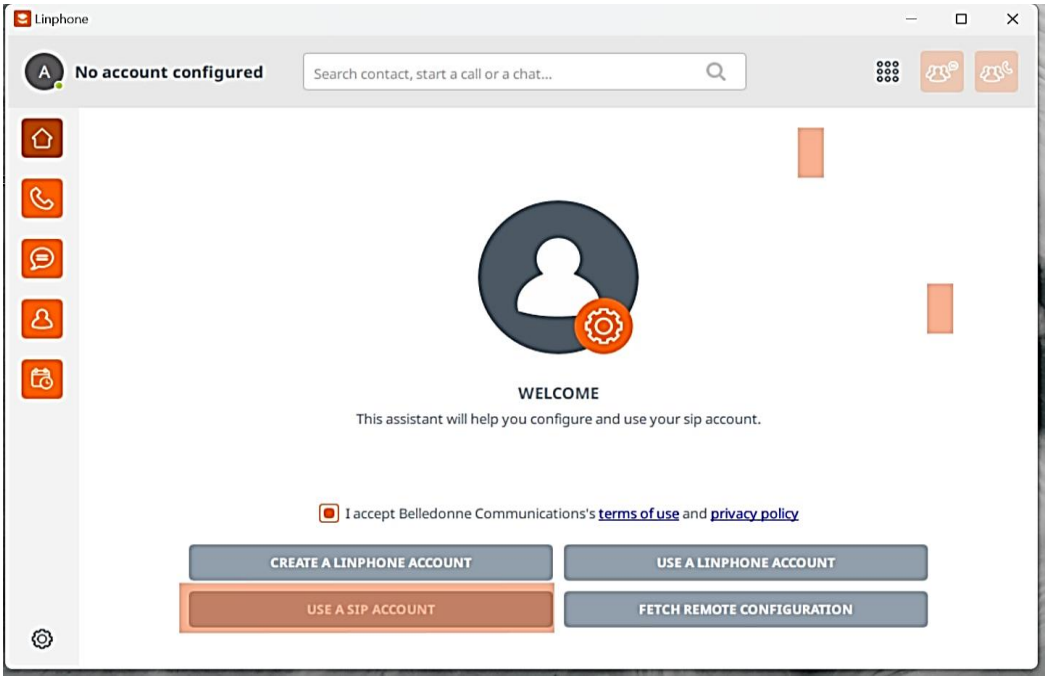


Figure III.25 ***Crée le compte SIP***

Dans la fenêtre qui s'ouvre, il suffit de remplir les champs illustrés suivant

L'utilisateur 1001 :

- Domain : 192.168.183.134

- Password : 1234

- Display name : amine

L'utilisateur 1002 :

- Domain : 192.168.183.134

- Password : 1234

- Display name : malha

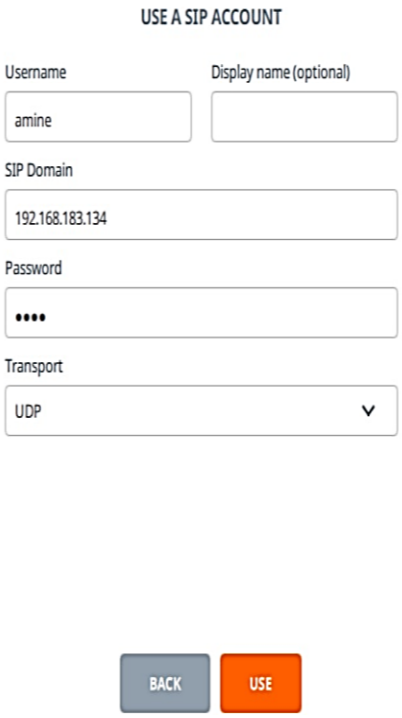


Figure III.26 *Configuration du compte du client 1001* **Figure III.27** *Configuration du compte du client 1002*

Remarque : l'authentification soit possible, ces valeurs doivent être Conformes à celles saisies dans le fichier sip.conf du serveur Asterisk. Une fois la configuration est achevée, le softphone se connectera Automatiquement au serveur et s'enregistrera. Un message « Available » s'affichera, indiquant que les communications sont désormais Possibles. Sinon, un message d'erreur explique le motif qui a fait Échouer le processus

Vérifier les compte d'utilisateur "1001" , 1002 est connecté avec le serveur SIP

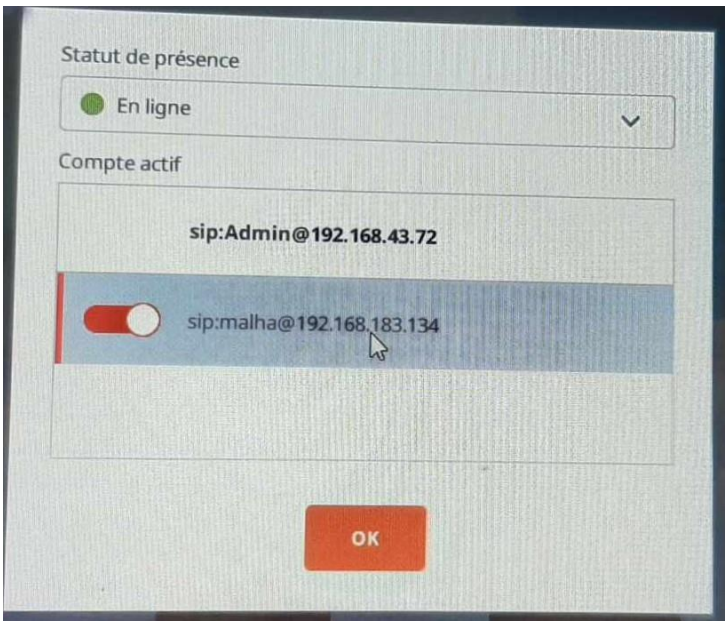


Figure III.28 Statut en ligne

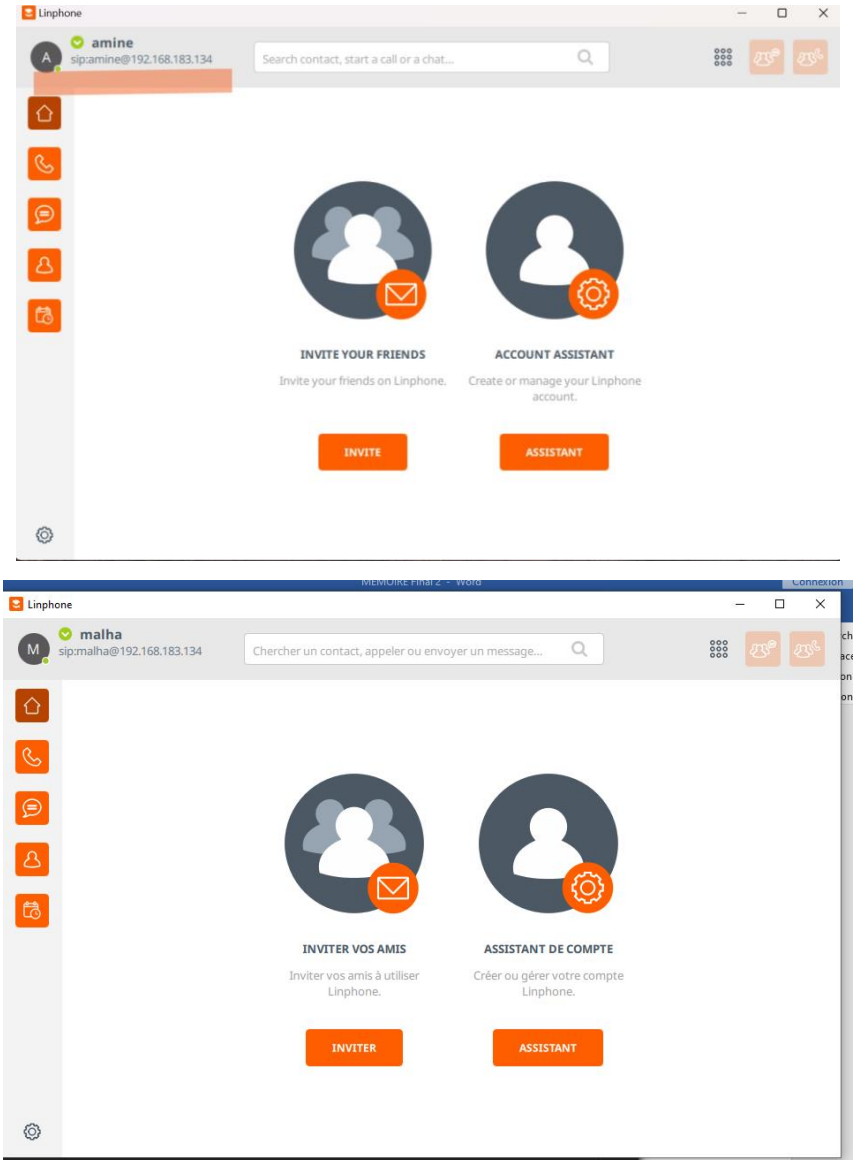


Figure III.29 Le softphone Linphone est connecté.

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

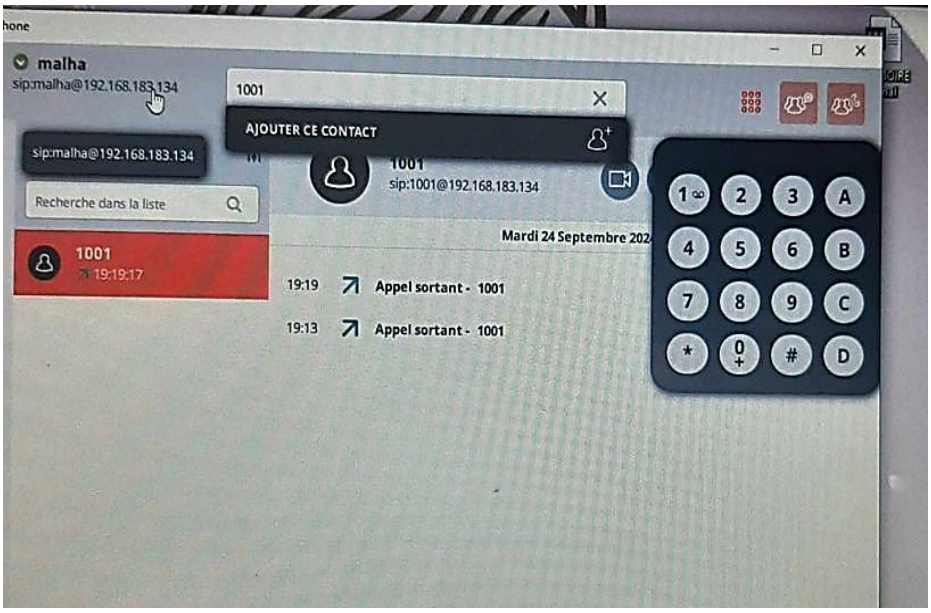


Figure III.30 taper le numéro

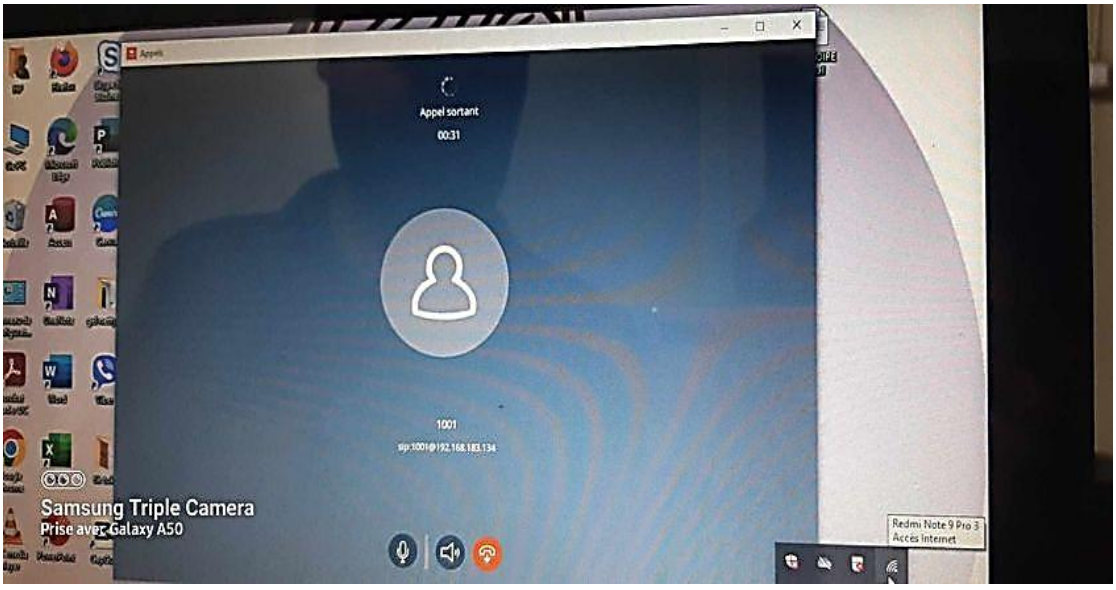


Figure III.31 Simulation d'un appel

. 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 1001 => 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

III.8 Conclusion

L'intégration d'Asterisk sur Linux Ubuntu, combinée avec le softphone Linphone, constitue une solution efficace pour établir un système de communication VoIP performant au sein des entreprises. Grâce à sa nature open source, Asterisk permet une personnalisation poussée, s'adaptant ainsi aux besoins spécifiques de chaque organisation.

Linphone, avec son interface conviviale, facilite l'accès aux fonctionnalités VoIP, rendant la communication plus fluide et intuitive. Une configuration adéquate d'Asterisk est essentielle pour assurer la qualité des appels et la sécurité des échanges, en intégrant des protocoles et des paramètres appropriés

Conclusion Générale

La VoIP (Voice over IP) représente une véritable révolution dans le domaine des télécommunications, offrant une solution moderne et abordable face aux systèmes de téléphonie classiques. Son architecture basée sur des protocoles IP permet une flexibilité exceptionnelle et favorise l'intégration avec d'autres services numériques, tels que la visioconférence et la messagerie instantanée.

Les protocoles de communication jouent un rôle crucial dans la qualité et l'efficacité des communications VoIP. SIP (Session Initiation Protocol) est le protocole de signalisation standard qui gère l'établissement, la modification et la terminaison des sessions de communication. Il permet aux utilisateurs de se connecter, de partager des informations et de gérer des appels, en s'assurant que toutes les parties sont synchronisées. RTP (Real-time Transport Protocol) quant à lui, est responsable du transport des flux audio et vidéo en temps réel, garantissant que les données arrivent en continu et dans le bon ordre. En parallèle, les codecs audio tels que G.711 et G.729 compressent et décompressent les données, influençant à la fois la qualité sonore et la bande passante utilisée. Le choix du codec est essentiel et doit tenir compte des besoins de qualité des appels et des capacités du réseau.

En raison de cette flexibilité, la VoIP améliore le cadre de travail des employés, leur permettant de rester connectés, quel que soit leur emplacement. Cependant, cette souplesse s'accompagne de vulnérabilités potentielles, nécessitant des mesures de sécurité appropriées pour protéger les données et garantir la qualité de service. L'utilisation de protocoles de chiffrement comme SRTP (Secure Real-time Transport Protocol) et l’implémentation de pare-feu sont indispensables pour protéger les communications et les informations sensibles.

L'intégration d'Asterisk sur Linux Ubuntu, en conjonction avec le softphone Linphone, constitue une solution efficace pour déployer un système de communication VoIP performant au sein des entreprises. Grâce à sa nature open source, Asterisk permet une personnalisation poussée, répondant ainsi aux besoins spécifiques de chaque organisation. Linphone, avec son interface conviviale, simplifie l'accès aux fonctionnalités VoIP, rendant les communications plus fluides et intuitives.

La simulation joue également un rôle clé dans le déploiement d'Asterisk. En utilisant des outils tels que SIPp pour générer des appels simulés et Wireshark pour analyser le trafic, les entreprises peuvent tester la performance du système dans diverses conditions, évaluer la latence et la gigue, et s'assurer de la qualité de service. Cela permet d'identifier et de résoudre les problèmes potentiels avant le déploiement, garantissant ainsi une expérience utilisateur optimale.

En somme, l'adoption de la VoIP via Asterisk représente une opportunité majeure pour les entreprises souhaitant moderniser leurs infrastructures de téléphonie. Les protocoles comme SIP et RTP, associés à une gestion adéquate des codecs, assurent des communications de haute qualité. La simulation permet de tester et d'optimiser le système, tout en garantissant la sécurité des échanges grâce à des protocoles de chiffrement robustes. En intégrant ces éléments, les entreprises peuvent non seulement améliorer la collaboration interne, mais également se positionner à la pointe de la technologie dans un environnement numérique en constante évolution.

Références bibliographies

[1] M. N. H. A. S. Mehta, et al. Voix sur IP. Journal des Communications et Réseaux, 225,21-431.2020

[2] D. W. Van Dyke. Comprendre la technologie VoIP. Wiley. 2019

[3] C. S. R. M. Chappell. Asterisk. O'Reilly Media. 2018

[4] S. K. Singh & S. R. Kumar. Sécurité dans les réseaux de voix sur IP : vulnérabilités et solutions. Journal International de la Sécurité de l'Information, 203 , 237-245.

[5] R. P. T. R. Patel & N. P. K. Singh. Sécurité VoIP : Un aperçu des menaces et des solutions. Réseaux Informatiques, 174, 107212. 2020

[6] Cisco Systems, Inc. Solutions VoIP de Cisco. https://www.cisco.com

[7] M .BOUMAZA- La mise en place de la téléphonie ip dans un réseau - Université - INSFP EX- ITEEM – 2016

[8] D. Wetteroth, OSI Reference Model for Telecommunications. McGraw Hill Professional, 2001.

[9] Mehta, M. N. H. A. S., et al.Voix sur IP : Un aperçu complet. Communications et Réseaux, 22(5), 421-431. 2020

[10] Chappell, C. S. R. M. Asterisk : Le guide définitif. O'Reilly Media.2018

[11] Singh, S. K., & Kumar, R. Sécurité dans les réseaux de voix sur IP : vulnérabilités et solutions. Journal International de la Sécurité de l'Information, 20(3), 237-245. 2021

[12] Patel, R. P. T. R., & Singh, N. P. K. Sécurité VoIP : Un aperçu des menaces et des solutions. Réseaux Informatiques, 174, 107212. 2020

[13] Laurent Ouakil and G. Pujolle, Téléphonie sur IP. Editions Eyrolles, 2011.

[14] P. Thermos and Ari Takanen, Securing VoIP Networks. Pearson Education, 2007.

[15] BIBI TRIKI ARSLANE, Gadiri Riyad – Etude de la sécurité dans la VOIP - Université - ABOUBAKAR BELKAÏD – Tlemcen – 2021

[16] M. Nour El Houda - Mémoire – Université - UNIVERSITE BADJI MOKHTAR ANNABA - 2019

[17] T. Dagiuklas and P. Galiotos, "Architecture and design of an enhanced H.323 VoIP gateway," Jun. 2003

[18] C. Rigault, Les réseaux télécoms basés IP et leurs interconnexions. Architectures et signalisations. Lulu.com, 2014.

[19] V. Kumar, M. Korpi, and Senthil Sengodan, IP Telephony with H.323. 2001.

[20] S. A. Ahson and M. Ilyas, SIP Handbook. CRC Press, 2018.

[21] G. A. Donahue, *Network Warrior*. O'Reilly Media, 2011.

[22] H. Sinnreich and A. B. Johnston, Internet Communications Using SIP. John Wiley & Sons, 2012.

[23] M. Ahmed and V. Gilles, Téléphonie SIP : concepts, usages et programmation en Java. Lavoisier, 2012.

[24] A. B. Johnston, *SIP:* Understanding the Session Initiation Protocol, Fourth Edition. Artech House, 2015.

[25] G. Camarillo, SIP Demystified. McGraw Hill Professional, 2001.

[26] B. Madani Houssam Eddine, Chennouna Mohamed -Mémoire -Université -

Université 8Mai 1945 – Guelma – 2019

[27] Olivier Hersent, D. Gurle, and Jean-Pierre Petit, L'essentiel de la VoIP. Paris: Dunod, 2007.

[28] C. Llorens, L. Levier, D. Valois, and B. Morin, *Tableaux de bord de la sécurité réseau*. Editions Eyrolles, 2011.

[29] H. Mahmood, Wireless and Mobile Hacking and Sniffing Techniques. Dr. Hidaia Mahmood Alassouli, 2021.

[30] D. Endler and M. D. Collier, Hacking exposed VoIP : voice over IP security secrets & solutions. New York: Mcgraw-Hill, 2007.

[31] A. SEFAR EL hancha, Yacine BRAHMI-Etude d'implémentation d'une solution VIOP sécurisée dans un réseau informatique d'entreprise -Université ANSTITUT SUPERIEUR

INFORMATIQUE - 2016

[32] N.DJOMO – Intégration d'un serveur voip dans un réseau d'entreprise– Université -

Notre Dame de Tshumbe - 2020

[33] T. Porter, Practical VoIP Security. Elsevier, 2006.

[34] Sébastien Déon, VoIP et ToIP Asterisk. Editions ENI, 2007

[35] O .Ben Rahal, Mohamed Sahmoudi, Mustapha Ouezghar-.Journal-Mise en oeuvre D'une solutionVOIP sous ASTERISK-2015.

[36] site net -VMWare Workstation Pro FAQ https://www.vmware.com/info/workstation-pro/