République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaïa

Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de Master en Informatique
Option : Administration et Sécurité des Réseaux

Thème

Mise en œuvre d'une solution de téléphonie sur IP (ToIP) basée sur Asterisk

Cas d'étude : Entreprise Portuaire de Béjaïa

Réalisé par :
KHETTAL Thiziri
KHEYAR Warda

Encadré par :
Mme . ZIDANI Ferroudja

Jury du mémoire :

Président	M. YAZID Mohand
Examinateur	Mme . BACHIRI Lina
Examinateur	M. FARAH Zoubeyr
Examinateur	Mme . SABRI Salima

Promotion 2024–2025

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.

On tient à remercier, tout particulièrement notre encadrant Mme. FERROUDJA ZIDANI 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 .Nous remercions particulièrement :M.YAZID MOHAND, président du jury,Mme.BACHIRI LINA, membre du jury,M. FARAH ZOUBEYR, membre du jury,Mme. SABRI SALIMA, membre du jury.

Dédicace

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

À la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non à mes demandes et exigences, et qui n'a épargné aucun effort pour me voir heureuse et en sécurité : mon adorable mère.

À l'homme à qui je dois la vie, celui qui a combattu toute sa vie pour me procurer tout ce dont j'avais besoin, qui m'a soutenue tout au long de mon parcours et qui a toujours été un exemple : mon cher père. Puisse Allah lui accorder Sa miséricorde et l'accueillir dans Son vaste paradis. Repose en paix, papa, à jamais dans mon cœur.

À mes sœurs : Souade, Karima et Wassila.

À mes frères : Ahcen et Redouane.

À mes amis : Idri Mofida, Moussaoui Nadjet.

À toutes les personnes qui, de près ou de loin, m'ont aidée à la réalisation de ce travail.
À tous mes enseignants de l'université Abderrahmane Mira de Béjaïa.

KHEYAR WARDA

Dédicace

Avec toute ma reconnaissance, je dédie ce travail aux personnes que j'aime profondément et à qui je ne pourrai jamais dire assez merci.

À mes chers parents,

Vous êtes la source de mon courage et de ma persévérance.
Par vos sacrifices silencieux, vos prières constantes,
et votre amour inconditionnel,
vous m'avez accompagné à chaque étape de ma vie.

Ce travail n'est qu'un modeste reflet de tout ce que je vous dois.Je souhaiterais vous dire papa, maman, que ma réussite aujourd'hui et pour vous et, surtout grâce à vous.

À mes frères : karim et yacine

À mes amis :bentouati roumaissa et chahinez

À toutes les personnes qui, de près ou de loin, m'ont aidée à la réalisation de ce travail.
À tous mes enseignants de l'université Abderrahmane Mira de Béjaïa.

KHETTAL THIZIRI

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

ACRONYMES

ACK	Accusé de réception (Acknowledgment).
CDR	Relevé de détails d'appel (Call Detail Record).
CLI	Interface en ligne de commande (Command Line Interface).
CODEC	Codeur-Décodeur (Coder-Decoder).
CRM	Gestion de la relation client (Customer Relationship Management).
DGAF	Direction Générale de l'Administration et des Finances.
DGAO	Direction Générale de l'Administration et de l'Organisation.
DHCP	Protocole de configuration dynamique des hôtes (Dynamic Host Configuration Protocol).
DMZ	Demilitarized Zone.
DNS	Système de noms de domaine (Domain Name System).
DSI	Direction des Systèmes d'Information.
EPB	Entreprise Portuaire de Béjaïa.
IP	Protocole Internet (Internet Protocol).
IPBX	Autocommutateur téléphonique IP.
IVR	Réponse vocale interactive (Interactive Voice Response).

LAN	Réseau local (Local Area Network).
MCU	Unité de contrôle multipoint (Multipoint Control Unit).
MySQL	Système de gestion de base de données relationnelle libre (My Structured Query Language).
NAT	Traduction d'adresses réseau (Network Address Translation).
PABX	Autocommutateur privé automatique (Private Automatic Branch Exchange).
PDG	Président Directeur Général.
RFC	Demande de commentaires (Request for Comments).
RTC	Réseau téléphonique commuté.
RTCP	Protocole de contrôle du transport en temps réel (Real-time Transport Control Protocol).
RTP	Protocole de transport en temps réel (Real-time Transport Protocol).
SDP	Protocole de description de session (Session Description Protocol).
SIP	Session Initiation Protocol.
TCP	Protocole de contrôle de transmission (Transmission Control Protocol).
ToIP	Téléphonie sur IP (Telephony over Internet Protocol).
UDP	Protocole de datagramme utilisateur (User Datagram Protocol).
URI	Identifiant uniforme de ressource (Uniform Resource Identifier).
UTF-8	Format de transformation Unicode en 8 bits (Unicode Transformation Format – 8 bits).

VPN Réseau privé virtuel (Virtual Private Network).

WAN Réseau étendu (Wide Area Network).

INTRODUCTION GÉNÉRALE

Introduction Générale

La convergence des réseaux de communication basés sur le protocole Protocole Internet (Internet Protocol) (IP) occupe aujourd'hui une place centrale dans le développement des systèmes de télécommunication. Cette transformation représente à la fois un défi majeur et une opportunité intéressante pour moderniser et optimiser les infrastructures de communication.
Dans un contexte où les technologies de l'information et de la communication évoluent constamment, les entreprises recherchent des solutions de téléphonie capables de s'intégrer facilement à leurs réseaux informatiques tout en offrant des fonctionnalités avancées. C'est dans cette optique que se sont développées les technologies de Téléphonie sur IP Téléphonie sur IP (Telephony over Internet Protocol) (ToIP), qui permettent de transmettre la voix (VoIP) sous forme de paquets de données à travers les réseaux IP, tels qu'Internet ou les réseaux locaux.
Le choix de la Téléphonie sur IP (ToIP) s'explique par ses nombreux avantages par rapport au système RTC utilisé actuellement. Le RTC repose sur des lignes physiques, ce qui limite le nombre d'appels simultanés : un seul appelant peut utiliser une ligne à la fois. En revanche, la ToIP permet à plusieurs utilisateurs de passer des appels en même temps via le réseau informatique existant, sans besoin de lignes dédiées. Elle offre aussi la possibilité d'effectuer des appels internes sans connexion Internet, grâce à la configuration locale du serveur Asterisk. Pour les appels externes, l'intégration d'un VPN sécurisé permet de garantir la confidentialité des communications, même à distance. Cette solution réduit les coûts, améliore la flexibilité et s'adapte facilement aux besoins évolutifs de l'entreprise. Un système de téléphonie IP repose principalement sur l'utilisation d'un Autocommutateur téléphonique IP (IPBX) (Internet Protocol Private Branch Exchange), un central téléphonique numérique qui assure la gestion des appels internes et externes. Il fonctionne en lien avec des logiciels appelés softphones, qui permettent aux utilisateurs de passer et de recevoir des appels depuis un ordinateur, un téléphone

IP ou un smartphone. L'IPBX propose des fonctionnalités avancées telles que la messagerie vocale, la redirection d'appel, les conférences, la musique d'attente personnalisée [8]. Toutefois, pour assurer la connectivité avec l'extérieur, il est indispensable de disposer d'une connexion Internet fournie par un opérateur.

Dans le cadre de notre formation, nous avons effectué un stage pratique au sein de Entreprise Portuaire de Béjaïa (EPB), avec pour objectif de mettre en œuvre une infrastructure complète de téléphonie sur IP (ToIP). Cela implique la configuration d'un IPBX basé sur Asterisk, l'intégration de fonctionnalités essentielles (messagerie vocale, serveur vocal interactif, etc.), ainsi que la mise en place d'un tunnel VPN sécurisé à l'aide de la solution Tailscale. Nous avons ainsi participé activement à toutes les étapes du projet : conception, installation, configuration et tests.

Ce memoire est structuré en trois chapitres principaux :

Le premier chapitre présente les fondements de la téléphonie sur IP (ToIP). Il explique ses principes de fonctionnement, la transmission de la voix, les protocoles utilisés (SIP, RTP...), ainsi que ses avantages et simite.

Le deuxième chapitre est consacré à la présentation de l'EPB et à l'analyse de l'infrastructure réseau existante. Il identifie les principales problématiques liées au systéme de téléphonie en place, notamment les limitations des équipements analogiques en termes de flexibilité, de gestion et de coûts. En réponse à ses constats, une solution basée sur l'intégration d'un serveur IPBX est proposée afin de centraliser les communications, d'optimiser les flux téléphoniques et de sécuriser les échanges externe via un Réseau privé virtuel (Virtual Private Network) (VPN).

Le troisième chapitre détaille la mise en œuvre technique du projet. Il décrit l'installation et la configuration du serveur Asterisk, la création d'un environnement de téléphonie interne(gestion des comptes SIP, IVR, etc.), ainsi que l'intégration d'un tunnel VPN basé sur Tailscale pour permettre les communications externes de manière sécurisée. Notre mémoire se termine par une conclusion générale résumant les grands points qui ont été abordés ainsi que des perspectives que nous souhaitons accomplir prochainement.

CHAPITRE 1

FONDEMENTS DE LA TÉLÉPHONIE SUR IP (TOIP) ET DE LA VOIX SUR IP (VOIP)

1.1 Introduction

La téléphonie sur IP (ToIP) désigne l'ensemble des technologies, protocoles, logiciels et équipements permettant de gérer un système complet de téléphonie en utilisant un réseau IP. Elle inclut la signalisation, la gestion des appels, les fonctionnalités avancées (messagerie vocale, conférences, etc.) La VoIP (Voice over IP), qui constitue un sous-ensemble de la ToIP, se concentre spécifiquement sur la transmission numérique de la voix. Dans ce chapitre, nous aborderons quelques notions fondamentales sur la ToIP. Nous commencerons par une présentation du Réseau téléphonique commuté (RTC) , ensuite nous expliquerons les principes de la VoIP, son fonctionnement, ainsi que les protocoles de signalisation et de transport associés, notamment SIP, SDP et RTP. Enfin nous aborderons les principaux avantages de cette technologie.

1.2 Le Réseau Téléphonique Commuté (RTC)

Le RTC (ou Réseau Téléphonique Commuté) est la technologie analogique historique qui permettait d'assurer les communications vocales entre deux utilisateurs distants. Il établit une liaison physique dédiée entre deux abonnés pendant toute la durée de la communication. Conçu initialement pour la transmission de la voix, il a été utilisé à partir de 1964 pour le transport de données en France [7].

1.2.1 Principe de fonctionnement

La commutation de circuits repose sur l'établissement d'un canal de communication dédié entre deux abonnés. Toute la bande passante reste réservée à ces derniers pendant toute la durée de l'échange, même en l'absence de parole. Ce type de communication nécessite une connexion continue, assurée par des commutateurs. Le signal vocal y est transmis sous forme analogique à travers des lignes électriques. Le processus débute lorsque l'émetteur produit un son, converti en signal électrique par un microphone. Ce signal est ensuite amplifié et transmis via une paire torsadée jusqu'au récepteur, où un haut-parleur le reconvertit en son audible[15].
Ce principe est illustré par le schéma suivant :

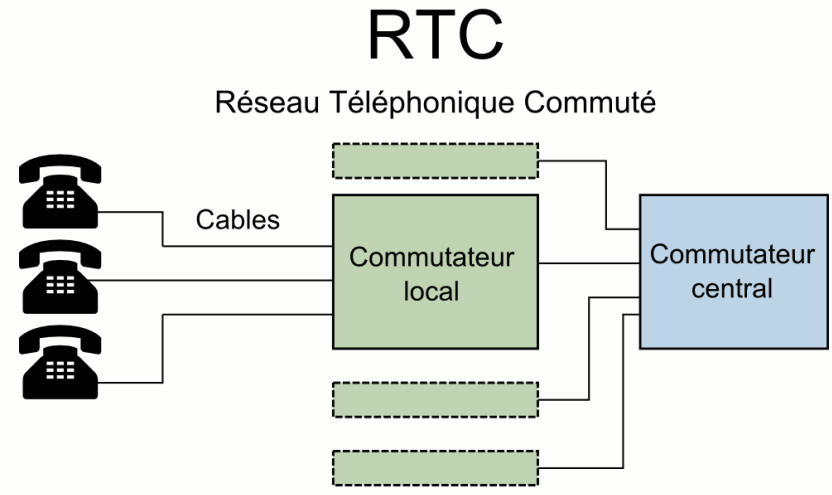

FIGURE 1.1 – Schéma illustrant le principe de fonctionnement du RTC[1]

1.2.2 Le standard téléphonique traditionnel Autocommutateur privé automatique (Private Automatic Branch Exchange) (PABX)

Le PABX (Private Automatic Branch Exchange), ou autocommutateur privé, est un système téléphonique utilisé par les entreprises pour gérer les communications internes et externes. Il permet de connecter les postes internes à des lignes du réseau téléphonique commuté (RTC). Le fonctionnement du PABX repose sur une infrastructure matérielle dédiée, souvent installée sur site, qui permet de :
- gérer les appels entre postes internes.
- acheminer les appels vers l'extérieur via des lignes analogiques
Bien que fiable, cette technologie présente plusieurs limitations elle nécessite un câblage spécifique, est peu flexible pour les extensions, et n'intègre pas nativement les outils informatiques modernes (messagerie, visioconférence, mobilité, etc.). C'est pourquoi de nombreuses entreprises migrent vers des solutions IPBX basées sur la téléphonie sur IP (ToIP), qui offrent plus

de souplesse, d'évolutivité et de fonctionnalités [7].

1.3 La Téléphonie IP

La téléphonie sur IP(ToIP), est une méthode de communication qui utiliser un réseau de données (comme Internet) pour transmettre non seulement la voix, mais aussi d'autres types d'échanges (texte, image, vidéo, etc.). Elle repose sur la conversion de la voix en données numeriques par un telephone IP, l'encapsulation de ces données en paquets, puis leur transmission à travers un réseau IP. La téléphonie par Internet fonctionne sur des réseaux privés ou publics. La ToIP ne se limite pas à être un simple moyen de transmettre la voix, elle implique également la définition d'un ensemble de protocoles appropriés et spécifiquement consacrés à la gestion des flux multimédias afin de garantir la qualité de service et répondre aux exigences des communications en temps réel[14] [11].

1.4 La VoIP

1.4.1 Définition

VoIP (Voice Over Internet Protocol) désigne la transmission de la voix sur un réseau IP, notamment via Internet. Elle constitue un sous-ensemble de la ToIP, qui englobe l'ensemble du système de téléphonie IP. La VoIP permet d'établir des communications vocales ou multimédia (audio, vidéo) entre deux ou plusieurs utilisateurs à travers un réseau IP. Parmi les applications de la VoIP on cite : Skype, Zoom, WhatsApp, Cisco Webex[23].
La VoIP comprend des communications de type :

— PC à PC, où chaque utilisateur utilise un logiciel appelé softphone pour passer des appels
— PC à téléphone IP, où Un ordinateur peut appeler un téléphone IP
— Téléphone IP à téléphone IP, où la communication s'effectue entre deux téléphones IP connectés au réseau VoIP [19].

Ainsi, elle repose sur l'échange de deux types d'informations entre les terminaux communicants :

- La voix (les données utiles) : Elle correspond au contenu reél de la communication.
- Les métadonnées de signalisation : Elles permettent d'établir, de gérer et de terminer l'appel (exemple : protocole SIP).

1.4.2 Fonctionnement de la VoIP

La VoIP fonctionne en convertissant la voix (signal analogique) en données numériques, qui sont ensuite encapsulées dans des paquets IP pour être transmises sur un réseau. Ce processus, comme le montre la figure suivante, implique plusieurs étapes clés[21].

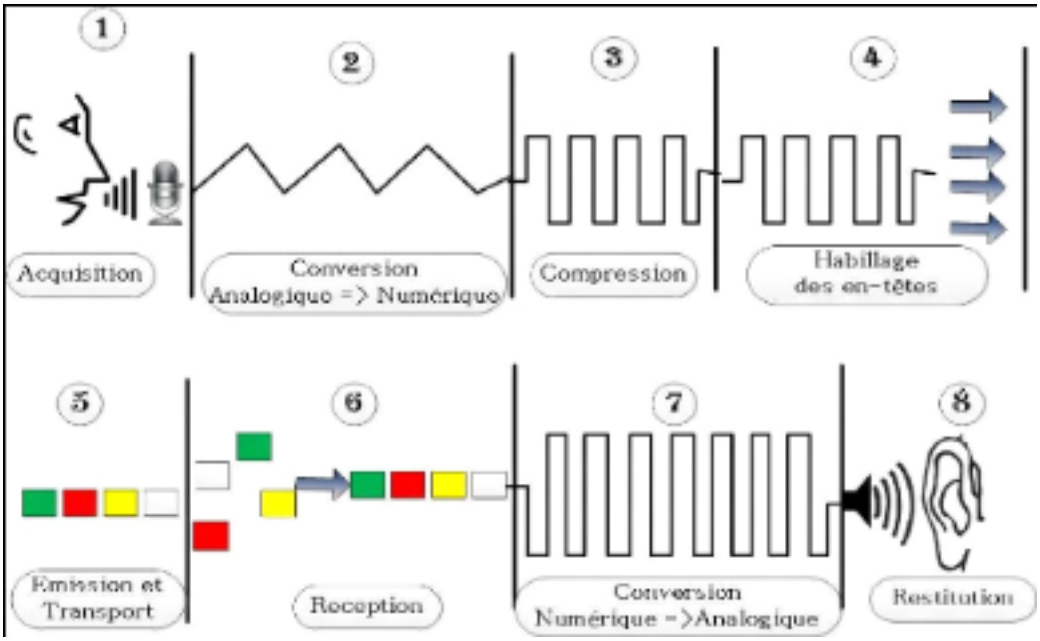

FIGURE 1.2 – Le principe de fonctionnement de la VoIP [10]

1.4.2.1 Acquisition du signal

Est la première étape du processus de transmission de la voix en VoIP. Elle consiste à capturer la voix humaine (ondes sonores) ou tout autre son à l'aide d'un microphone et à la convertir en un signal électrique analogique.

1.4.2.2 Numérisation et compression

La numérisation est une étape clé dans le processus de transmission de la voix en VoIP. Elle consiste à convertir le signal électrique analogique (issu du microphone) en un format numérique. Cette conversion est réalisée à l'aide d'un Codeur-Décodeur (Coder-Decoder) (CODEC). **Un codec (encodeur-décodeur) :** est un algorithme ou un dispositif matériel qui réalise la numérisation du signal analogique. Il effectue les étapes d'échantillonnage, de quantification et de codage. Les codecs sont également responsables de la compression des données numériques pour réduire la bande passante nécessaire à la transmission. Ainsi ,lors de la réception le décodage qui est une fonction du codec, permet décompresse les données et les reconvertit en signal analogique pour restituer la voix et parmi les codecs audio les plus courant on cite :

- G.711 : un codec non compressé qui offre une excellente qualité audio mais consomme beaucoup de bande passante (64 kbps par canal).
- G.729 : un codec compressé audio utilisé principalement dans la VoIP. Il permet d'encoder la voix à un débit de 8 kbps, offrant une bonne qualité tout en réduisant la bande passante nécessaire aux communications. Il est particulièrement adapté aux environnements où les ressources réseau sont limitées.
- Opus : un codec audio performant et adaptable. Opus est un codec audio conçu pour offrir une qualité sonore exceptionnelle tout en s'adaptant dynamiquement aux conditions du réseau. Cela signifie qu'il ajuste en temps réel plusieurs paramètres, tels que le débit binaire (de 6 kbps à 510 kbps), la latence et la qualité sonore, en fonction de la bande passante disponible et des variations du réseau. Contrairement à des codecs comme G.729, qui sont optimisés uniquement pour la voix avec un faible débit (8 kbps), Opus prend en charge un large spectre audio, allant de la voix aux fichiers musicaux, tout en offrant une meilleure robustesse face aux pertes de paquets. Grâce à cette flexibilité et à ses performances accrues, Opus est utilisé dans des domaines variés comme la VoIP, WebRTC, le streaming et les jeux en ligne.

Ainsi, plusieurs codecs vidéo sont utilisés pour assurer la compression

- H.264 (AVC) : Très répandu pour la diffusion vidéo et la visioconférence.
- H.265 (HEVC) : Meilleure compression que le H.264, utilisé pour la 4K/8K.
- VP8 : est un codec vidéo développé par On2 Technologies, puis acquis par Google en 2010. Il s'agit d'un codec de compression vidéo open source et libre de droits, conçu pour offrir une compression efficace tout en maintenant une bonne qualité d'image[21].

1.4.2.3 L'encapsulation

L'encapsulation est un processus qui consiste à structurer les données numériques en paquets IP avant leur transmission sur le réseau. Dans le cadre de la VoIP, ces paquets incluent plusieurs couches des protocoles, notamment IP, UDP, RTP et RTCP, qui assurent une transmission fluide et synchronisée de la voix et de la vidéo en temps réel.

La couche IP : IP (Internet Protocol) est chargé de l'acheminement des paquets à travers le réseau en fonction des adresses IP source et destination. Il permet le découpage et la reconstitution des paquets afin qu'ils atteignent leur destination, même si l'itinéraire varie en fonction de la congestion du réseau.

La couche UDP : Protocole de datagramme utilisateur (User Datagram Protocol) (UDP) est un protocole de transport léger, rapide et adapté aux communications en temps réel comme la VoIP. Contrairement à Protocole de contrôle de transmission (Transmission Control Protocol) (TCP), il ne garantit ni l'ordre d'arrivée des paquets ni leur intégrité, mais cette absence de correction d'erreurs permet de réduire la latence et d'éviter des retards liés aux retransmissions.

la couche RTP : Le protocole Protocole de transport en temps réel (Real-time Transport Protocol) (RTP) est utilisé pour le transport de bout en bout de flux multimédias soumis à des contraintes temporelles strictes, comme dans le cas de la téléphonie sur IP. Conçu pour compléter UDP, il offre un contrôle adapté aux données temps réel. RTP permet de rétablir les propriétés temps réel des flux média en agissant à deux niveaux : d'une part, la synchronisation des flux, et d'autre part, la reconstitution de l'ordre des paquets émis ainsi que la détection des pertes de paquets[12].

Dans l'en-tête d'un paquet RTP, on trouve les champs suivants :

- **Numéro de séquence :** Chaque paquet RTP contient un numéro de séquence. Ce dernier est utilisé pour détecter les pertes de paquets et pour rétablir l'ordre de réception au niveau de destinataire.
- **Horodatage (timestamp) :** Un horodatage est ajouté à chaque paquet afin d' indiquer le moment précis où le premier octet de données RTP a été généré. Cet horodatage permet de synchroniser la lecture des paquets multimédias. Il fournit une référence temporelle essentielle pour les données envoyées, ce qui est crucial pour la reconstruction correcte des flux audio et vidéo. Grâce à l'horodatage, le récepteur peut déterminer à quel moment chaque échantillon doit être joué pour maintenir le rythme approprié de la séquence audio ou vidéo.
- **Identification du codec et du format des données :** Le champ Type de payload dans l'en-tête RTP spécifie le type de charge utile qui est transporté dans le paquet RTP. Il indique quel codec est utilisé pour encoder l'audio ou la vidéo (par exemple, G.711, G.729 pour l'audio, ou H.264 pour la vidéo).
- **Identification de la source :** Chaque flux RTP possède un identifiant unique appelé SSRC (Synchronization Source Identifier), qui permet d'éviter les conflits lorsque plusieurs flux sont transmis simultanément.
- **Extensibilité :** RTP est conçu pour être adaptable, permettant d'intégrer diverses extensions comme la correction d'erreurs ou la priorisation des flux[7].

La couche RTCP (RTP Control Protocol) : Protocole de contrôle du transport en temps réel (Real-time Transport Control Protocol) (RTCP) est un protocole complémentaire à RTP, chargé de la supervision et de l'amélioration de la transmission des flux multimédias. Contrairement à RTP, RTCP ne transporte pas de médias mais échange des informations de contrôle entre les participants d'une session VoIP[12].
Ainsi, RTP et RTCP travaillent ensemble pour assurer une transmission efficace et optimisée des flux multimédias en VoIP. Tandis que RTP transporte les données en temps réel, RTCP surveille la qualité de la transmission et synchronise les flux.

1.4.2.4 Emission et transport :

Une fois que la voix est transformée en paquets IP, ceux-ci, identifiés et numérotés peuvent transiter sur n'importe quel réseau IP.

1.4.2.5 Réception :

Les paquets vocaux vont être décompressés et reconstitués une fois qu'ils atteignent leurs nœuds de destination.

1.4.2.6 Conversion numérique analogique :

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

1.4.2.7 Restitution :

Enfin, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur. Afin d'assurer la gestion des sessions de communication vocales sur IP (VoIP), plusieurs protocoles de signalisation sont utilisés. Le plus couramment employé est le protocole Session Initiation Protocol (SIP) que nous allons présenter dans la section suivante.

1.4.3 Le protocole SIP (Session Initiation Protocol)

SIP (Session Initiation Protocol) est un protocole de signalisation défini par la Demande de commentaires (Request for Comments) (RFC) 3261. Il permet d'établir, de modifier et de terminer des sessions multimédias sur un réseau IP[13] [9].

1.4.3.1 Fonctions principales du protocole SIP

SIP assure différentes fonctions nécessaires au bon déroulement des communications sur ip voici les principales :

— **Établissement d'une session :** SIP utilise des messages textuels pour initier une communication. Par exemple, un message INVITE est envoyé pour démarrer un appel.

— **Gestion des sessions :** SIP permet de modifier les paramètres d'une session en cours (par exemple, ajouter un autre participant ou commencer par une session audio et ajouter de la vidéo en cours de communication).

— **Terminaison d'une session :** Un message BYE est utilisé pour mettre fin à une session active.

— **Localisation de l'utilisateur :** SIP permet de localiser un utilisateur sur un réseau IP en associant son identifiant SIP (par exemple : sip :alice@exemple.com) à son adresse IP réélle. Cette fonction est assurée via le serveur d'enregistrement (Registar), qui conserve les informations de présence des utilisateurs. Elle est indispensable dans les environnements où les utilisateurs peuvent se connecter depuis des adresses IP dynamiques ou mobiles.

Lorsqu'un utilisateur passe un appel via son softphone, une requête SIP est transmise au serveur VoIP. Celui-ci localise le destinataire, puis établie la connexion entre les deux parties. SIP ne transporte pas les données audio ou vidéo(ce role revient à RTP), mais gère la signalisation de la session.

1.4.3.2 Caractéristiques principales du protocole SIP

Le protocole SIP présente plusieurs caractéristiques essentielles, que nous allons exposer ci-dessous.

— **Création et enregistrement de comptes SIP :** Chaque utilisateur dispose d'un identifiant SIP unique. Pour être a joignable, ce compte doit être enregistré sur un serveur SIP (proxy ou registar) ayant une adresse IP statique. Ce serveur permet de localiser l'utilisateur, même si son adresse IP change.

— **Modification des caractéristiques pendant une session :** SIP permet d'adapter la session active (ajout de participants, passage d'un appel audio à un appel vidéo, etc.) selon la capacité des terminaux.

— **Modes de communication supportés :** Avec Sip, les utilisateurs qui ouvrent une session peuvent communiquer selon trois modes [3] :

  - Unicast (Point-à-point) : communication entre deux terminaux.
  - Multicast : communication en groupe via une unité de contrôle Unité de contrôle multipoint (Multipoint Control Unit) (MCU) .
  - Mode combiné : fusionne les deux modes précédents (pour les conférences).

— **Gestion des participants :** Au cours d'une session d'appel, des participants ultérieures peuvent se joindre à ceux déjà présents en s'invitant directement, en étant transférés ou en étant placés dans une file d'attente (cette capacité s'apparente à celles offertes par un PABX, où l'appelant peut être redirigé vers un numéro spécifique ou placé en attente).

— **Négociation des médias :** SIP s'appuie sur le protocole Protocole de description de session (Session Description Protocol) (SDP) pour déterminer les types de média (audio, vidé) et les codecs prise en charge par les terminaux.[3]

— **Adressage SIP Identifiant uniforme de ressource (Uniform Resource Identifier) (URI) :** Chaque utilisateur est identifié par une adresse SIP au format suivant [3] :

```
sip : identifiant[:mot-de-passe]@serveur[?paramètres]
```

- sip : indique le protocole utilisé pour la communication.
- identifiant : représente le nom ou le numéro unique de l'utilisateur.
- motdepasse : optionnel, il sert à l'authentification de l'utilisateur auprès du serveur.
- serveur : désigne le serveur responsable du compte SIP de l'utilisateur. Il peut être identifié par une adresse IP ou par un nom de domaine (résolu via le DNS-Système de Nom de Domaine).
- paramètres : également optionnels, ils permettent d'ajuster le comportement standard (par exemple, spécifier un protocole de transport ou ajouter des informations comme l'objet de appel).

En SIP, il existe deux types d'adresses utilisées pour identifier un utilisateur et gérer les communications :

Adresse SIP publique : C'est l'adresse sous laquelle un utilisateur est joignable sur Internet. Elle est souvent basée sur un nom de domaine ou une adresse IP publique.
Exemple :

- sip :alice@exemple.com → L'utilisateur Alice est joignable via le domaine "exemple.com".
- sip : 1001@203.0.113.10 → L'utilisateur "1001" est joignable à l'adresse IP publique 203.0.113.10.

Adresse de contact : C'est l'adresse réelle d'un utilisateur enregistrée sur le serveur SIP, permettant d'établir une connexion directe. Elle peut être différente de l'adresse SIP publique, notamment lorsque l'utilisateur se trouve derrière un Traduction d'adresses réseau (Network Address Translation) (NAT).
Exemple :

- Adresse SIP publique : sip :alice@exemple.com
- Adresse de contact réelle : sip :alice@192.168.1.100 :5060 ;transport=udp

— **Messages échangés :** Dans le cadre des communications SIP, plusieurs types de messages sont échangés entre les équipements afin d'assurer l'établissement, la gestion et la terminaison des sessions. Ces messages jouent un rôle essentiel dans la structuration des interactions entre les utilisateurs et les serveurs SIP [3].
Le protocole SIP repose sur un ensemble de requêtes et de codes de réponse qui sont présenter ci-dessous.
Principales requêtes SIP :

- INVITE : Utilisée pour inviter un utilisateur ou une application à participer à une session. Elle initie l'établissement de l'appel.

- ACK : Confirme la réception d'une réponse définitive à une requête INVITE par le terminal appelant.
- OPTIONS : Permet de déterminer les capacités du terminal SIP appelé en interrogeant un proxy server.
- BYE : Utilisée pour signaler la fin d'une session par le terminal appelé.
- CANCEL : Permet d'annuler une requête en attente qui n'a pas encore reçu de réponse finale.
- REGISTER : Permet à un client de s'enregistrer auprès d'un serveur SIP en associant son adresse SIP à un emplacement réseau.

Codes de réponse SIP :
Lorsqu'un serveur SIP reçoit une requête, il répond avec un code d'état à trois chiffres accompagné d'une explication textuelle Format de transformation Unicode en 8 bits (Unicode Transformation Format – 8 bits) (UTF-8) précisant le résultat du traitement. Ces codes sont classés en six catégories [9][3] :

- 1xx - Informations : La requête a été reçue et est en cours de traitement.
- 2xx - Succès : L'action demandée a été reçue, comprise et exécutée avec succès.
- 3xx - Redirection : Une action supplémentaire est requise pour compléter la requête.
- 4xx - Erreur client : La requête contient une erreur de syntaxe ou ne peut être traitée par le serveur.
- 5xx - Erreur serveur : Le serveur a rencontré un problème l'empêchant de traiter une requête valide.
- 6xx - Échec global : La requête ne peut être traitée par aucun serveur.

1.4.3.3 L'architecture du protocole SIP

L'architecture SIP est conçue pour permettre la gestion des sessions de communication en temps réel, comme les appels vocaux, les vidéoconférences ou les messages instantanés. Elle repose sur plusieurs composants clés qui travaillent ensemble pour établir, modifier et terminer des sessions [9][13].

- **L'agent utilisateur (User Agent) :** est l'entité qui représente l'utilisateur (ex. softphone) qui initie ou reçoit les appels.
- **Le serveur d'enregistrement (Registrar server) :** Le Registrar est un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données (figure 1.3).

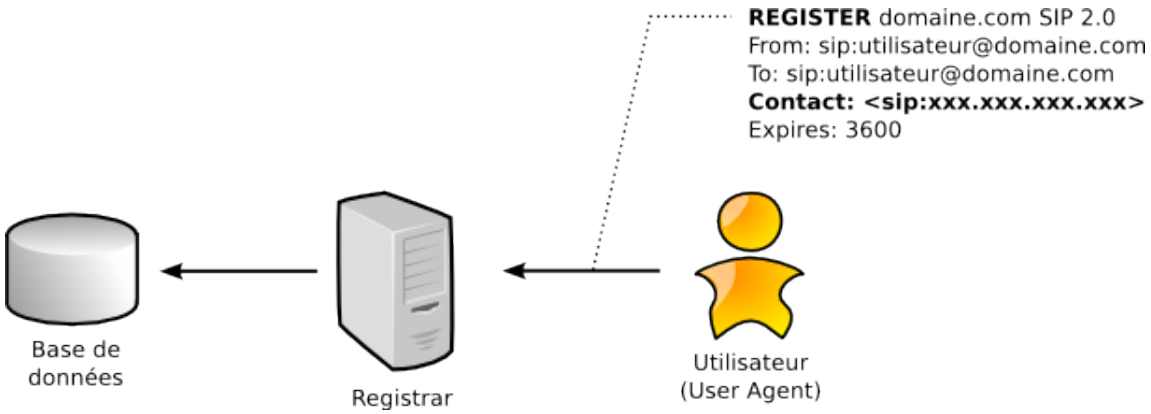

FIGURE 1.3 – Enregistrement d'un utilisateur [18]

- **Le serveur Proxy SIP :** est un serveur intermédiaire entre deux User Agents qui ne connaissent pas leurs emplacements respectifs (adresse IP). En effet, l'association URI-Adresse IP a été stockée préalablement dans une base de données par un Registrar. Le Proxy peut donc interroger cette base de données pour diriger les messages vers le destinataire. La figure ci-dessus montre les étapes de l'interrogation de la base de données via un proxy.

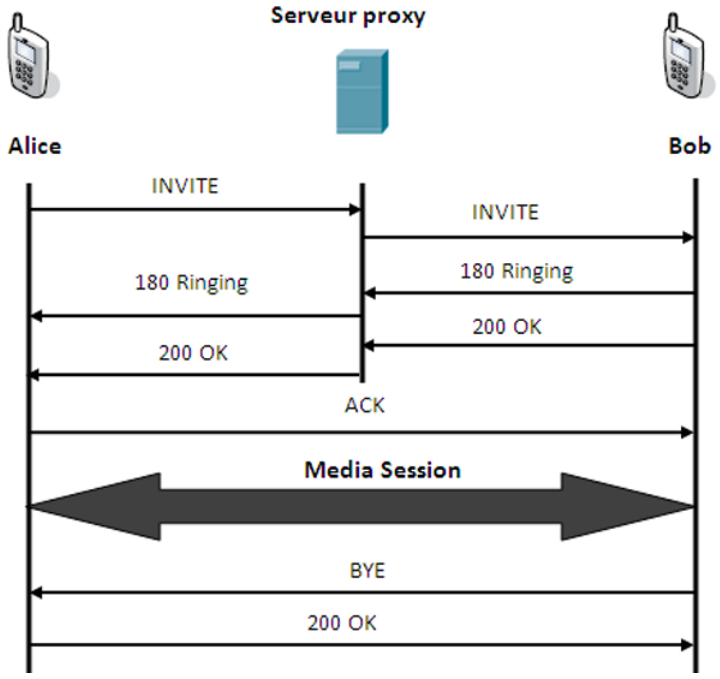

FIGURE 1.4 – Session SIP à travers un proxy [18]

Le serveur proxy joue un rôle d'intermédiaire en relayant les messages SIP entre Alice et Bob. Il ne gère pas le flux média (voix/vidéo), qui passe directement entre les deux participants une fois l'appel établi.

- **Le serveur de redirection (Redirect Server) :** Un utilisateur peut envoyer une requête d'invitation à une autre personne par l'intermédiaire d'un serveur de redirection. Ce serveur se chargera

de retrouver cette personne et de renvoyer les informations nécessaires au client appelant, pour qu'il puisse établir une connexion directe avec l'interlocuteur désiré. La figure 1.4 illustre le déroulement d'un appel SIP impliquant un Redirect Server, mettant en évidence les échanges de messages entre les différents acteurs du processus.

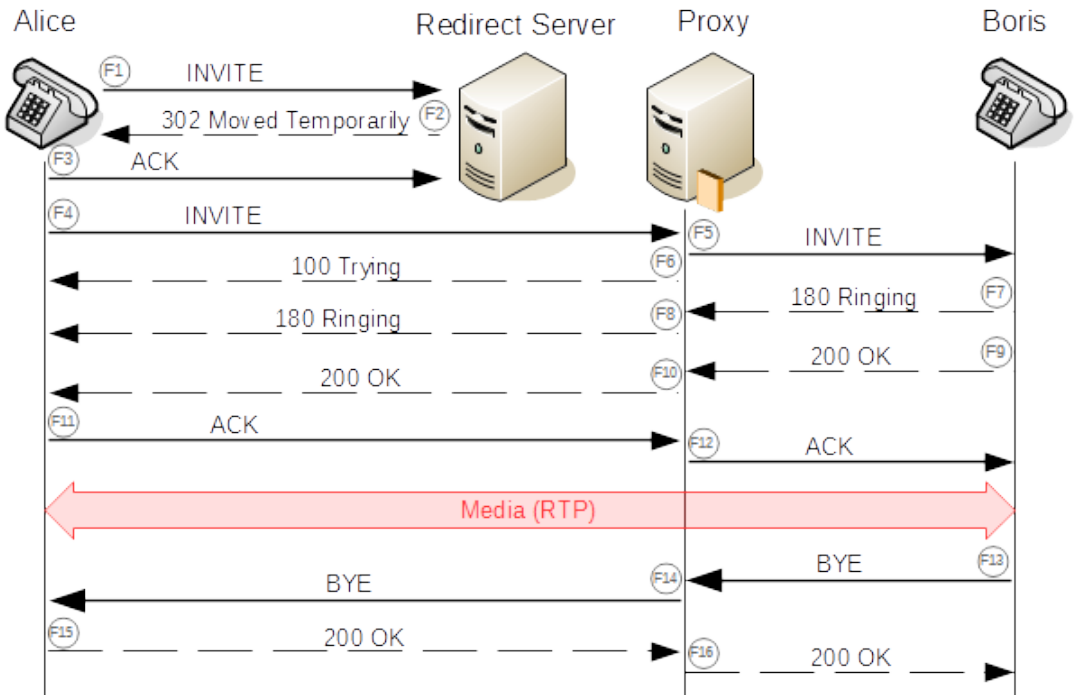

FIGURE 1.5 – Principe du protocole SIP [9]

- Alice envoie une requête INVITE au Redirect Server (F1) : Alice veut contacter Boris et envoie une requête SIP INVITE au Redirect Server.
- Le Redirect Server répond avec "302 Moved Temporarily" (F2) : Le Redirect Server indique qu'Alice doit contacter un autre serveur (le Proxy SIP) pour joindre Boris.
- Alice envoie un ACK au Redirect Server (F3) : L'ACK est l'accusé de réception de la réponse "302 Moved Temporarily".
- Alice envoie une nouvelle requête INVITE au Proxy (F4) : Maintenant qu'Alice sait qu'elle doit passer par le Proxy, elle envoie un nouvel INVITE à ce dernier.
- Le Proxy répond "100 Trying" (F5) : Le Proxy indique qu'il traite la requête
- Le Proxy relaie l'INVITE à Boris (F6) : Le Proxy transmet l'invitation à Boris
- Boris commence à sonner et répond avec "180 Ringing" (F7) : Boris est en train de recevoir l'appel et son téléphone sonne
- Le Proxy relaie la réponse "180 Ringing" à Alice (F8) : Alice est informée que Boris est en train de sonner
- Boris accepte l'appel et répond avec "200 OK" (F9) : Boris décroche l'appel et envoie une réponse 200 OK.
- Le Proxy relaie la réponse "200 OK" à Alice (F10) : Alice est informée que Boris a décroché.

- Alice envoie un Accusé de réception (Acknowledgment) (ACK)ACK à Boris via le Proxy (F11-F12) : L'ACK confirme la réception de la réponse 200 OK et établit la connexion.
- Établissement du flux RTP (Media) (F13) : La communication vocale entre Alice et Boris commence (flux RTP = Real-time Transport Protocol).
- Alice met fin à l'appel en envoyant un BYE (F14) : Lorsque la conversation se termine, Alice envoie un message BYE.
- Le Proxy relaie le BYE à Boris (F15) : Le Proxy transmet la demande de fin d'appel à Boris.
- Boris confirme avec "200 OK" (F16-F17) : Boris répond 200 OK pour confirmer la fin de l'appel.

1.4.4 Le protocole SDP (Session Description Protocol)

Le protocole SIP gére la signalisation, mais il ne s'occupe pas du contenu multimédia lui meme. Pour cela, SIP s'appuie sur le protocole SDP (RFC 4566), utilisé pour décrire les caractéristiques des flux à échanger[5].
SDP permet aux deux terminaux de négocier les éléments suivants

— Les types de média : audio, vidéo, text ...
— Les codecs utilisés ; G.711, G.729, Opus, etc.
— Les ports de communication.
— Le protocole de transport : RTP sur UDP.

1.5 Qualité de Service (QoS) dans la VoIP

1.5.1 Définition

La qualité de service désigne la mesure de l'excellence ou de la performance d'une entreprise ou d'une organisation dans la prestation de services à ses clients ou utilisateurs. Elle englobe divers aspects tels que la fiabilité, la réactivité, la courtoisie, la compétence, la pertinence et la satisfaction générale du client par rapport aux services reçus. La gestion de la qualité de service vise à assurer que les attentes des clients sont non seulement satisfaites, mais également dépassées lorsque cela est possible[6].

1.5.2 Les paramètres critiques en VoIP

Pour garantir une communication vocale fluide et de qualité en VoIP, certains paramètres techniques doivent être rigoureusement surveillés et optimisés. Ces paramètres jouent un rôle es-

sentiel dans l'expérience utilisateur [2].

Paramètre	Définition	Seuil recommandé
Latence (Delay)	Temps nécessaire à un paquet pour aller de l'émetteur au récepteur.	Inférieure à 150 ms pour éviter les retards perceptibles.
Gigue (Jitter)	Variation du délai de transmission des paquets.	Inférieure à 30 ms pour une qualité vocale fluide.
Perte de paquets	Pourcentage de paquets vocaux perdus durant la transmission.	Inférieure à 1 % pour éviter les coupures de son.
Débit (Bandwidth)	Quantité de données pouvant être transmises par seconde.	100 kbps à 200 kbps par appel selon le codec utilisé.
MOS (Mean Opinion Score)	Indicateur de la qualité perçue de la voix, notée de 1 à 5.	Supérieure à 3,5 pour une bonne qualité d'appel.

TABLE 1.1 – Paramètres critiques pour une communication VoIP de qualité

1.5.3 Impact de la Qualité de Service (QoS) sur la VoIP

la qualité de service est essentielle pour assurer la fiabilité des appels VoIP. En donnant la priorité à la QoS VoIP, pour éviter les problèmes d'appels lors de conversations importantes et améliorer la gestion du réseau. En outre, la mise en œuvre des paramètres et des meilleures pratiques en matière de qualité de service peut améliorer considérablement la qualité des appels et l'expérience des utilisateurs [2].

1.6 Les principaux avantages de la téléphonie sur IP (ToIP)

Différentes raisons peuvent pousser les entreprises à s'orienter vers la téléphonie sur IP (ToIP) comme solution de communication. Les avantages les plus marqués sont [22] [20] :

— **Réduction des coûts :** La la téléphonie sur IP (ToIP) permet de réaliser des économies importantes, notamment pour les entreprises. Contrairement à la téléphonie traditionnelle, elle utilise la connexion Internet existante pour transmettre les appels, ce qui supprime les frais liés aux lignes téléphoniques classiques. Les appels, notamment internationaux, sont souvent bien moins chers, voire gratuits entre utilisateurs VoIP. De plus, les coûts d'installation sont généralement faibles, voire inexistants, et les forfaits mensuels sont adaptés au nombre d'utilisateurs, ce qui rend la solution plus flexible et économique.

— **Mobilité :** La ToIP fonctionne entièrement via Internet, ce qui permet aux utilisateurs d'accéder à leur système téléphonique (IPBX) et à leur numéro professionnel depuis

n'importe quel appareil connecté (ordinateur portable, tablette, smartphone). Cela facilite grandement le travail à distance et la mobilité, faisant de la VoIP une solution incontournable pour les entreprises souhaitant moderniser leur mode de fonctionnement et adopter des pratiques plus flexibles.

— **Flexibilité :** Au lieu d'attendre des heures pour modifier l'infrastructure physique, comme c'est le cas avec la téléphonie analogique, la ToIP permet de modifier immédiatement les types de licences, les intégrations, les détails concernant les utilisateurs et bien d'autres choses encore, généralement sans même avoir besoin d'un technicien sur place.

— **Evolutivité :** Un système de téléphonie IP (ToIP) est facilement extensible. L'ajout ou la suppression d'utilisateurs s'effectue en quelques clics depuis l'interface d'administration du serveur IPBX. De plus, il est possible de connecter des utilisateurs distants (succursales, collaborateurs nomades, etc.) au système principal, ce qui facilite la croissance de l'entreprise.

— **Intégration avec d'autre outils :** Conformément à la philosophie des communications unifiées, les systèmes téléphoniques ToIP s'intègrent facilement vec des outils métiers et des applications de communication unifiée (CRM, ERP, messageries, etc.). On peut par exemple activer la numérotation directe depuis un navigateur (click-to-call), recevoir des messages vocaux par e-mail ou synchroniser automatiquement les contacts.

— **Fonctionnalités analytiques :** L'un des avantages les plus évidents d'un système téléphonique VoIP est que, en tant que logiciel informatique, il peut suivre, enregistrer et même analyser les données des appels. Cela donne un accès instantané à une mine d'informations, notamment la durée de l'appel, l'objet de l'appel, les entrées IVR et bien plus encore. Pour les organisations dotées de centres de contact ou d'autres services à forte intensité d'appels, cet avantage de la VoIP vaut à lui seul la peine d'être adopté.

1.7 Conclusion

Tout au long de ce chapitre, nous avons présenté les bases de la VoIP, son fonctionnement, ainsi que les principaux protocoles de signalisation et de transport (SIP, RTP, SDP) sur lesquels elle repose.

En tant que composante essentielle de la téléphonie sur IP (ToIP), la VoIP permet de remplacer les lignes téléphoniques classiques par des réseaux de données, la ToIP permet ainsi une plus grande flexibilité, une réduction significative des coûts, ainsi qu'une intégration avec d'autres outils numériques(CRM, ERP, etc.) [22].

CHAPITRE 2

EVALUATION DU SYSTÉME DE TÉLÉPHONIE DE L'EPB ET PROPOSITION D'UNE SOLUTION TOIP

2.1 Introduction

La transition de la téléphonie traditionnelle vers la téléphonie sur IP (ToIP) représente une phase Essentielle pour les Organisations. Cette nouvelle technologie permet non seulement de réduire les coûts des appels, mais aussi d'utiliser des services modernes comme la vidéoconférence, l'envoi de messages vocaux par internet, ou encore la connexion avec d'autres outils informatiques de l'entreprise.
Ce chapitre est consacré à la présentation du l'Entreprise Portuaire de Béjaïa (EPB) dans laquelle s'est déroulé notre stage. Nous commencerons par une brève présentation historique et organisationnel de l'EPB en mettant l'accent sur sa structure interne. Ensuite, nous procéderons à une analyse de l'architecture réseau existante, en identifiant les principales limitations du systéme de telephonie actuel, notammenten terme de performance, de sécurité et de gestion. Enfin, nous introduirons la solution ToIP proposée, basée sur la mise en place d'un serveur IPBX complet, mieux adapté aux besoins de l'entreprise.

2.2 Présentation du Port de Béjaïa

Le Port de Béjaïa, anciennement connu sous le nom de Bougie, est un site maritime historique qui remonte à l'Antiquité. Initialement un comptoir phénicien puis romain connu sous le nom de Saldae, Béjaïa s'est transformée au XIe siècle en la capitale du royaume des Hammadides, se positionnant comme un pôle culturel et scientifique important dans la région méditerranéenne.

C'est aussi de cet endroit que dérive le terme « bougie », en référence aux chandelles en cire que la cité exportait vers l'Europe. Durant la période coloniale française, le port a reçu de nouvelles installations maritimes, puis a fait l'objet d'une modernisation progressive suite à l'indépendance de l'Algérie. Actuellement, c'est un port multifonctionnel, administré par l'Entreprise Portuaire de Béjaïa (EPB), qui reçoit divers types de trafic, notamment pétrolier, des conteneurs, des vracs solides et liquides, ainsi que des navires à rouler.

FIGURE 2.1 – port de bejaia [4]

2.2.1 Structure de l'EPB

L'Entreprise Portuaire de Béjaïa (EPB) est structurée selon un modèle organisationnel héirarchique, illustré dans la figure 2.2. Elle est placée sous la supervision du Ministère des Transports, du Groupe SERPORT et du Conseil d'administration.

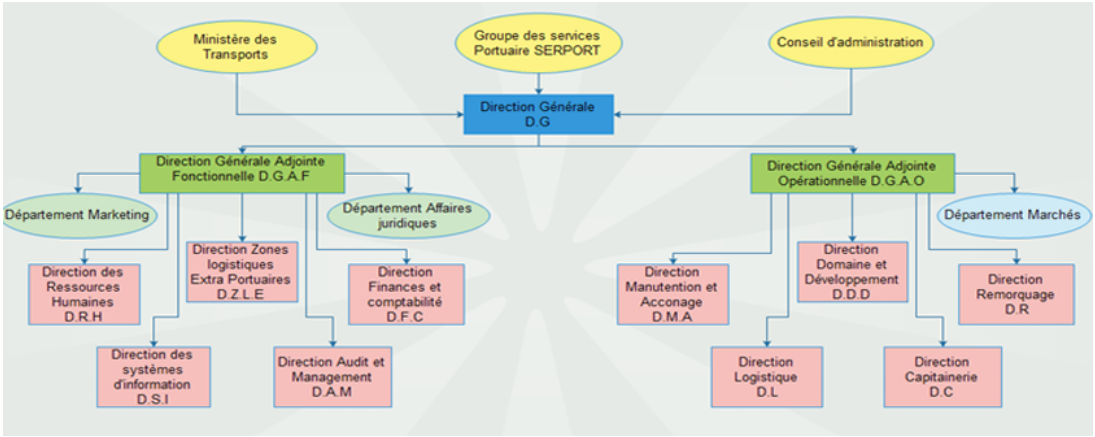

FIGURE 2.2 – Illustration de l'organigramme de l'EPB

Au sommet de cette hiérarchie se trouve la Direction Générale (D.G). Elle est soutenue par deux

directions adjointes :

— Direction Générale de l'Administration et des Finances (DGAF) , chargée des fonctions administratives et de gestion,

— La Direction Générale de l'Administration et de l'Organisation (DGAO), responsable des activités liées à l'exploitation portuaire.

Parmi les directions rattachées à la DGAF, on trouve la Direction des Systèmes d'Information (DSI) , qui joue un rôle essentiel dans la gestion et le développement des outils numériques et des infrastructures informatiques de l'entreprise. C'est au sein de cette direction que s'inscrit notre projet de modernisation de la téléphonie, par l'introduction d'une solution de téléphonie sur IP (ToIP) adaptée aux besoins de l'entreprise.

2.2.2 Le centre informatique de l'EPB

La structure du centre informatique comprend trois sections dirigées par l'assistant du Président Directeur Général (PDG), responsable des Systèmes d'Information. Chaque section est organisée en services, comme le démontre l'organigramme ci-dessous.

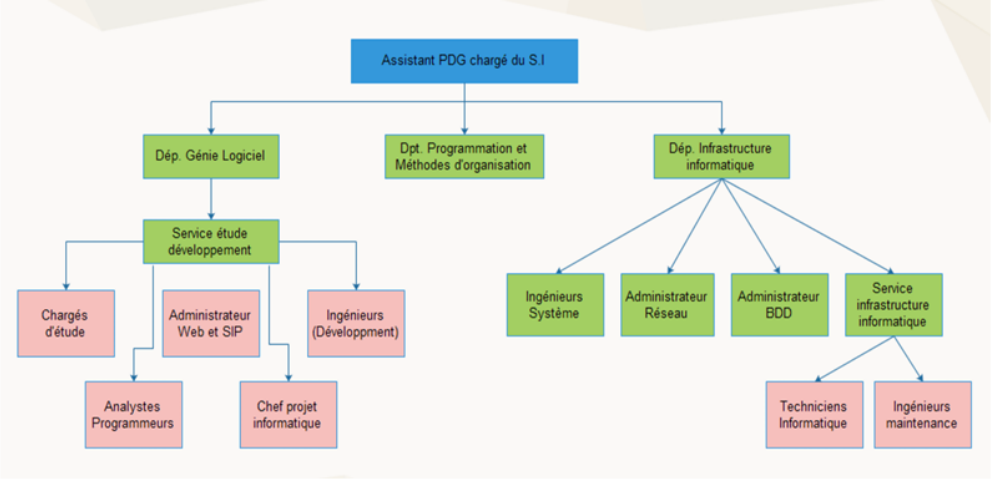

FIGURE 2.3 – Organigramme du département des systèmes d'informations

Afin de comprendre l'environnement dans lequel la solution de téléphonie sur IP (ToIP) a été deployée, il est indispensable de procéder à une étude de l'infrastructure informatique existante, notamment le réseau local (LAN) et ses principales composantes. Cette analyse nous permettra d'identifier les limites du système existant et de justifier les améliorations apportées par la solution de téléphonie sur IP proposée.

2.3 L'etude de l'existant

2.3.1 Réseau local de l'EPB

Le réseau local (LAN) de l'Entreprise Portuaire de Béjaïa (EPB) joue un rôle essentiel dans le bon fonctionnement de ses services. Cela facilite l'échange rapide et sécurisé d'informations entre divers postes de travail situés dans les bureaux et les départements techniques. Ce réseau permet aussi aux employés de se connecter à Internet, d'envoyer des courriels et d'utiliser des applications internes essentielles à leur travail quotidien, telles que la gestion documentaire, l'organisation des opérations portuaires ou encore le système de messagerie professionnel.

2.3.2 Présentation de l'architecture informatique du Port de Béjaïa

Sur le plan technique, l'architecture informatique du port de Béjaïa repose sur une infrastructure numérique en amélioration continue, conçue pour optimiser la gestion des services et assurer la fluidité des opérations portuaires. Elle regroupe plusieurs systèmes interconnectés, tels que :

— la surveillance des équipements,

— la gestion de la sécurité réseau,

— des solutions de téléphonie et de communication interne.

Cette organisation favorise la centralisation des données, renforce la collaboration entre les départements et permet un accès en temps réel aux informations essentielles, garantissant ainsi un fonctionnement optimal et un suivi efficace des opérations portuaires. La figure suivante illustre l'architecture réseau actuelle de l'EPB.

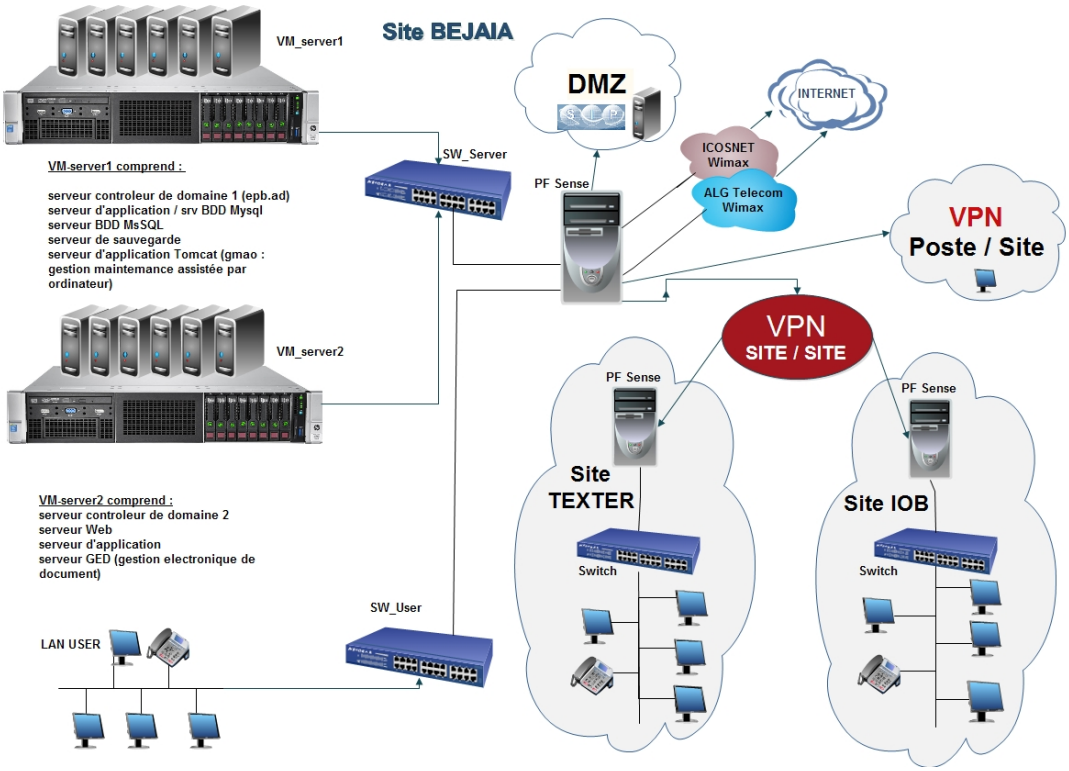

FIGURE 2.4 – Architecture du réseau informatique actuel de l'EPB

L'architecture repose principalement sur deux hyperviseurs virtualisés :

- ⋆ **VM_Hyperviseur 1 :** gère l'authentification, les bases de données, les sauvegardes et héberge plusieurs machines virtuelles . Il contient notamment les serveurs suivant :
  - **Contrôleur de domaine principal (Active Derctory) :** permet la création des sessions utilisateurs et assure l'intégrité, l'authentification et la confidentialité des accès.
  - **Serveur de bases de données Système de gestion de base de données relationnelle libre (My Structured Query Language) (MySQL) :** gère le stockage, la manipulation et l'interrogation des données des différentes applications.
  - **Serveur Tomcat :** héberge les systèmes de gestion des bases de données et exécute les requêtes SQL .
  - **Serveur de sauvegarde :** permet de sécuriser les données en conservant des copies régulières afin de pouvoir les restaurer en cas de défaillance.
- ⋆ **VM_Hyperviseur 2 :** prend en charge la gestion électronique des documents, l'hébergement du site web interne, ainsi que le contrôle de l'Active Directory et le domaine d'entreprise (système d'information portuaire). Il regroupe plusieurs serveurs, tels que :
  - **Contrôleur de domaine secondaire (Active Derctory)**
  - **Serveur Web (intranet/extranet) :**
    - Intranet : utilisé par les employés pour consulter les informations internes de l'entreprise.
    - Extranet : permet à certains partenaires ou clients d'accéder à des informations partagées, tout en garantissant la sécurité des échanges.

- **Le serveur GED (Gestion Électronique de Documents) :** est un système informatique permettant de centraliser, stocker, organiser et partager les documents électroniques de l'entreprise de manière sécurisée. Il offre un accès facilité aux documents depuis les différents sites de l'entreprise, y compris à distance, via une interface web ou une connexion sécurisée.
- **Serveur Système de noms de domaine (Domain Name System) (DNS) :** Le serveur DNS permet la résolution des noms de domaine en adresses IP. Il est essentiel pour l'accès aux services réseau, que ce soit en local ou via Internet.
- **Serveur Protocole de configuration dynamique des hôtes (Dynamic Host Configuration Protocol) (DHCP) :** Le serveur DHCP attribue automatiquement une adresse IP aux appareils connectés au réseau, ce qui facilite leur connexion sans configuration manuelle.

Les deux hyperviseurs principaux sont installés dans le data center de l'EPB. Ils reposent sur une infrastructure virtualisée, connectée à deux switchs principaux (SW_server et SW_User), et protégée par un pare-feu central pfSense.

— **PfSense (LAN / WAN / DMZ) :** PfSense est conçu pour surveiller, filtrer et contrôler le trafic entrant et sortant du réseau selon des règles de sécurité prédéterminées. Il constitue une barrière de protection entre le réseau interne de confiance et les réseaux externes non fiables.
Le pare-feu PfSense installé sur l'un des hyperviseurs, assure la segmentation du réseau en plusieurs zone fonctionnelles :

  - **Réseau étendu (Wide Area Network) (WAN) :** accès à Internet via deux fournisseurs (ALG Telecom).
  - **Réseau local (Local Area Network) (LAN) :** réseau local interne, connecté aux postes utilisateurs via le commutateur SW_User.
  - **Demilitarized Zone (DMZ) :** la zone démilitarisée (DMZ) est une zone réseau placée entre le réseau local de l'entreprise et Internet. Elle héberge les services accessibles depuis l'extérieur, tels que les serveurs web ou de messagerie. Dans l'architecture de l'EPB, la DMZ permet d'isoler ces serveurs exposés afin que, même en cas de compromission, les ressources sensibles de réseau interne reste protégées.

— **Switchs :**
SW_Server : assure la connexion des Hyperviseurs virtualisés (VM_Hyperviseur 1 et VM_Hyperviseur 2).
SW_Lan : relie les postes clients du réseau internes (LAN_USER).

— **Connexions Internet :** L'entreprise dispose de deux connexions ADSL ainsi que de deux connexions fibre optique haut débit (50Mbps et 30Mbps).

— **Data center (Salle serveur) :**Le Data center, détenu et exploité localement par l' entreprise, centralise les principaux équipements informatiques. Il comprend les serveurs,les systèmes de stockage, les équipements réseau (Switch, routeurs, pare-feu), ainsi que le câblage nécessaire à leurs organisation et à leur interconnexion. Son objectif est de garantir une disponibilité maximale, une sécurité physique et logique, ainsi qu'une efficacité énergétique optimale.

2.4 Evaluation du réseau de l'EPB

L'Entreprise Portuaire de Béjaïa (EPB) utilise toujours une infrastructure de téléphonie reposant sur le Réseau Téléphonique Commuté (RTC), à travers un PABX analogique. Ce système, bien que fonctionnel, est aujourd'hui dépassé face aux exigences modernes de communication. Il implique une séparation stricte entre les flux de voix et de données, rendant difficile toute centralisation, automatisation ou évolution rapide de la téléphonie d'entreprise.
Cette dissociation empêche l'EPB de bénéficier d'une gestion unifiée des services, limite la mobilité des collaborateurs et alourdit les coûts d'exploitation et de maintenance. De plus, l'ajout de nouvelles fonctionnalités (comme la messagerie vocale, la visioconférence, l'intégration avec un CRM ou un ERP, etc.) s'avère très complexe, voire impossible sans un changement d'infrastructure.
Dans un contexte où la transformation numérique devient un impératif stratégique, et où les besoins en flexibilité, mobilité et sécurité sont grandissants, ce type d'architecture classique ne répond plus aux enjeux actuels d'une entreprise moderne. Face à ces constats, la migration vers une solution de Téléphonie sur IP (ToIP), basée sur des technologies ouvertes comme Asterisk, s'impose comme une alternative logique et durable. Elle permet non seulement de mutualiser l'usage du réseau pour la voix et les données, mais aussi d'intégrer la téléphonie aux outils métiers et d'ouvrir la voie à des fonctionnalités avancées, le tout avec un meilleur contrôle des coûts.

2.5 Propositions de solution

Afin de remédier aux limitations identifiées dans l'infrastructure actuelle de l'EPB, plusieurs actions ont été mises en œuvre pour moderniser le systéme de communication, renforcer la sécurité et optimiser les flux d'échanges internes et externes.

- **Déploiement d'un serveur Asterisk :** La première étape a consisté à déployer un serveur Asterisk dédié, exclusivement réservé à la gestion de la téléphonie sur IP (ToIP). Cela va garantir une stabilité, une meilleure performance et facilite la maintenance du service. Le

serveur Asterisk intègre plusieurs fonctionnalités essentielle :
- Configuration du protocole SIP, pour permettre aux téléphones IP, qu'ils soient logiciels (softphones) ou physiques de communiquer entre eux via le réseau local. Il prend en charge l'établissement, la gestion et la terminaison des appels VoIP.
- Mise en place d'un serveur vocal interactif Réponse vocale interactive (Interactive Voice Response) (IVR), pour orienter automatiquement les appels entrans vers les services appropriés.
- Activation de la messagerie vocale, pour permettre aux employés de laisser et de recevoir des messages en cas d'absence ou d'indisponibilité.
- Ajout d'une musique d'attente personnalisée, pour améliorer l'expérience de l'appelant pendant les mises en attente.
- Fonctionnalité de parcage d'appel, pour permettre de mettre un appel en attente sur une extension spécifique pour qu'un autre poste le récupère.

- **Placement du serveur Asterisk dans la DMZ :** Pour garantir la sécurité des échanges, le serveur Asterisk est placé dans une zone DMZ, qui isole le serveur de téléphonie IP (ToIP) du réseau interne (LAN) et du WAN. Cette architecture limite les risques d'intrusion : même en cas de compromission d'un élément du système, l'accès à la DMZ reste limité et filtré, ce qui empêche toute propagation vers les autres zones du réseau.
- **Intégration d'un VPN poste-à-poste via Tailscale :**Afin de répondre aux besoins des utilisateurs distants et nomades, un VPN poste-à-poste basé sur Tailscale a été intégré. Cette solution complète le VPN site-à-site existant en permettant aux appareils mobiles ou hors-site d'accéder au réseau ToIP de manière sécurisée et sans configuration complexe.

2.6 Mise en place de la nouvelle architecture réseau de l'EPB

La nouvelle architecture réseau de l'EPB, illustrée par la figure ci-dessous, est conçue pour moderniser l'infrastructure existante tout en renforçant la sécurité, la fiabilité et la performance des communications internes et externes. Elle intègre les éléments suivants :

- Un serveur Asterisk dédié, placé dans la zone DMZ, pour assurer la gestion centralisée de la téléphonie sur IP (ToIP). Son positionnement en DMZ permet d'isoler les services de communication du reste du réseau interne, réduisant ainsi les risques de compromission.
- Un VPN de type Tailscale, basé sur le protocole WireGuard, à été integré pour permettre aux utilisateurs distants de se connecter de manière sécurisée au système de téléphonie IP (ToIP) sans exposé directement le serveur Asterisk à Internet.
  Cette nouvelle architecture permet à l'EPB de disposer :
  - D'un système de communication unifié et évolutif, capable de s'adapter aux besoins fu-

turs (ajout de postes, nouvelles fonctionnalités, intégration avec d'autres outils métiers).
- D'une infrastructure réseau plus sécurisée, grâce à la segmentation via la DMZ, l'utilisation de pare-feux (pfSense) et le chiffrement des connexions VPN.
- D'une meilleur expérience utilisateur, que ce soit pour les collaborateurs sur site ou pour ceux travaillant à distance,.

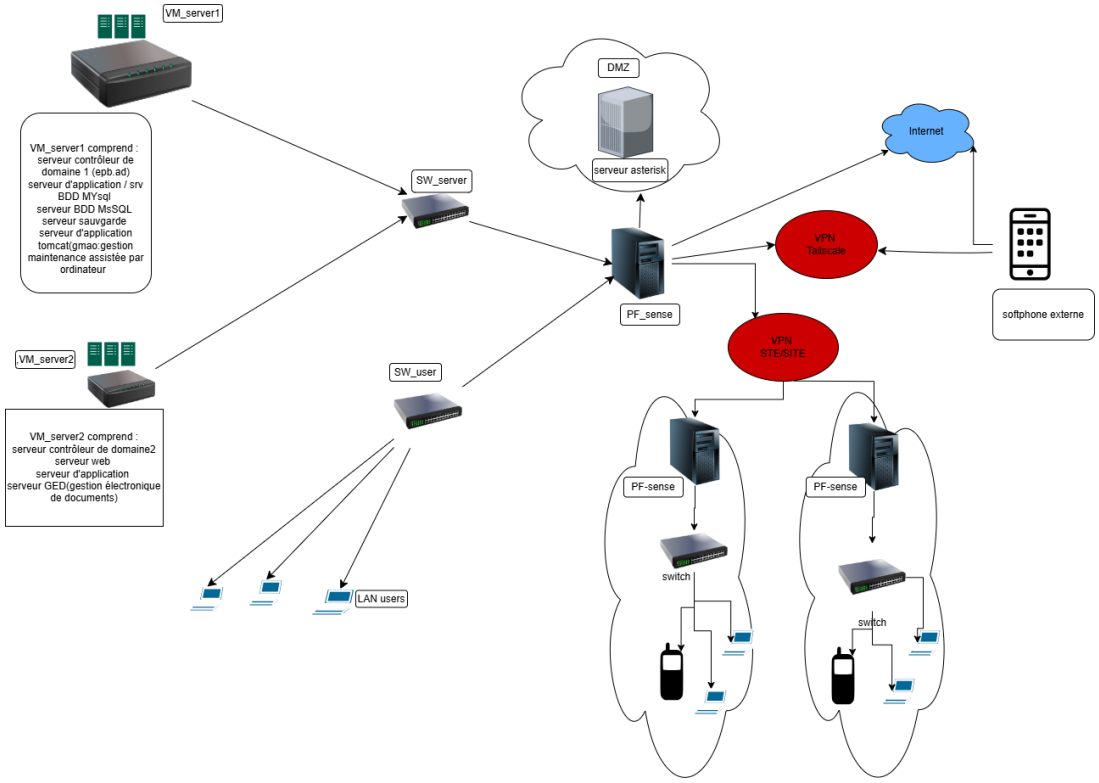

FIGURE 2.5 – Architecture du nouveau réseau de L'EPB

2.7 Conclusion

Dans ce chapitre, nous avons tout d'abord présenté l'Entreprise Portuaire de Béjaïa (EPB), son organisation et son infrastructure informatique existante pour comprendre son fonctionnement et ses besoins en communication.
Notre analysé pour leurs architecture réseau en place a révélé que le système de téléphonie reposait encore sur une technologie analogique (RTC via PABX) impliquant une séparation entre les services voix et données. Cette configuration, devenue obsoléte, limitait la flexibilité, l'évolutivité et l'efficacité des communications interne.
Nous avons alors proposé une solution de communication unifiée reposant sur le déploiement d'un serveur ToIP basé sur Asterisk permettant de centraliser la gestion des appels tout en offrant des fonctionnalités avancées (IVR, messagerie vocale, musique d'attente, etc.).
Afin de renforcer la sécurité, le serveur Asterisk est placé dans la DMZ. En outre, l'intégration

du VPN Tailscale permet aux utilisateurs distant ou en télétravail d'accéder de manière sécurisée au système de téléphonie IP.

CHAPITRE 3

DÉPLOIEMENT ET CONFIGURATION D'UN IPBX ASTERISK POUR LA TOIP

3.1 Introduction

Dans ce chapitre, nous présentons la mise en oeuvre d'une solution de Téléphonie sur IP (ToIP) au sein du réseau informatique de l'EPB. Après l'analyse des besoins et des limitations de l'ancienne infrastructure, nous avons choisi de mettre en place Asterisk comme serveur IPBX pour centraliser la gestion des communications.
Nous détaillerons d'abord les étapes d'installation et de configuration d'Asterisk sur un système Linux, puis nous expliquerons la création des comptes utilisateurs (extensions SIP) et l'intégration des principales fonctionnalités telles que la messagerie vocale, les appels de groupe, le serveur vocal interactif (IVR), ainsi que la mise en place d'une connexion distante sécurisée grâce au VPN Tailscale. Enfin, nous présenterons la configuration des clients SIP (softphones) pour les utilisateurs internes et mobiles.

3.2 Le standard téléphonique IPBX

Un IPBX (Internet Protocol Private Branch Exchange) est un standard téléphonique utilisé au sein des entreprises pour gérer les communications internes et externes en s'appuyant sur le protocole IP. Contrairement au PABX traditionnel, basé sur le réseau téléphonique commuté, l'IPBX utilise une infrastructure réseau basée sur le protocole IP et peut être connecté au réseau téléphonique public via un trunk SIP. Ainsi, l'IPBX permet une gestion plus souple, évolutive et économique des appels internes et externes.

Le fonctionnement d'un IPBX est basé sur la technologie ToIP (Téléphonie sur IP), qui permet de transmettre les communications vocales à traver un réseau IP. Cette technologie remplace les lignes téléphoniques classiques par des équipements compatibles avec le protocole SIP, tels que les téléphones IP, les ordinateurs ou encore les tablettes. Il existe aujourd'hui plusieurs solutions IPBX adaptées aux différents besoins des entreprises, qu'elles soient open source ou commerciales. Parmi les plus répandues, on peut citer [14] [23] :

- FreePBX : une interface graphique intuitive reposant sur Asterisk, conçue pour simplifier la gestion et la configuration du système sans avoir à modifier directement les fichiers de configuration.
- 3CX : une solution propriétaire orientée Windows, qui propose une interface conviviale et un ensemble complet de fonctionnalités prêtes à l'emploi.
- Issabel : une distribution open source dérivée de FreePBX, intégrant des outils supplémentaires comme un module Gestion de la relation client (Customer Relationship Management) (CRM), pour une gestion centralisée des communications et des clients.
- Elastix : une ancienne distribution tout-en-un bâtie sur Asterisk, qui a été largement utilisée avant d'être remplacée par d'autres forks tels qu'Issabel.

Pour évaluer le choix de la solution de téléphonie IP la plus adaptée aux besoins de l'Entreprise Portuaire de Béjaïa (EPB), nous avons comparé Asterisk à d'autres solutions populaires telles que FreePBX, 3CX et Issabel. Le tableau suivant met en évidence les différences en termes de flexibilité, d'interface, de coût, et d'évolutivité.

Asterisk	**FreePBX**	**3CX**
Gratuit (open source)	Gratuit / payant	Licence payante
Personnalisation	Très élevée (config. manuelle)	Moyenne (interface web)
Ligne de commande (CLI)	Interface web graphique	Interface web graphique
Linux (principalement)	Linux	Windows
Très active	Active	Moyenne
Très flexible	Moyenne	Faible
Manuelle	Assistée	Très assistée
Excellentes	Bonnes	Bonnes

TABLE 3.1 – Comparaison entre Asterisk et d'autres solutions de téléphonie IP

Dans le cadre de notre projet, on a choisi d'utiliser Asterisk, une solution open source puissante et flexible, très utilisée pour la mise en place de standards téléphoniques professionnels. Asterisk offre un haut degré de personnalisation et permet de déployer un système complet de téléphonie d'entreprise, aussi bien pour les communications internes qu'externes.

3.3 Présentation d'Asterisk

3.3.1 Historique

Asterisk a été créé lorsque Mark Spencer a souhaité acheter un PBX traditionnel pour sa compagnie en 1999. Estimant que le coût d'achat était excessif, il décide de développer sa propre solution en open source, accessible à tous. Le terme Asterisk vient du caractère « * », souvent utilisé comme joker pour représenter « tout » dans les commandes Unix et DOS. Dans l'objectif de concevoir des cartes d'interface à faible coût avec le réseau téléphonique traditionnel, son équipe a vite fait de se rapprocher de celle dirigée par Jim Dixon (Zapata Telephony Project). Ils ont visé à élaborer des cartes compatibles avec des plateformes fondées sur Intel, afin de rendre possible l'installation d'un PBX entièrement opérationnel sur tout PC disposant du système d'exploitation Linux, d'une carte d'interface et du logiciel Asterisk.

3.3.2 définition

Asterisk est un IPBX logiciel open source conçu pour fonctionner sur des systèmes de type Unix/Linux. Il offre toutes les fonctionnalités attendues d'un standard téléphonique professionnel, avec une grande modularité et une compatibilité étendue avec les équipements de téléphonie sur IP (ToIP) analogiques et numériques. Grâce à sa souplesse et à sa communauté active, Asterisk est régulièrement mis à jour et reste compatible avec de nombreux protocoles de téléphonie (SIP, IAX, H.323...).

3.3.3 Fonctionnalités

Asterisk offre un éventail complet de fonctionnalités professionnelles, souvent réservées aux solutions commerciales de téléphonie sur IP (ToIP) :

- Gestion des appels entrants et sortants
- Identification de l'appelant
- Standard vocal interactif (IVR)
- Boîte vocale
- Transfert, redirection et filtrage des appels
- Appels en conférence
- Enregistrement des appels
- Facturation détaillée Relevé de détails d'appel (Call Detail Record) (CDR)

— Écoute discrète et interception pour la supervision
— Musique d'attente personnalisée

3.3.4 Architecture

L'architecture d'Asterisk (voir figure 3.1) repose sur un noyau central qui assure la gestion des communications téléphoniques. Ce noyau interagit avec différents modules chargés de fournir des fonctionnalités spécifiques, comme :

- Modules de codecs : chargés de la conversion de la voix en paquets de données et inversement (exemple : G.711, G.729, etc.)
- Modules de protocoles : gèrent les communications via les protocoles supportés comme SIP, IAX ou H.323
- Modules de matériels : pour interfacer avec des cartes téléphoniques analogiques ou numériques
- Modules d'applications : fournissent des services tels que la messagerie vocale, les conférences, la mise en attente, etc.

Le fonctionnement du système est défini à travers des fichiers de configuration, notamment :

- pjsip.conf : définit les utilisateurs et les points de terminaison SIP.
- extensions.conf : contient le plan de numérotation (dialplan) qui gère la logique d'appel.
- voicemail.conf : configure les boîtes vocales des utilisateurs.

Ces fichiers définissent comment le système réagit à chaque type d'appel.
Asterisk utilise également les interfaces réseau pour :

— Échanger les messages de signalisation (par exemple via SIP pourl'établissement de sessions).
— Transmettre la voix sous forme de paquets IP (via RTP)

Grâce à cette architecture modulaire, Asterisk peut interagir avec divers équipements :

- Terminaux SIP (téléphones IP, softphones, applications web),
- Trunks SIP (accès au réseau téléphonique externe)
- Interface d'administration (CLI, GUI comme FreePBX).

Cette modularité permet à Asterisk de s'adapter aussi bien aux petites structures qu'aux grandes entreprises, jusqu'aux centres d'appels complexes.

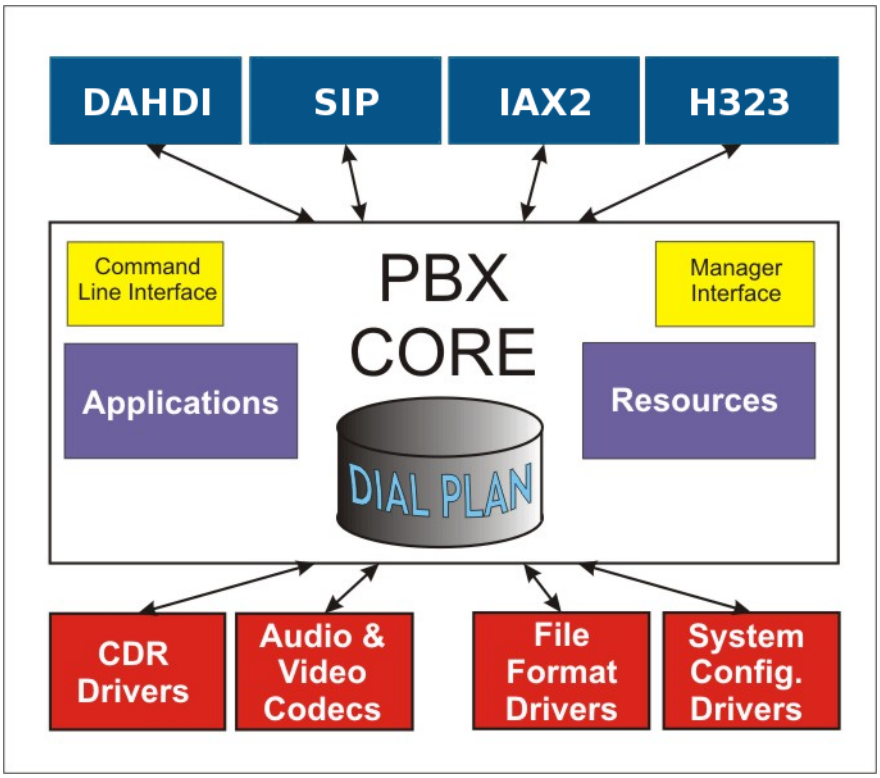

FIGURE 3.1 – Architecture fonctionnelle du serveur Asterisk[16]

3.4 Environnement de travail

Avant d'installer Asterisk, il est essentiel de définir précisément l'environnement technique utilisé. Cela garantit la compatibilité entre les composants, facilite la reproductibilité de l'installation, et permet une meilleure traçabilité du déploiement.

3.4.1 Système d'exploitation

Le système utilisé est Debian 12 (Bookworm), une distribution GNU/Linux reconnue pour sa stabilité, sa fiabilité et sa large adoption dans les environnements serveur. Debian offre une excellente gestion des paquets avec apt, ce qui facilite l'installation des dépendances nécessaires au bon fonctionnement d'Asterisk. Sa fiabilité en fait une plateforme idéale pour les services critiques comme un IPBX.

3.4.2 Machine virtuelle

Pour des raisons de flexibilité et de sécurité, l'installation d'Asterisk a été réalisée dans une machine virtuelle (VM). Cette approche permet de travailler dans un environnement isolé, de prendre facilement des instantanés (snapshots), et de restaurer le système en cas d'erreur ou de dysfonctionnement. Elle est particulièrement adaptée à un contexte pédagogique ou de test.
Les caractéristiques de la machine virtuelle sont les suivantes :

- Hyperviseur : Oracle VM VirtualBox (ou autre, selon le cas)
- Système invité : Debian 12 (64 bits)
- Mémoire vive (RAM) : 4 Go
- Processeur : 2 cœurs
- Disque dur : 20 Go (allocation dynamique)
- Accès réseau : Mode Pont (Bridge Adapter), permettant à la machine virtuelle d'être visible sur le réseau local et de communiquer avec d'autres équipements .
- Connexion Internet : Activée pour permettre la mise à jour du système et l'installation des paquets nécessaires.

Meme dans un environnement virtualisé, cette configuration permet une expérimentation réaliste d'un serveur de téléphonie IP, incluant la configuration de comptes SIP, les tests de communication, ainsi que l'intégration des fonctionnalités avancées d'Asterisk. La figure suivante présente l'environnement de la machine virtuelle utilisé pour le déploiement du serveur.

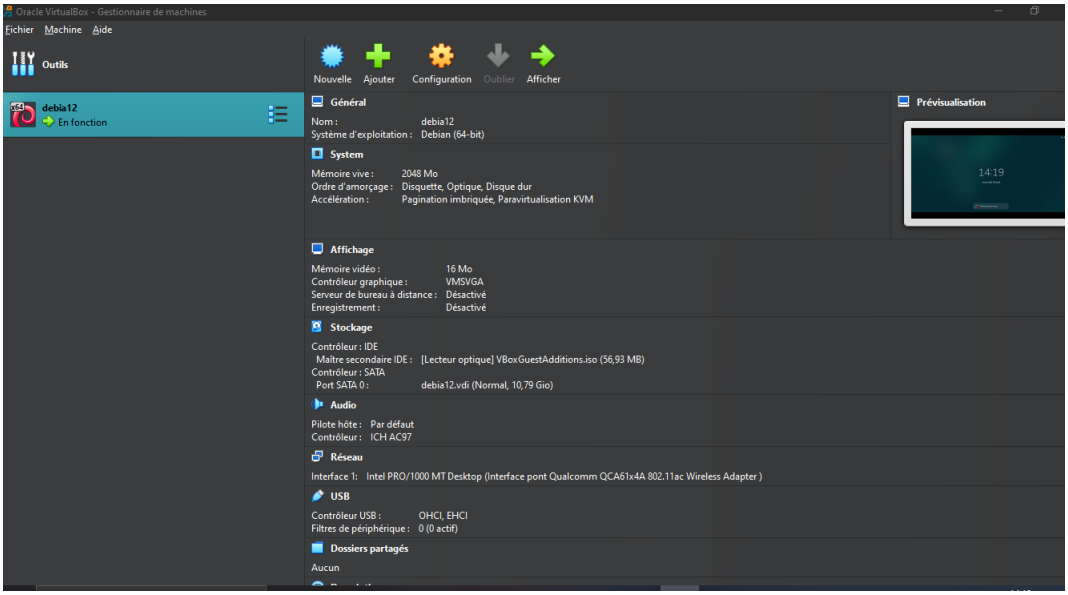

FIGURE 3.2 – Configuration générale de la machine virtuelle Debian sous VirtualBox

3.5 Les étapes d'Installation d'Asterisk 20

Cette section décrit de manière détaillée les étapes techniques nécessaires à l'installation d'Asterisk version 20 sur le système Debian 12 précédemment configuré. Le choix de cette version repose sur sa stabilité, ses nouvelles fonctionnalités et sa compatibilité avec les dernières versions des bibliothèques de la téléphonie sur IP. L'installation inclut les étapes suivantes :

- Téléchargement des sources : Récupération de la dernière version stable du code source depuis le site officiel d'Asterisk.
- Installation des dépendances : Installation des bibliothèques et outils requis pour compiler Asterisk (comme build-essential, libxml2-dev, libncurses5-dev, etc.).
- Compilation : Configuration du système via ./configure, choix des modules à compiler via make menuselect, puis compilation avec make.
- Installation : Déploiement des fichiers compilés dans le système via make install, suivi de make samples pour installer les fichiers de configuration par défaut.
- Création des utilisateurs et des droits : Ajout d'un utilisateur dédié (souvent asterisk) et configuration des permissions adéquates.
- Lancement du service : Démarrage du service Asterisk et vérification de son bon fonctionnement via la console Interface en ligne de commande (Command Line Interface) (CLI) (asterisk -rvvv).

Enfin, une configuration de base est mise en place afin de préparer le serveur à accueillir des terminaux SIP et à établir des communications internes.

Dans ce qui suit on décrit en détail le processus d'instalation

1. Mise à jour des paquets : Cette commande permet de mettre à jour la liste des paquets disponibles sur le système
   `apt update`

2. Installation des outils nécessaires
   `apt install nano wget tar curl`
3. Désactivation de AppArmor : AppArmor peut poser des problèmes avec Asterisk. Ces commandes arrêtent et désactivent ce service de sécurité.
   `systemctl stop apparmor`
   `systemctl disable apparmor`

4. Accès au répertoire source : On se place dans le répertoire /usr/src, qui est couramment utilisé pour compiler les logiciels à partir du code source.
   `cd /usr/src`

5. Téléchargement d'Asterisk : On télécharge l'archive contenant le code source de la dernière version stable d'Asterisk 20.
   wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20

6. Extraction de l'archive : Cette commande extrait le contenu de l'archive téléchargée.
   tar -zxvf asterisk-20-current.tar.gz

7. Suppression de l'archive :On entre dans le dossier du code source d'Asterisk. La version exacte peut varier selon l'archive téléchargée.
   rm asterisk-20-current.tar.gz

8. Accès au répertoire d'Asterisk : On entre dans le dossier du code source d'Asterisk. La version exacte peut varier selon l'archive téléchargée.
   cd asterisk-20.12.0/

9. Installation des dépendances : Ce script installe toutes les bibliothèques nécessaires pour compiler Asterisk.
   contrib/scripts/install_prereq install

10. Configuration du projet : Cette commande configure le projet Asterisk pour préparer la compilation selon les options disponibles sur le système.
    ./configure

11. Sélection des modules à compiler : Une interface s'ouvre pour choisir les modules que l'on souhaite activer (codecs, applications, formats, etc.).
    make menuselect

12. Compilation :On compile Asterisk à partir du code source. Cette étape peut prendre quelques minutes.
    Make

13. Installation d'Asterisk : Une fois compilé, Asterisk est installé dans le système.
    make install

14. Installation des fichiers d'exemple : Cette commande installe les fichiers de configuration d'exemple (pjsip.conf, extensions.conf, etc.).
    make samples

15. Sauvegarde des fichiers de configuration originaux :Par précaution, on sauvegarde les fichiers d'exemple dans un dossier séparé pour ne pas écraser les fichiers de configuration personnalisés.
    mkdir /etc/asterisk/samples
    mv /etc/asterisk/*.* /etc/asterisk/samples/

16. Création d'une configuration de base : Cette commande génère une configuration minimale prête à l'emploi pour un petit PBX.
    make basic-pbx

17. Création du service système : On installe les fichiers de service nécessaires pour démarrer Asterisk avec systemd.
    make config

18. Activation et démarrage d'Asterisk : Asterisk est activé au démarrage du système, et lancé immédiatement.
    systemctl enable asterisk
    systemctl start asterisk

19. Accès à la console Asterisk : Cette commande permet d'accéder à la console interactive d'Asterisk pour surveiller et tester le système.
    /usr/sbin/asterisk -r

3.6 Identification des fichiers de configuration

Une fois l'installation d'Asterisk terminée, plusieurs répertoires et fichiers essentiels sont créés automatiquement. Ils sont essentiels pour le bon fonctionnement du système, la gestion des appels et l'ajout de fonctionnalités personnalisées.

principaux Répertoires d'Asterisk :

- **/usr/sbin/ :** Contient le fichier binaire d'Asterisk (programme principal).
- **/usr/lib/asterisk/ :** Contient les fichiers qu'Asterisk utilise pour fonctionner.
- **/usr/lib/asterisk/modules/** Contient les modules pour les applications, les codecs, et les drivers.

- **`/var/lib/asterisk/sounds/`:** Contient les fichiers audio utilisés par Asterisk.
- **`/etc/asterisk/` :** Répertoire principal de configuration, il contient tous les fichiers .conf (fichiers de configuration) permettant de définir les comptes utilisateurs, les plans de numérotation, les boîtes vocales, les règles de routage, etc.

3.7 Mise en place d'un serveur de téléphonie interne

3.7.1 Configuration des comptes utilisateurs

Pour permettre la communication interne audio/vidéo entre plusieurs utilisateurs SIP (softphones ou téléphones IP), la configuration des comptes utilisateurs doit se fait directement dans fichier pjsip.conf . Chaque utilisateur est configuré à travers trois blocs : endpoint, auth, et aor.

Configuration du transport SIP :

```
[transport-udp]    ;  Nom du transport .
type=transport ; Indique qu'il s'agit d'un bloc de transport SIP.
protocol=udp ; le protocole utilise pour transporter les paquets SIP.
bind=0.0.0.0:5060 ; Le serveur écoute sur toutes les interfaces   ré
   seau à   l adresse   IP 0.0.0.0 et le port SIP standard 5060
```

Déclaration de l'utilisateur Nadjat (1001)

```
[nadjat]   ; Nom du terminal SIP (softphone ou téléphone IP).
type=endpoint   ;  C est  une configuration de terminal SIP.
context=default   ; Le contexte du dialplan utilisé est default (dans
    extensions.conf).
auth=nadjat11  ; Fait référence à   l  authentification   définie plus
   bas.
aors=nadjat  ; Référence à  l AOR  (Address Of Record),  c est
    l  identifiant   SIP
disallow=all   ;  Désactive tous les codecs.
allow=ulaw  ; Autorise les codecs audio
allow=alaw  ; Autorise les codecs audio
allow=g729  ;  Autorise les codecs vidéo.
allow=h264   ; Autorise les codecs vidéo
```

```
allow=vp8  ;Autorise les codecs vidéo
Authentification Nadjat
[nadjat11] ; Bloc de configuration   d  authentification   pour nadjat
type=auth ; Spécifie  q u il   s agit   d un  bloc
     d  authentification  .
auth_type=userpass  ; Utilisation  d un  nom  d utilisateur  et
    d un  mot de passe
username=nadjat ; Identifiant SIP.
password=ninanina  ; Mot de passe associé.
[nadjat] ; AOR pour l'utilisateur nadjat.
type=aor ; Adresse d'enregistrement SIP.
max_contacts=3 ; Autorise trois connexion active pour ce compte.
```

Déclaration de l'utilisateur Warda (1002)

```
[warda]
type=endpoint
context=default
auth=warda12
aors=warda
disallow=all
allow=ulaw
allow=alaw
allow=g729
allow=h264
allow=vp8
[warda12]
type=auth
auth_type=userpass
username=warda
password=ninanina
[warda]
type=aor
max_contacts=3
```

Déclaration de l'utilisateur karim (1003)

```
[karim]
type=endpoint
context=default
auth=karim13
```

```
aors=karim
disallow=all
allow=ulaw
allow=alaw
allow=g729
allow=h264
allow=vp8
 [karim13]
type=auth
auth_type=userpass
username=karim
password=ninanina
[karim]
type=aor
max_contacts=3
```

La figure suivante illustre le contenu du fichier pjsip.conf, utilisé pour la configuration des comptes SIP et des paramètres de transport dans le serveur Asterisk.

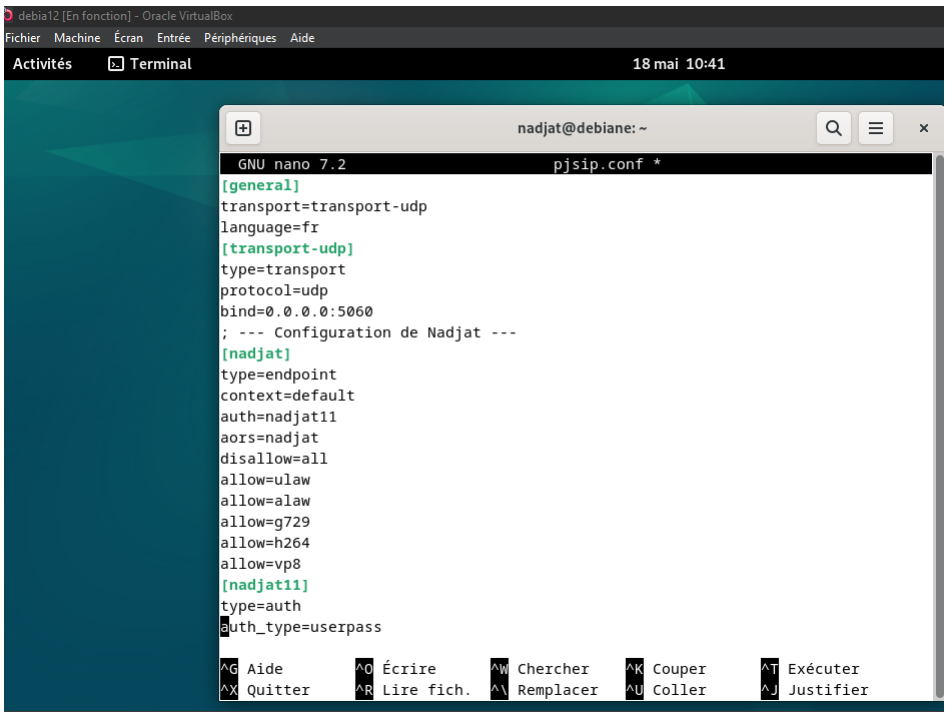

FIGURE 3.3 – Configuration de fichier pjsip.conf

3.7.2 Configuration de plan de numération extentions.conf

Le dialplan est l'élément central qui gère le fonctionnement du serveur Asterisk. Il offre la possibilité de savoir comment les appels doivent être gérés selon les numéros appelés par les utilisateurs. Dans ce projet, on utilise le contexte principal appelé [default] pour gérer les appels entre les utilisateurs configurés dans le fichier pjsip.conf.
La configuration suivante permet d'établir des communications audio et vidéo entre les utilisateurs enregistrés sur le serveur.

3.7.2.1 Configuration du Dialplan (à insérer dans extensions.conf)

Pour permettre des communications audio/vidéo, les appels sont configurés comme suit :

```
[default]
 ; Nadjat (1001)\\
exten => 1001,1,Dial(PJSIP/nadjat,30,TtV(video))

; Warda (1002)\\
exten => 1002,1,Dial(PJSIP/warda,30,TtV(video))

 ; Karim (1003)\\
exten => 1003,1,Dial(PJSIP/karim,30,TtV(video))
```

Explication des paramètres :
si l'appelant compose 1001, l'appel est dirigé vers Nadjat via PJSIP/nadjat. Il en est de même pour Warda (1002) et Karim (1003). La commande Dial() établit la communication avec une sonnerie de 30 secondes et les options TtV activent les transferts d'appel et la prise en charge de la vidéo.

3.7.2.2 Configuration du Dialplan pour un Appel de Groupe

Il est aussi possible de configurer une extension qui appelle plusieurs utilisateurs en même temps.
Dans le fichier extensions.conf, on ajoute une nouvelle extension qui va faire sonner plusieurs utilisateurs (Nadjat, Warda et Karim) en même temps.

```
exten => 1000,1,Answer()
 same => n,NoOp(Appel de groupe lancé)
```

```
 same => n,Dial(PJSIP/karim&PJSIP/warda&PJSIP/nadjat,20)
 same => n,Hangup()
exten => 2000,1,Answer()
 same => n,ConfBridge(8888)
same => n,Hangup()
```

Explication :
Lorsqu'un utilisateur compose le numéro 1000, les trois téléphones configurés (karim, warda, nadjat) sonnent simultanément pendant 20 secondes. Le premier utilisateur qui décroche est immédiatement redirigé dans la salle de conférence numéro 8888. Une fois qu'il est dans cette salle, il attend que d'autres participants la rejoignent. Extension 2000 : Cette extension permet aux autres utilisateurs de rejoindre manuellement la même salle de conférence 8888. Il leur suffit de composer 2000, et ils seront automatiquement connectés à la conférence.

- **Configuration des profils de conférence dans le fichier confbridge.conf :**

```
[general]

[default_bridge]
type=bridge

[default_user]
type=user
```

Explication : Ces deux profils seront utilisés dans la commande ConfBridge() dans le dialplan, afin de créer une salle de conférence fonctionnelle où plusieurs utilisateurs peuvent se parler en simultané.

3.7.3 Messagerie vocale (Voicemail)

La messagerie vocale permet à un utilisateur de laisser un message audio lorsqu'un correspondant ne répond pas à l'appel ou est occupé. Ces messages sont stockés sur le serveur et peuvent être consultés ultérieurement depuis un téléphone SIP via un numéro dédié. Asterisk propose une solution intégrée pour la mise en place de boîtes vocales via deux fichiers principaux :

- **Configuration du fichier voicemail.conf**

Ce fichier contient les paramètres généraux et les boîtes vocales de chaque utilisateur. Il définit aussi le format des messages .

```
[general]
```

```
format=wav49|gsm|wav
attach=yes
emailsubject=Message vocal de ${CALLERID}

[default]
1001 => 34,nadjat
1002 => 50,warda
1003 => 75,karim
```

Explication :

— `1001` : Numéro de l'extension de l'utilisateur.

— `34` : Mot de passe pour accéder à la messagerie vocale via le téléphone.

— `nadjat` : Nom de l'utilisateur (affichage dans les messages).

— `attach=yes` : Envoie le message vocal en pièce jointe par e-mail.

— `format=wav49|gsm|wav` : Formats audio dans lesquels les messages sont enregistrés.

- **Intégration dans le plan d'appel (`extensions.conf`)** : Pour permettre à chaque poste SIP de recevoir des messages en cas de non-réponse, on ajoute la directive suivante dans le plan de numérotation pour chaque utilisateur :

```
exten => 1001,n,VoiceMail(1002@default)
exten => 1002,n,VoiceMail(1002@default)
exten => 1003,n,VoiceMail(1002@default)

; Pour écouter les messages vocaux
exten => 5000,1,Set(CHANNEL(language)=fr)
exten => 5000,n,VoiceMailMain()
exten => 5000,n,Hangup()
```

Explication :

— `VoiceMail(1002@default)` : Si l'appel échoue, il est redirigé vers la boîte vocale de l'utilisateur 1002 dans le contexte `default`.

— `Set(CHANNEL(language)=fr)` : définit la langue de l'interface vocale en français.

— `VoiceMailMain()` : lance le menu de consultation de la messagerie vocale. L'utilisateur doit entrer son numéro de boîte et son mot de passe.

— `Hangup()` : termine l'appel après la consultation.

3.7.4 Mise en place d'un serveur IVR (Interactive Voice Response)

L'IVR (Interactive Voice Response) est une fonctionnalité essentielle d'un système téléphonique moderne. Elle permet à un appelant d'interagir avec un serveur vocal automatisé à l'aide du clavier de son téléphone. Grâce à ce système, les appels sont redirigés automatiquement vers les services appropriés selon les choix effectués par les utilisateurs comme représenté dans le schéma suivant.

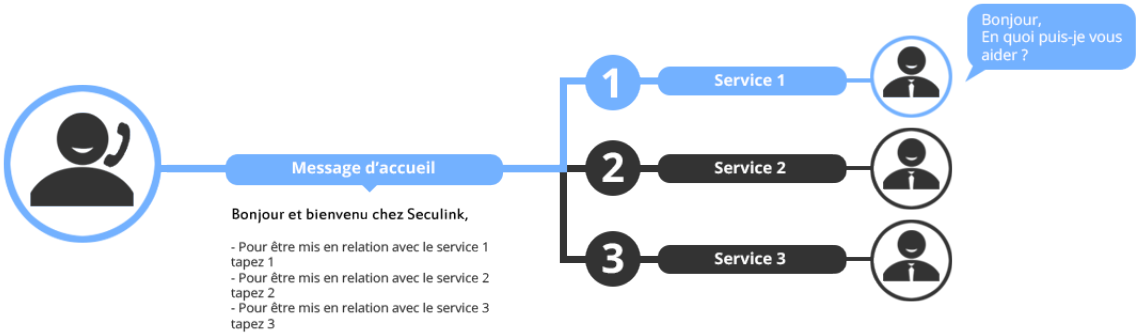

FIGURE 3.4 – Principe de fonctionnement d'un IVR [17]

Un menu vocal simple est mis en place : lorsqu'un appelant compose le 1234, un message de bienvenue est diffusé, puis plusieurs options lui sont proposées :

- Appuyer sur 1 pour être dirigé vers un agent de réception.
- Appuyer sur 2 pour être dirigé vers un agent de réservation.
- Appuyer sur 3 pour laisser un message vocal.

3.7.4.1 Etapes de la mise en œuvre

— **Etape 1 :Enregistrement des messages vocaux**

Utilisez l'application d'enregistrement audio disponible sur Debian pour créer les messages vocaux nécessaires au menus IVR (tels que welcome_msg, reception_info, et reservation_info) au format FLAC et l'image ci-dessous montre l'interface de l'enregistreur de son.

FIGURE 3.5 – Interface de l'enregistreur de son avec la liste des messages enregistrés

- **Message d'accueil (welcome_msg) :** Bienvenue sur notre service. Pour la réception, appuyez sur 1, pour la réservation, appuyez sur 2.

- **Message pour la réception(reception_info) :** Vous avez choisi la réception notre va vous répondre.

- **Message pour la réservation (reservation_info) :** Vous avez choisi la réservation notre agent va vous repondre.

- **Message pour laisser un message vocale (record-msg) :** Veuiller laisser un message apres l'annonce lorsque vous avez terminer appuyer sur la touche diese (#) .
- **Message de remeciment(thank-you) :** merci pour votre message nous vous répondrons dès que possible. Au revoir.

— **Étape 2 : Conversion des fichiers audio**
Convertir les fichiers audio enregistrés au format FLAC en fichiers au format WAV, compatible avec Asterisk, en utilisant la commande suivante : **ffmpeg -i welcome_msg.flac -ar 8000 -ac 1 welcome_msg.wav** ,On répéte la commande pour tous les fichiers.

— **Étape 3 : Copier les fichiers audio dans le répertoire des sons d'Asterisk**
sudo cp /home/nadjat/Bureau/*.wav /var/lib/asterisk/sounds/

— **Etape 4 : Configuration de la langue par défaut (Français)**
Pour que le serveur Asterisk utilise les fichiers audio en français (par exemple pour les messages d'erreur, les annonces dans l'IVR ou la messagerie vocale), il est nécessaire de définir la langue par défaut dans le fichier de configuration principal **asterisk.conf**.

```
[options]
defaultlanguage = fr; Définit la langue par défaut à "fr" (français
    )
languageprefix = fr ; Utilise le préfixe de langue pour rechercher
    les fichiers audio
```

— **Etape 5 : Configuration de l'IVR dans extensions.conf**

Voici l' extrait du fichier extensions.conf :

```
; IVR Menu principal
exten => 1234,1,Answer()
same => n,Playback(welcom-msg)
same => n,WaitExten(10)
; Option 1 : Transférer à Nadjat
exten => 1,1,Playback(reception-info)
same => n,Hangup()
; Option 2 : Informations sur la réservation (Warda)
exten => 2,1,Playback(reservation-info)
same => n,Playback(thank_you)
same => n,Hangup()
; Option 3 : Enregistrement  d un  message vocal
exten => 3,1,Playback(record_msg)
same => n,Record(/var/spool/asterisk/voicemail/default/client-message
    .wav,5,30)
same => n,Playback(thank_you)
same => n,Hangup()
; Gestion des erreurs
exten => i,1,Playback(invalid_option)
same => n,Goto(1234,1)
exten => t,1,Playback(timeout_msg)
same => n,Hangup()
```

Explications :

ce code établit un menu vocal interactif (IVR) au sein d'Asterisk. Quand un appelant compose le 1234, l'appel est pris en charge (Answer()), ensuite un message de bienvenue est joué (Playback(welcom-msg)), et cela est suivi d'une attente pour une saisie (WaitExten(10)). Trois options sont disponibles : en choisissant 1, l'appelant reçoit un message concernant l'accueil (Nadjat) ; en choisissant l'option2 , il obtient des renseignements sur la réservation (Warda),

avec l'option 3, il peut enregistrer un message vocal. En cas de saisie incorrecte (i) ou de dépassement de temps (t), des traitements sont prévus pour bien gérer ces erreurs.

— **Etape 6 : lecture des messages vocaux enregistrés :**
Pour écouter les messages vocaux enregistrés, on utilise la commande aplay sur le fichier message enregistré dans le répertoire **/var/spool/asterisk/voicemail/** comme suit :
aplay /var/spool/asterisk/voicemail/client-message.wav

3.7.5 Mise en attente avec musique dans Asterisk

La mise en attente permet à un utilisateur de suspendre temporairement une conversation téléphonique, tout en laissant l'appelant "en ligne", accompagné d'une musique d'attente. C'est une fonctionnalité essentielle dans les systèmes de téléphonie professionnelle (par exemple pour : transférer l'appel, chercher une information, répondre à un second appel).

3.7.5.1 Fonctionnement

Dans Asterisk, la mise en attente repose sur plusieurs éléments de configuration répartis dans les fichiers suivants :

- extensions.conf → Pour le comportement des appels.
- features.conf → Pour définir les touches de mise en attente et autres actions interactives (attente, transfert).
- musiconhold.conf → Pour configurer la musique d'attente.

Configuration de la mise en attente

1. Configuration dans features.conf :

```
  [general]
parkext => 700              ; Extension pour initier le parcage
d appel
parkpos => 701-720           ; Plage d extensions pour les
appels mis en attente
context => parkedcalls       ; Contexte d appel à utiliser
pour les appels en attente
courtesytone = beep           ; Bip sonore avant de reprendre
l'appel
parkedmusicclass = default    ;Classe de musique à jouer pendant
l'attente
```

```
[featuremap]
blindxfer => #      ;pour mettre en attente
```

2. Activation de la musique dans extensions.conf :
   Chaque extension d'utilisateur (ex : 1001) peut être configurée avec une musique d'attente personnalisée :

```
exten => 1001,1,Set(CHANNEL(musicclass)=default)
same => n,Dial(PJSIP/nadjat,30,TtV(video),10,m(default)b)
```

   Explication Lors d'un appel, si l'utilisateur souhaite faire une autre action (par exemple consulter une information ou passer un autre appel), il peut appuyer sur la touche # pour mettre l'appel en attente. À ce moment-là :

   — L'autre personne (l'appelant) est placée en attente.
   — Une musique d'attente est automatiquement jouée, ce qui permet à l'appelant de savoir que la communication est toujours active.
   — Pendant ce temps, l'utilisateur peut effectuer son action sans raccrocher.

   L'autre personne (l'appelant) est placée en attente.

3.7.6 Configuration des clients SIP (Softphones)

3.7.6.1 Définition

Un softphone est une application logicielle qui permet de passer et de recevoir des appels VoIP à l'aide d'un ordinateur ou d'un smartphone. Il fonctionne comme un téléphone IP, mais virtuellement, via une interface graphique.[22] **Softphones utilisés dans notre projet**
Pour tester la configuration du serveur Asterisk, on a utilisé deux types de clients SIP :

— Linphone (installé sur smartphone Android).
— MicroSIP(installé sur PC Windows).

3.7.6.2 Les étapes de configuration de microsip

Voici les étapes suivies pour configurer MicroSIP sur un poste client Windows :

1. Installation et lancement de l'application MicroSIP.
2. L'interface principale affiche un pavé numérique.
3. Cliquer sur la petite flèche en haut à droite, puis sélectionner « Compte » ou « Ajouter un compte ». (comme la figure 3.5 montre).

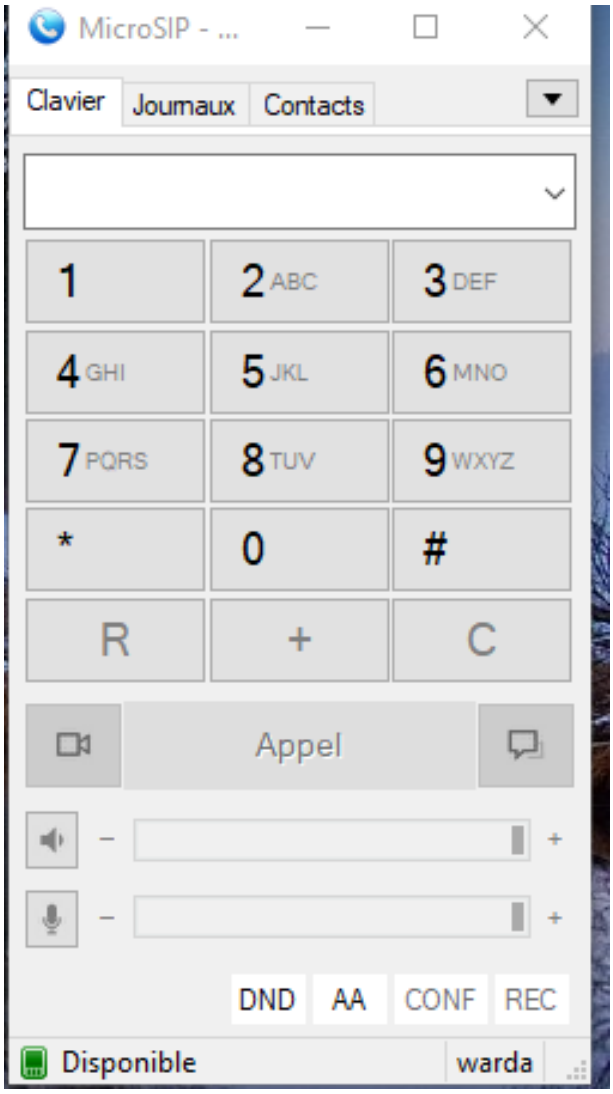

FIGURE 3.6 – Capture d'écran de l'interface principale de l'application

4. Renseigner les champs suivants avec les informations SIP définies dans pjsip.conf :
   • Nom d'utilisateur : identifiant SIP (ex. nadjat).
   • Mot de passe : mot de passe correspondant (ex. ninanina).
   • Domaine / Serveur SIP : l'adresse IP ou le nom du serveur Asterisk.
5. Cocher les options selon les besoins du fournisseur (ou laisser les options par défaut si Asterisk est en local).
6. Cliquer sur « Sauvegarder ».
   La figure suivante montre l'interface des parametres à configurer :

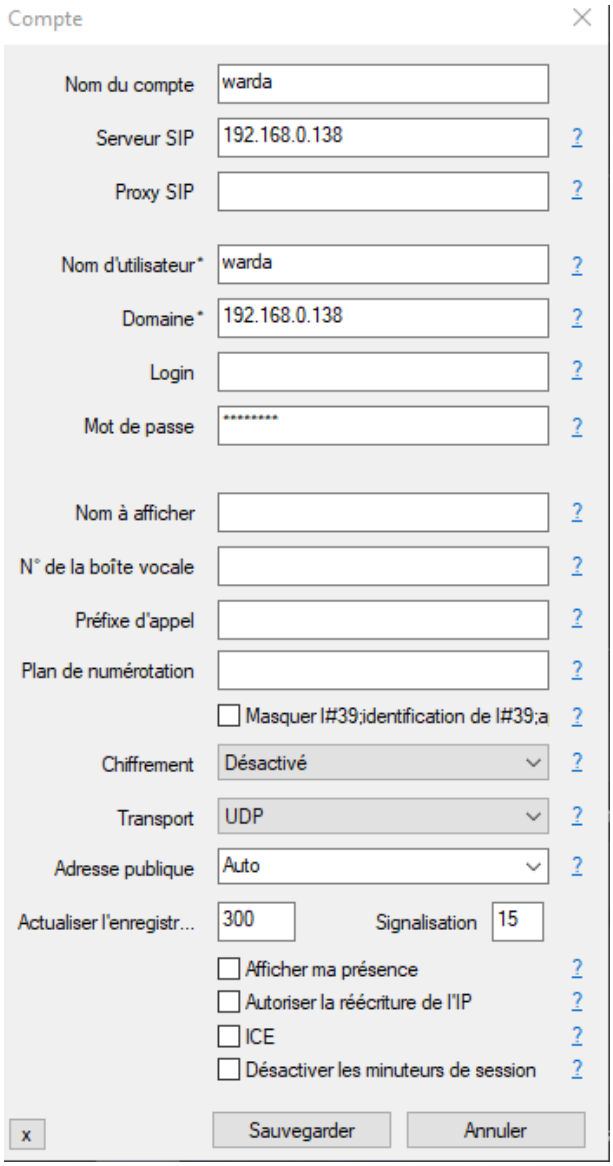

FIGURE 3.7 – Capture de l'écran de configuration du compte SIP

3.7.6.3 Les étapes de configuration de l'application Linphone sur smartphone

•Pour configurer un compte SIP dans Linphone, on a suivi les étapes ci-dessous :

1. Lancer l'application Linphone
2. Accéder au menu Paramètres .
3. Sélectionner l'option Comptes, puis appuyer sur Ajouter un compte SIP.
4. Remplir les champs de connexion avec les information du serveur Asrerisk comme la figure suivante montre :
   •Nom d'utilisateur (ex. nadjet).
   •Mot de passe (ex. ninanina).

•Domaine / serveur SIP (l'adresse IP ou le nom du serveur Asterisk).
•Nom d'affichage (facultatif).
•Type de transport (TLS, UDP ou TCP selon les recommandations de votre fournisseur).

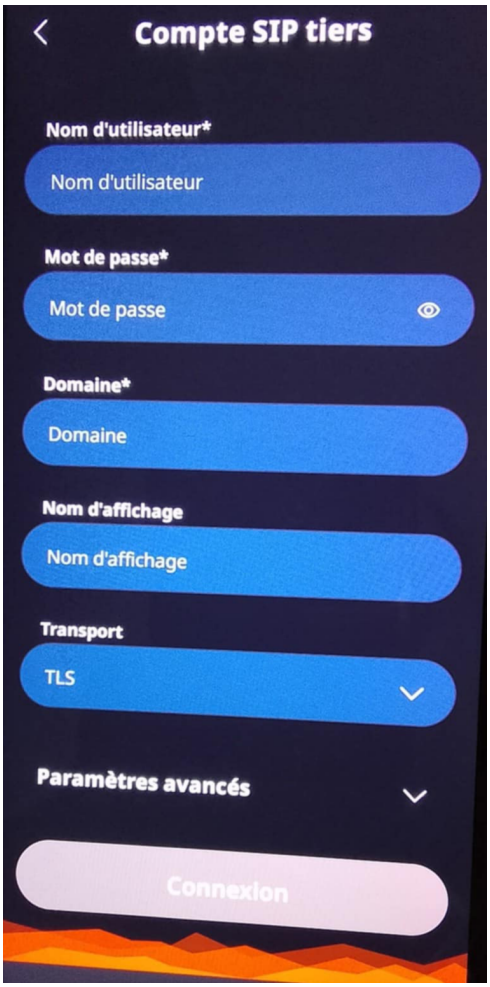

FIGURE 3.8 – Interface de configuration d'un compte SIP dans Linphone

3.7.7 Tests de communication entre utilisateurs internes

Après la configuration des utilisateurs internes, nous avons validé les appels audio et vidéo pour vérifier le bon fonctionnement de la solution VoIP. Les tests ont été réalisés avec les interfaces MicroSIP et Linphone, et les échanges techniques ont été observés dans la console Asterisk via la commande :**sudo asterisk -rvvv**

— Tests d'appels audio Les figures suivantes présentent les interfaces et la console lors d'un appel audio entre les utilisateurs interne.

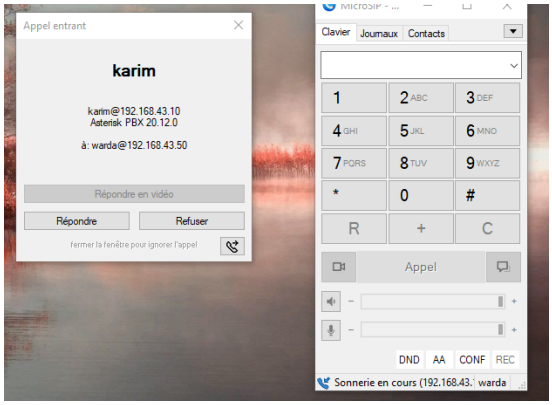

FIGURE 3.9 – Interface de MicroSIP lors l'appel audio.

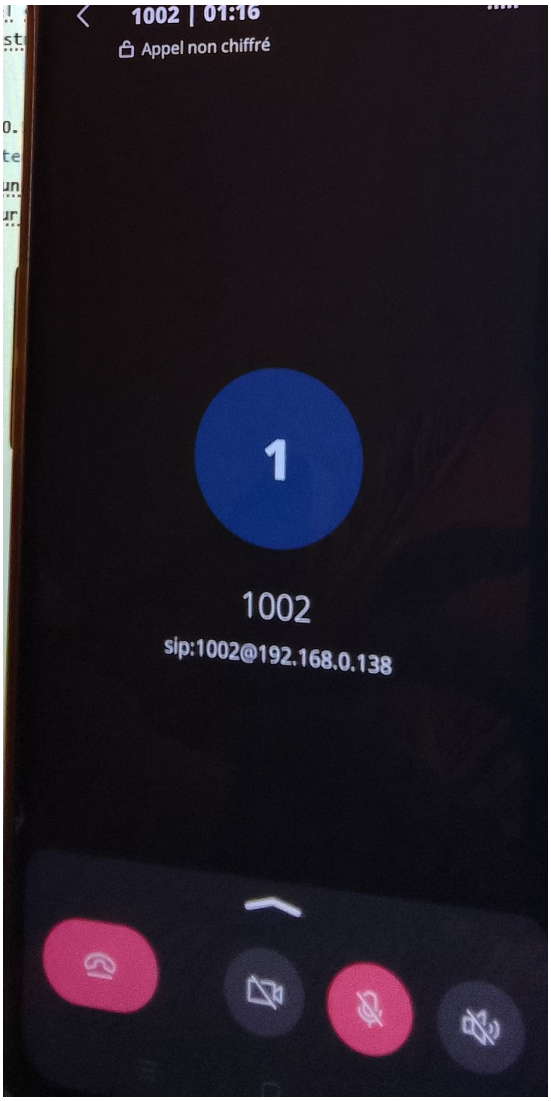

FIGURE 3.10 – Interface de Linphone lors l'appel vedio.

```
    -- Executing [1002@default:1] Dial("PJSIP/karim-00000000", "PJSIP/warda,30,TtV(video),10,m(default)
b") in new stack
[May 28 08:26:25] WARNING[2850][C-00000001]: app.c:3124 parse_options: Unrecognized option: 'V'
    -- Called PJSIP/warda
    -- PJSIP/warda-00000001 is ringing
       > 0x7f3d0c0954a0 -- Strict RTP learning after remote address set to: 192.168.43.50:4000
    -- PJSIP/warda-00000001 answered PJSIP/karim-00000000
       > 0x7f3d0c07f170 -- Strict RTP learning after remote address set to: 192.168.43.1:60549
    -- Channel PJSIP/warda-00000001 joined 'simple_bridge' basic-bridge <efddb259-3351-4c13-afc6-0fd3a7
31bc69>
    -- Channel PJSIP/karim-00000000 joined 'simple_bridge' basic-bridge <efddb259-3351-4c13-afc6-0fd3a7
31bc69>
       > 0x7f3d0c0954a0 -- Strict RTP switching to RTP target address 192.168.43.50:4000 as source
       > 0x7f3d0c07f170 -- Strict RTP switching to RTP target address 192.168.43.1:60549 as source
(0x7f3d0c0948f0) RTP audio difference is 277599856 set mark
       > 0x7f3d0c0954a0 -- Strict RTP learning complete - Locking on source address 192.168.43.50:4000
       > 0x7f3d0c07f170 -- Strict RTP learning complete - Locking on source address 192.168.43.1:60549
```

FIGURE 3.11 – Déroulement d'un appel interne entre utilisateurs

— Tests d'appels vidéo

Les figures suivantes illustrent les interfaces et la console pendant un appel vidéo.

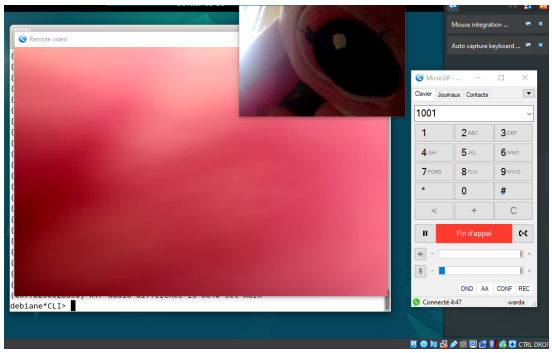

FIGURE 3.12 – Interface de MicroSIP pendant l'appel vedio.

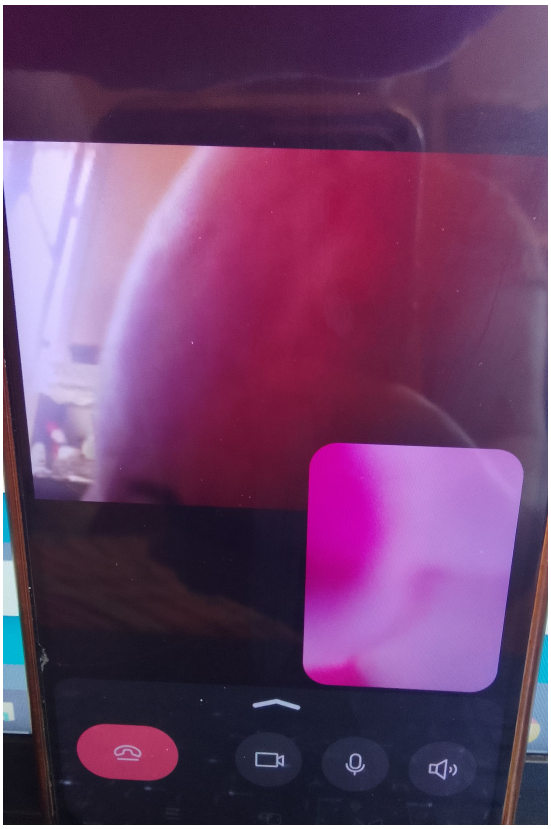

FIGURE 3.13 – Interface de Linphone pendant l'appel audio.

```
    -- Executing [1002@default:1] Dial("PJSIP/karim-00000000", "PJSIP/warda,30,TtV(video),10,m(default)
b") in new stack
[May 28 08:26:25] WARNING[2850][C-00000001]: app.c:3124 parse_options: Unrecognized option: 'V'
    -- Called PJSIP/warda
    -- PJSIP/warda-00000001 is ringing
       > 0x7f3d0c0954a0 -- Strict RTP learning after remote address set to: 192.168.43.50:4000
    -- PJSIP/warda-00000001 answered PJSIP/karim-00000000
       > 0x7f3d0c07f170 -- Strict RTP learning after remote address set to: 192.168.43.1:60549
    -- Channel PJSIP/warda-00000001 joined 'simple_bridge' basic-bridge <efddb259-3351-4c13-afc6-0fd3a7
31bc69>
    -- Channel PJSIP/karim-00000000 joined 'simple_bridge' basic-bridge <efddb259-3351-4c13-afc6-0fd3a7
31bc69>
       > 0x7f3d0c0954a0 -- Strict RTP switching to RTP target address 192.168.43.50:4000 as source
       > 0x7f3d0c07f170 -- Strict RTP switching to RTP target address 192.168.43.1:60549 as source
(0x7f3d0c0948f0) RTP audio difference is 277599856 set mark
       > 0x7f3d0c0954a0 -- Strict RTP learning complete - Locking on source address 192.168.43.50:4000
       > 0x7f3d0c07f170 -- Strict RTP learning complete - Locking on source address 192.168.43.1:60549
```

FIGURE 3.14 – Déroulement d'un appel interne entre utilisateurs

Ces tests prouvent que la solution VoIP permet des appels audio et vidéo entre les utilisateurs internes, avec un suivi en temps réel des échanges sur la console Asterisk.

3.8 Mise en place d'une solution d'appels externes

Dans le cadre de ce projet, nous avons déployé une solution de téléphonie IP basée sur Asterisk, qui autorise un utilisateur éloigné à effectuer des appels vers l'extérieur. Pour permettre à un

utilisateur distant d'établir une connexion sécurisée avec le serveur Asterisk et d'émettre des appels vers l'extérieur, nous avons utilisé Tailscale, une solution VPN simple, rapide à déployer et basée sur le protocole WireGuard.

3.8.1 Présentation de Tailscale

Tailscale est un fournisseur d'accès VPN moderne et sécurisé , Il permet d'établir chiffrées grâce au open source WireGuard , Il simplifie la création d'un réseau privé virtuel (VPN), où chaque machine connectée reçoit une adresse IP privée sécurisée de type 100.x.x.x. Tous les appareils connectés au même compte Tailscale peuvent communiquer comme s'ils étaient sur un même réseau local, quel que soit leur emplacement (chez soi, au bureau, ou en mobilité).
La figure suivante présente l'interface d'administration Tailscale, affichant la liste des appareils connectés au réseau virtuel, leur adresse IP attribuée, leur état de connexion et leur système d'exploitation.

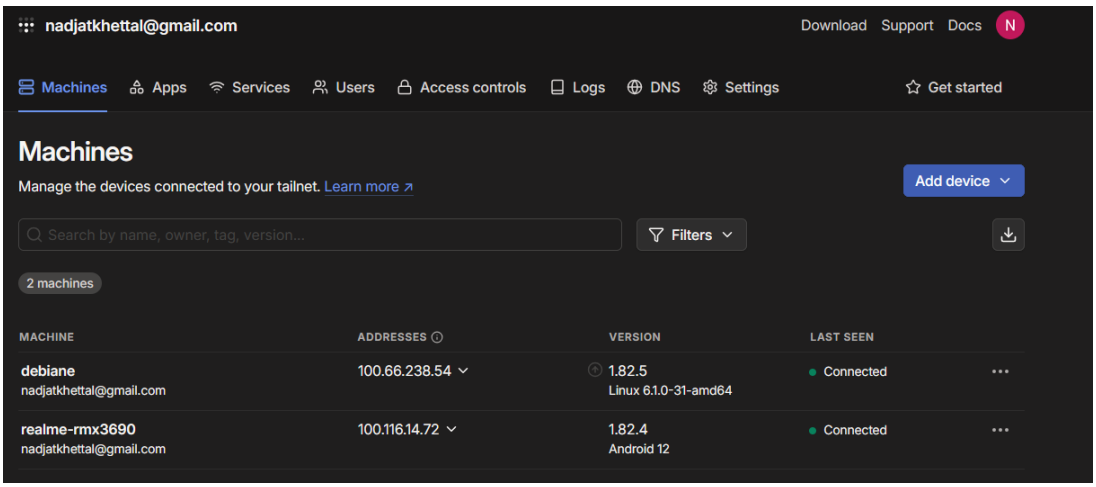

FIGURE 3.15 – Liste des appareils connectés via l'interface Tailscale

3.8.2 Fonctionnement de Tailscale

Le fonctionnement de Tailscale repose sur plusieurs principes clés :

- Utilisation de WireGuard : Tailscale utilise le protocole WireGuard pour chiffrer les échanges. WireGuard est un protocole VPN rapide, simple à configuré et sécurisé.
- Sécurité basée sur des clés publiques/privées : Chaque appareil possède une paire de clés pour authentifier et chiffrer les échanges (ChaCha20, Poly1305, Curve25519).
- Authentification simplifiée : l'utilisateur s'authentifie une seule fois via un fournisseur cloud (Google).

- Compatibilité multiplateforme : Tailscale est disponible sur Windows, macOS, Linux, Android, iOS, Synology NAS…

3.8.3 Sécurité du VPN

Un réseau privé virtuel (VPN) crée une connexion réseau privée entre plusieurs appareils via Internet. Les VPN servent à transmettre des données de manière sûre et anonyme sur des réseaux publics. Ils fonctionnent en masquant les adresses IP des utilisateurs et en chiffrant les données de manière à ce qu'elles soient illisibles pour toute personne non autorisée à les recevoir. La sécurité d'un VPN repose sur plusieurs aspects essentiels :

— **Chiffrement :** pour garantir la confidentialité des données.
— **Authentification :** pour s'assurer que seules les personnes autorisées ont accès au tunnel VPN.
— **Intégrité :** pour que les données ne soient pas modifiées ou corrompues pendant la transmission.

Ces fonctions sont assurées par le protocole VPN utilisé. Dans le cas de Tailscale, c'est le protocole WireGuard qui joue le rôle de moteur cryptographique.

3.8.3.1 Le protocole WireGuard

WireGuard est un protocole VPN moderne qui crée un tunnel sécurisé et rapide entre des appareils sur Internet. Il utilise une cryptographie avancée pour protéger les données échangées. Etant facile à configurer et très performant, il est parfaitement adaptées à la téléphonie sur IP (ToIP). WireGuard utilise des algorithmes cryptographiques modernes :

- ChaCha20 pour un chiffrement rapide et sécurisé.
- Poly1305 pour authentifier les paquets et garantir leur intégrité.
- Curve25519 pour un échange sécurisé des clés.
- BLAKE2s pour le hachage sécurisé des données.

3.8.4 Étapes de mise en place de la solution d'appel externe

Les principales étapes de mise en œuvre sont :

1. **Création du compte Tailscale**
   - Création d'un compte gratuit sur https ://tailscale.com.
   - Authentification via Google .

2. **Installation de Tailscale Sur le serveur Asterisk**
   - commande télécharge et installe le paquet Tailscale sur le système Debian.
   curl -fsSL https ://tailscale.com/install.sh | sh
   - Connexion au VPN Tailscale :
   sudo tailscale up
   - La commande affiche un lien :
   To authenticate, visit : https ://login.tailscale.com/a/xxxxxxxxxxx
   - Une fois authentifié avec le compte Tailscale, vous verrez ce message :
   Success. Machine is now connected to Tailscale.
   - Vérification de l'adresse IP Tailscale du serveur :
   tailscale ip -4 : 100.66.238.54
3. **Installation de Tailscale sur le client (softphone)**
   - Installer Tailscale sur le smartphone via Google Play (ou via le site : https ://tailscale.com/download).
   - Se connecter avec le même compte Tailscale que le serveur.
   - L'appareil rejoint automatiquement le réseau VPN.

4. **Configuration d'un utilisateur SIP dans Asterisk (amel) dans le fichier pjsip.conf**

```
[amel]
type=endpoint
context=external
auth=amel-auth
aors=amel
disallow=all
allow=ulaw
allow=alaw
allow=g729
allow=h264
allow=vp8

[amel-auth]
type=auth
auth_type=userpass
username=amel
password=ninanina

[amel]
type=aor
max_contacts=1
```

5. **Intégration dans le fichier extensions.conf**

```
  [external]
  ;amel
same => n,Set(CHANNEL(musicclass)=default)
exten => 1004,1,Dial(PJSIP/amel,30,TtV(video),10,m(default)b)
exten => 1004,n,Playback(record_msg)
exten => 1004,n,VoiceMail(1004@default)
```

•Explication
ce bloc se trouve dans le contexte [external] du fichier extensions.conf, qui est généralement destiné à configurer les extensions des utilisateurs externes ceux qui se connectent via un VPN Tailscale.

6. **Test d'un appel externe**

Après avoir configuré l'utilisateur externe dans Asterisk, nous avons effectué un test d'appel externe entre un utilisateur interne (karim) et un utilisateur externe (amel). Cet appel passe par le serveur Asterisk et l'IVR avant d'atteindre l'utilisateur final.
Pour vérifier que tout fonctionne correctement, nous avons ouvert la console CLI d'Asterisk avec la commande sudo asterisk -rvvv et nous avons observé les échanges en direct.
Dans ce test, l'utilisateur interne karim est connecté au réseau local (par exemple, 192.168.x.x) tandis que l'utilisateur externe amel accède au réseau via un VPN Tailscale, avec une adresse IP attribuée par Tailscale (par exemple, 100.116.x.x). Ces adresses IP distinctes montrent bien que les deux utilisateurs sont situés dans des réseaux différents : karim est dans le réseau interne de l'entreprise, et amel est dans un réseau externe mais sécurisé grâce au VPN Tailscale. Cela met en évidence la capacité du VPN Tailscale à relier des utilisateurs situés sur des réseaux différents tout en garantissant la sécurité des échanges.

— Les images suivantes montrent les interfaces de MicroSIP et Linphone pendant l'appel

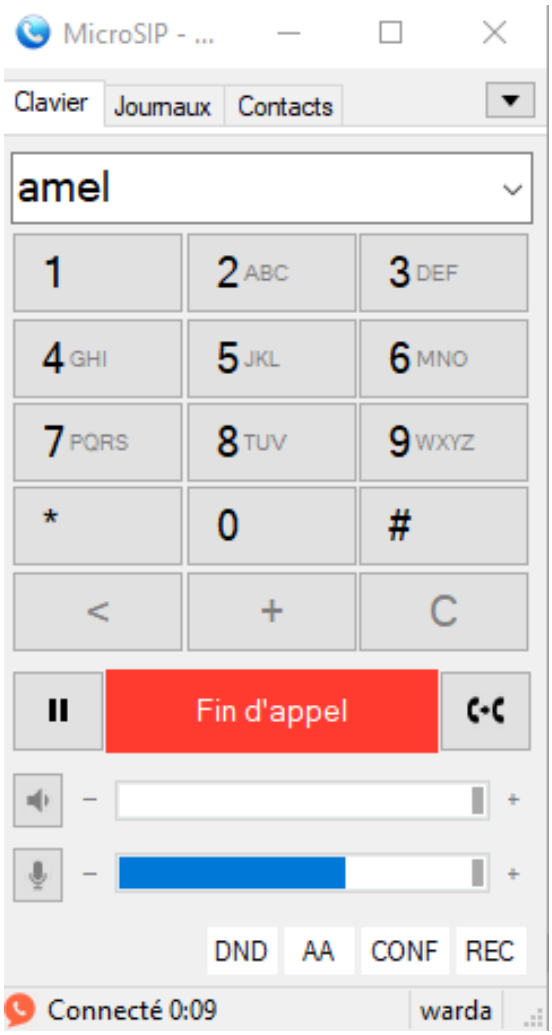

FIGURE 3.16 – Interface de MicroSIP pendant l'appel.

FIGURE 3.17 – Interface de Linphone pendant l'appel.

— Le déroulement de l'appel entre l'utilisateur interne et l'utilisateur externe est illustré ci-dessous.

```
'0x7f7a4c065e20) RTP audio difference is 279524160 set mark
      > 0x7f7a4c040610 -- Strict RTP learning complete - Locking on source address 192.168.0.197:4004
      > 0x7f7a4c0454e0 -- Strict RTP learning complete - Locking on source address 100.116.14.72:39423
    -- Channel PJSIP/warda-00000005 left 'simple_bridge' basic-bridge <13e768b8-1241-4db0-a136-f27e22fbb89
l>
    -- Channel PJSIP/amel-00000004 left 'simple_bridge' basic-bridge <13e768b8-1241-4db0-a136-f27e22fbb89d
>
  == Spawn extension (default, 1002, 1) exited non-zero on 'PJSIP/amel-00000004'
    -- Executing [1234@default:1] Answer("PJSIP/amel-00000006", "") in new stack
       > 0x7f7a4c05a6b0 -- Strict RTP learning after remote address set to: 100.116.14.72:32847
    -- Executing [1234@default:2] Playback("PJSIP/amel-00000006", "welcom-msg") in new stack
    -- <PJSIP/amel-00000006> Playing 'welcom-msg.slin' (language 'fr')
       > 0x7f7a4c05a6b0 -- Strict RTP switching to RTP target address 100.116.14.72:32847 as source
       > 0x7f7a4c05a6b0 -- Strict RTP learning complete - Locking on source address 100.116.14.72:32847
    -- Executing [1234@default:3] WaitExten("PJSIP/amel-00000006", "10") in new stack
    -- Executing [2@default:1] Playback("PJSIP/amel-00000006", "reservation-info") in new stack
    -- <PJSIP/amel-00000006> Playing 'reservation-info.slin' (language 'fr')
    -- Executing [2@default:2] Set("PJSIP/amel-00000006", "CHANNEL(musicclass)=default") in new stack
    -- Executing [2@default:3] Dial("PJSIP/amel-00000006", "PJSIP/warda,10,m(default)b") in new stack
    -- Called PJSIP/warda
    -- Started music on hold, class 'default', on channel 'PJSIP/amel-00000006'
    -- PJSIP/warda-00000007 is ringing
       > 0x7f7a4c0b3380 -- Strict RTP learning after remote address set to: 192.168.0.197:4006
    -- PJSIP/warda-00000007 answered PJSIP/amel-00000006
```

FIGURE 3.18 – Déroulement d'un appel entre un utilisateur interne et un utilisateur externe

Ces tests montrent que les appels entre les utilisateurs internes et externes passent correctement, prouvant que Tailscale est une solution efficace et fiable pour les connexions distantes.

3.9 Conclusion

Ce chapitre a présenté en détail la mise en oeuvre d'un systéme de téléphonie sur IP basé sur le serveur IPBX Asterisk 20. L'instalation et la configuration du serveur nous ont permit de mettre en place un système de téléphonie complet assurant des fonctionnalités essentielles telle que la messagerie vocale, le serveur vocal interactif (IVR), la gestion des comptes SIP, la musique d'attente, ainsi que les appels externes, effectués via la connexion sécurisée grâce à un VPN Tailscale pour les utilisateurs distants.

CONCLUSION GÉNÉRALE

La téléphonie sur IP (ToIP) s'impose aujourd'hui comme une technologie incontournable pour moderniser les systèmes de communications des entreprises. Elle constitue une alternative flexible, économique et riche en fonctionnalités par rapport aux infrastructures téléphoniques traditionnelles. Dans ce mémoire, nous avons mené un projet concret visant à déployer une solution de téléphonie IP adaptée aux besoins de l'Entreprise Portuaire de Béjaïa (EPB). L'objectif principal était de concevoir et de mettre en œuvre une architecture complète, fiable et sécurisée, capable de gérer efficacement les communications internes et externes.

Pour cela, nous avons opté pour le logiciel libre Asterisk 20, installé sur un système Debian Linux. Les configurations effectuées sur Asterisk nous ont permis de concevoir un serveur IPBX capable de gérer des comptes SIP, les appels interne et externes, la messagerie vocale, le serveur vocal interactif (IVR), ainsi que d'autres fonctionnalités avancées. Afin d'assurer la continuité des communications, nous avons utilisé un VPN Tailscale. Ce dernier est basé sur le protocole WireGuard permettant des connexions chiffrées de bout en bout pour les utilisateurs distants (comme les télétravailleurs ou les agents en déplacement). Le serveur Asterisk a également été placé dans une DMZ pour isoler les services exposés et de renforcer la sécurité de l'architecture réseau. Ce projet nous a permis d'acquérir une solide expérience pratique dans plusieurs domaines clés de l'informatique et des télécommunications :
En administration système Linux, avec l'installation et la configuration de Debian comme base du fonctionnement de la solution ToIP.
En configuration de serveur Asterisk, notamment à travers la manipulation des fichiers de configuration principaux pjsip.conf et extensions.conf.
En compréhension des protocoles SIP et RTP, utilisés respectivement pour la signalisation et le transport de la voix . Bien que le système mis en place répend aux objectifs initiaux, plusieurs axes d'amélioration sont envisageables pour le futur. Parmi eux : l'intégration de téléphones IP physiques, l'ajout de services supplémentaires comme la visioconférence et l'interconnexion

avec des outils métiers comme les CRM (CustomerRelationship Management) [22]et les ERP (Enterprise Resource Planning). Ces outils permettraient d'automatiser certaines tâches, d'améliorer la qualité du service client, et d'accroître la productivité globale. En effet, les CRM permettent de visualiser en temps réel les informations du client lors d'un appel entrant, de leur côté, les ERP permettent d'automatiser certaines tâches comme la facturation, la gestion des commandes ou le suivi des interventions.

En conclusion, ce mémoire démontre qu'il est possible, grâce à des outils open source et à une approche rigoureuse, de moderniser efficacement la téléphonie d'une entreprise comme le Port de Béjaïa. Cette démarche offre non seulement un gain significatif en termes de coûts et de fonctionnalités, mais prépare également l'entreprise à intégrer les technologies de communication de demain.

4 juillet 2025

BIBLIOGRAPHIE

[1] Andée. Visite guidée de la téléphonie. https://www.andee.fr/index.php/blog/12-visite-guidee-de-la-telephonie, 2025. Consulté le 25 avril 2025.

[2] CloudTalk. Qu'est-ce que la qos dans la téléphonie d'entreprise ?, 2023. Consulté le 2 juillet 2025.

[3] Didier Debourdeau. Voip – voix sur ip, 2002. Consulté le 15 mars 2025.

[4] DNA Algérie. Le pire évité de justesse au port de béjaïa, 2025. Consulté le 5 mai 2025.

[5] Bouygues Telecom Entreprises. Comprendre le protocole sip : fonctionnement et avantages, 2024. Consulté le 2 avril 2025.

[6] Eurofiscalis. Qualité de service (qos) : Définition, avantages et fonctionnement, 2023. Consulté le 2 juillet 2025.

[7] FrameIP. La téléphonie voip : fonctionnement, avantages et infrastructure, 2024. Consulté le 12 mars 2025.

[8] frameip. La voip et la toip pour les nuls. https ://www.frameip.com/toip-voip-pour-les-nuls/21-8211comment-fonctionne-la-voip, 2025. Consulté le 12 mars 2025.

[9] François-Emmanuel Geoffnet. *Protocole SIP : Consulte VoIP, analyse avec Wireshark, protocole, et mise en œuvre avec Asterisk*. Leanpub, 2021. consulté le 15 mars 2025.

[10] Tshiam Arsène Jean-luc. Mise en place d'un système de téléphonie par voip via le serveur trixbox. Travail de graduat, Université Liberté, Faculté des Sciences Informatiques, République démocratique du Congo, 2016. Consulté le 2 mars 2025.

[11] Kavkom. La téléphonie ip : définition et fonctionnement. https ://kavkom.com/articles/telephonie/telephonie-ip-definition-et-fonctionnement/, 2025. Consulté le 3 mars 2025.

[12] Amor Lazzez. Voip technology : Security issues analysis. *arXiv preprint arXiv :1312.2225*, 2013. consulter le 4 mars 2025.

[13] Ahmadreza Montazerolghaem, Mohammad Hossein Yaghmaee, and Alberto Leon-Garcia. Opensip : Toward software-defined sip networking. *IEEE Transactions on Network and Service Management*, 2019. consulter 22 avril 2025.

[14] Napsis. la telephonie ip. https ://www.napsis.fr/telephonie-ip/, 2025. Consulté le 3 mars 2025.

[15] Napsis. Réseau rtc : comprendre la téléphonie traditionnelle. https ://www.napsis.fr/actualite/reseau-rtc-telephonie/., 2025. Consulté le 12 mars 2025.

[16] Asterisk Project. Asterisk architecture – the big picture, 2024. Consulté le 26 mai 2025.

[17] Seculink Maroc. Serveur vocal interactif (svi). `https://www.seculink.ma/site/index.php?q=svi`, 2025. Consulté le 25 mars 2025.

[18] Techno-Science.net. Voip - définition et explication, 2024. Consulté le 12 mars 2025.

[19] Wikipedia contributors. mode acce. `https://ami-gestion.fr/acces-telephonie-ip/`, 2020. Consulté le 5 mars 2025.

[20] Wikipedia contributors. avantage. `https://www.cloudtalk.io/fr/blog/comment-fonctionne-la-voip/`, 2025. Consulté le 10 mars 2025.

[21] Wikipedia contributors. codec. `https://www.napsis.fr/telephonie-ip/voip-voix-ip/`, 2025. Consulté le 10 mars 2025.

[22] Wikipedia contributors. codec avantage. `https://www.ringover.fr/blog/voip`, 2025. Consulté le 10 mars 2025.

[23] Wikipedia contributors. La voip. `https://fr.wikipedia.org/wiki/Voix_sur_IP`, 2025. Consulté le 3 mars 2025.

Résumé

La transmission de l'information et la communication occupent aujourd'hui une place centrale dans les infrastrictures modernes. Parmi les technologies les plus marquantes figure la Téléphonie sur IP (ToIP), qui permet le transport de la voix sous forme de paquets de données à travers les réseaux IP. Elle s'impose grâce à ses nombreux avantages en termes d'intégration, de fiabilité, d'évolutivité et de réduction des coûts.

Ce mémoire s'inscrit dans le cadre d'un projet réalisé au sein de l'Entreprise Portuaire de Béjaïa (EPB), et vise à concevoir et sécuriser une solution de téléphonie sur IP adaptée aux besoins de l'entreprise. Après une analyse de l'architecture du réseau existante et des limitations du système téléphonique en place, une solution basée sur un serveur IPBX Asterisk a été proposée et déployée. La nouvelles infrastructure intègre des services avancés tels que la messagerie vocale, l'IVR, la musique d'attente et repose sur des mécanismes de sécurité tels que parfeu (pfSense), segmentation réseau (DMZ), VPN Tailscale pour les accès distants et une authentification stricte des utilisateurs. Le résultat final est un système VoIP fiable, sécurisé et adaptable, répondant aux exigences d'un environnement professionnel comme celui de l'EPB.
Mots clé : Téléphonie sur IP (ToIP), Asterisk, IPBX, VoIP, VPN Tailscale, DMZ,EPB.

Abstract

Information transmission and communication occupy a central place in modern infrastructures today. Among the most prominent technologies is Telephony over IP (ToIP), which allows voice transmission in the form of data packets across IP networks. It is gaining ground thanks to its numerous advantages in terms of integration, reliability, scalability, and cost reduction.

This thesis is part of a project carried out within the Béjaïa Port Company (EPB) and aims to design and secure an IP telephony solution tailored to the company's needs. After analyzing the existing network architecture and the limitations of the existing telephone system, a solution based on an Asterisk IPBX server was proposed and deployed. The new infrastructure integrates advanced services such as voicemail, IVR, and music on hold, and relies on security mechanisms such as firewall (pfSense), network segmentation (DMZ), Tailscale VPN for remote access, and strict user authentication. The end result is a reliable, secure, and adaptable VoIP system that meets the requirements of a professional environment such as that of the EPB.
Keywords : Telephony over IP (ToIP), Asterisk, IPBX, VoIP, Tailscale VPN, DMZ,EPB.