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

Faculté des Sciences Exactes
Département Informatique

Mémoire De Fin De Cycle

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

Thème

Etude et Mise en Place D'une Solution VoIP Sécurisée

Cas d'etude : Entreprise Portuaire de Béjaïa

Réalisé par :

M. ADNANE Nasser
M. MERSEL Nabyl

Devant le jury composé de :

Président : *M*. AISSANI Sofiane
Examinatrice : M^{me}. BACHIRI Lina
Examinateur : *M*. KHEMMARI Mohamed
Encadreur : M^{me}. LARBI Wahiba
Co-encadreur : *M*. LARBI Ali

Promotion 2016-2017

Nous remercions tout d'abords, dieu le tout puissant de nous avoir accordé la force, la volonté et la connaissance pour accomplir ce travail ;

Nous tenons à remercier notre promotrice madame Larbi Wahiba et co-promoteur monsieur Larbi Ali, pour leurs précieux conseils et orientations ;

Nos remerciements vont à monsieur Aissani Sofiane de nous avoir fait l'honneur de présider le jury, et à madame Bachiri Lina et monsieur Khemmari Mohamed qui nous ont honoré en acceptant d'assister et examiner notre travail.

Nous tenons à remercier l'ensemble du personnel de la direction des systèmes d'informations de l'entreprise Portuaire de Béjaïa en particulier notre encadreur monsieur Touati Badreddine qui nous a apporté son aide tout au long de notre stage ;

Nos remerciements vont également à tous les enseignants qui nous ont aidé tout au long de notre travail pour l'esprit de coopération et la courtoisie dont ils ont fait preuve à notre égard ;

Comme nous remercions toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce modeste travail.

Dédicace

Je dédie ce modeste travail :

A mes très chers parents qui ont toujours été là pour moi et qui m'ont donné un magnifique modèle de courage, de labeur et persévérance...

A mes chères sœurs...

A mes grands-parents...

A mes oncles et tantes...

A mes cousins et cousines...

A mon binôme...

A vous mes amis et tous ceux qui m'estiment et qui me sont chers...

ADNANE Nasser

Dédicace

Je tiens vivement, à dédier ce modeste travail :

A ceux qui m'ont tout donné sans rien en retour ;
A ceux qui m'ont encouragé et soutenu dans les moments les plus difficiles et ceux à qui je dois tant ;

A la mémoire de mon cher père ;
A ma mère qui a éclairé mon chemin et encouragé, pour son amour et son soutient continu tout au long de mes etudes, que dieu tout puissant me la garde, et lui procure santé ,bonheur et longue vie ;

A mes sœurs : Ouarda , Imene ;

A Tous les membres de ma famille ;

A mon binôme ;

A tous mes amis sans exception ;

MERSEL Nabyl

Table des matières

Table des figures

Abréviation

CNAN : Compagnie Nationale Algérienne de Navigation
CODEC : Codeur Décodeur
CLI : Command Line Interface
DoS : Deny of Service
DR : Direction Remorquage
DSI : Direction des systems d'informations
EPB : Entreprise Portuaire de Béjaïa
GSM : Global System for Mobile Communications
HTTP : HyperText Transfer Protocol
IAX : Inter-Asterisk eXchange
ID : Identificateur
IETF : Internet Engineering Task Force Protocol
IP : Internet Protocol
IPBX : Internet Private Branch eXchange
ISDN : Integrated Service Data Network
ITU : International Telecommunications Union
IVR : Interactive Voice Response
LAN : Local Area Network
MC : Multipoint Control
MCU : Multipoint Control Units
MGCP : Media Gateway Control Protocol
MIKEY : Multimedia Internet KEYing
MP : Processeurs Multipoints
ONP : Office National des Ports
PABX : Private Automatic Branch eXchange
PC : Portable Computer
PSTN : Public Switched Telephone Network
QoS : Quality of Service
RAS : Registration/Admission/Status
RNIS : Réseau Numérique à Intégration de Service
RSVP : Ressource reservation Protocol
RTC : Réseau Téléphonique de Commuté
RTCP : Real-time Transport Control Protocol

RTP : Real-Time Transport Protocol
SIP : Session Initiation Protocol
SNM : Société Nationale de Manutention
SO.NA.MA : Société Nationale de Manutention
SRTP : Secure Real-time Transport Protocol
SVN : Subversion
TCP : Transport Control Protocol
TDM : Time Division Multiplexing
TLS : Transport Layer Security
ToIP : Telephony over Internet Protocol
UAC : User Agent Client
UAS : User Agent Server
UDP : User Datagram Protocol
URI : Uniform Resource Identifier
URL : Uniform Resource Locator
VoIP : Voice over Internet Protocol
VOMIT : Voice Over Misconfigured Internet Telephones
VPN : Virtual Private Network
WAN : World Area Network

Introduction générale

Le développement d'Internet a modifié profondément la façon d'utiliser notre téléphone. En effet, la technologie de la téléphonie classique est aujourd'hui en passe d'être supplantée par la téléphonie sur IP (Internet Protocol). La migration des entreprises vers ce genre de technologie à pour but principal de : minimiser le coût des communications ; utiliser le même réseau pour offrir des services de données, de voix, et d'images ; et réduire les coûts de configuration et d'assistance.

Similaire au téléphone, la voix sur IP (VoIP : Voice over Internet Protocol) permet de transmettre la voix en se référant au protocole IP et cela permet d'effectuer des appels téléphoniques via Internet.

L'intégration progressive de la VoIP, en ajoutant des cartes extensions IP, facilite l'adoption du téléphone IP dans les grandes sociétés possédant une plateforme classique et voulant bénéficier de la voix sur IP.

Le développement des PABXs (Private Automatic Branch eXchange) software représente la solution proposée par des fournisseurs tels que Cisco et Asterisk. Cette approche permet de bénéficier d'une grande flexibilité, d'une très bonne intégration au monde des données et de voix, et surtout d'un prix beaucoup plus intéressant.

Comme cette solution est basée sur la technologie IP, elle est toutefois affectée par les vulnérabilités qui menacent la sécurité de protocole et l'infrastructure réseau sur laquelle elle est déployée. Cette dernière est le majeur problème pour les entreprises et un grand défi pour les développeurs. Certaines attaques sur les réseaux VoIP, comme les attaques de déni de service, et les vols d'identité, peuvent causer des pertes catastrophiques et énormes pour les entreprises.

Pour cela, la sécurité de la VoIP, n'est pas seulement une nécessité mais plutôt une obligation, avec laquelle nous pouvons réduire, au maximum, le risque d'attaques sur

la VoIP. De ce fait, une solution VoIP doit couvrir toute l'infrastructure du réseau déployé, tel que les outils et les équipements de gestion des communications et des utilisateurs, le système d'exploitation sur lesquels sont installés ces outils, et les protocoles de signalisation et de transport de données.

Le travail que nous avons effectué a pour objectif de faire une étude sur les protocoles de la VoIP ; une étude de l'existant de l'entreprise portuaire de Béjaïa afin de mettre en place une solution de VoIP, basée sur le serveur Asetrisk et le client X-Lite. Pour finir, nous avons fait une étude des vulnérabilités et des attaques sur la VoIP, ainsi que les configurations utilisées pour sécuriser cette dernière.

Ce mémoire se compose de quatre chapitres, Le premier défini la voix sur IP et ses éléments, décrit et explique son architecture et ses protocoles, et énumère les majeurs points forts de cette technologie ainsi que ses faiblesses.

Le deuxième chapitre, consiste à faire une présentation de l'EPB (Entreprise Portuaire de Béjaïa), sa structure, ses projets, ses missions, ses activités, ... etc. En mettant un accent particulier sur son réseau informatique, tout en procédons à l'analyse des conditions permettant l'implémentation de la VoIP.

Le troisième chapitre, consiste à la mise en place d'une solution de VoIP pour les entreprises basée sur le serveur Asterisk et le client X-Lite. Mais également la mise en place d'un IVR (Interactive Voice Response) incluant notre base de données.

Le dernier chapitre du mémoire, s'intéresse aux tests et à la réalisation de quelques attaques sur l'infrastructure de VoIP déployée. Une implémentation des différentes solutions et mesures nécessaires à la protection contre ces attaques est réalisée.

Chapitre 1

Etude générale de la voix sur IP

Introduction

La voix sur IP (Internet Protocol) constitue actuellement une évolution très importante dans le domaine des Télécommunications. Avant 1970, la transmission de la voix s'effectuait de façon analogique sur des réseaux dédiés à la téléphonie, la technologie utilisée était la technologie électromécanique (Crossbar). Dans les années 80, une premiére évolution a été le passage à la transmission numérique TDM (Time Division Multiplexing). La transmission de la voix sur les réseaux informatiques à commutation de paquets IP constitue aujourd'hui une évolution majeure comparable aux précédentes.

L'objectif de ce chapitre est l'étude de cette technologie et de ses différents aspects. Nous parlerons en détail de l'architecture de la VoIP (Voice over Internet Protocol), ses éléments et son principe de fonctionnement. Nous détaillerons aussi des protocoles VoIP de signalisation et de transport ainsi que leurs principes de fonctionnement et de leurs principaux avantages et inconvénients.

1 Présentation de la voix sur IP

1.1 Définition

VoIP signifie Voice over Internet Protocol ou Voix sur IP. Comme son nom l'indique, la VoIP permet de transmettre du son (en particulier la voix) dans des paquets IP circulant sur Internet[1].

1.2 Architecture

Etant une nouvelle téchnologie de communication, la VoIP n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les trois principaux protocoles sont H.323, SIP (Session Initiation Protocol) et MGCP/MEGACO. Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP.

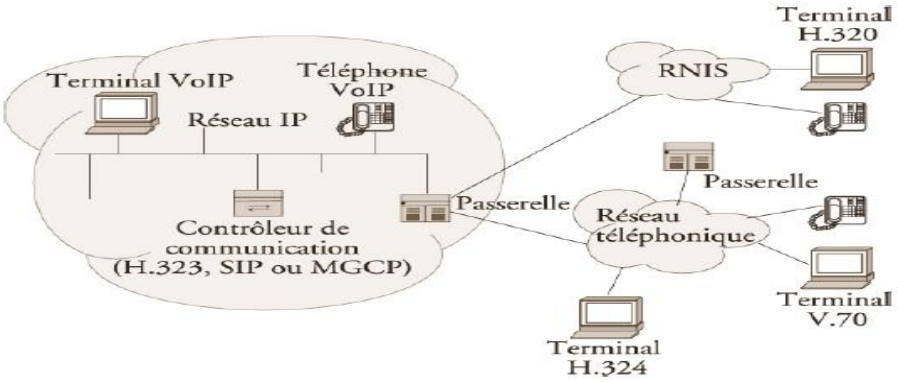

FIGURE 1.1 – Architecture générale de la voix sur IP[1].

La figure 1.1 décrit, de façon générale, la topologie d'un réseau de téléphonie IP. Elle comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques, pour garantir une plus ou moins grande qualité de service. Le réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/contrôleur de commutation, appelées Gatekeeper. Nous retrouvons les éléments communs suivants :

- **Le routeur :** Permet d'aiguiller les données et de router les paquets entre deux réseaux. Certains routeurs permettent de simuler un Gatekeeper, grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP.
- **La passerelle :** Permet d'interfacer le réseau commuté et le réseau IP.
- **Le PABX :** Est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur, et le RTC (Réseau Téléphonique Commuté). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.
- **Les Terminaux :** Sont généralement de type logiciel (software phone) ou matériel (hardphone), le softphone est installé dans le PC de l'utilisateur. L'interface audio peut être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé.

• **Le hardphone :** est un téléphone IP qui utilise la technologie de la Voix sur IP, pour permettre des appels téléphoniques sur un réseau IP, tel que l'Internet, au lieu de l'ordinaire système PSTN (Public Switched Telephone Network). Les appels peuvent parcourir par le réseau internet comme par un réseau privé. Un terminal utilise des protocoles comme le SIP ou l'un des protocoles propriétaires tel que celui utilisée par Skype[1].

1.3 Principe de fonctionnement

Depuis de nombreuses années, il était possible de transmettre un signal à une destination éloignée sous forme de données numériques. Avant la transmission, il faut numériser le signal à l'aide d'un CODEC (Codeur Décodeur), le signal est ensuite transmis. Pour être utilisable, il doit être transformé de nouveau en un signal analogique.

La VoIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format de meilleure qualité. Le signal numérique est plus tolérant au bruit que l'analogique.

Les réseaux TCP/IP sont des supports de circulation de paquets IP, contenant un en-tête (pour contrôler la communication) et une charge utile, pour transporter les données. Il existe plusieurs protocoles qui peuvent supporter la voix sur IP tel que : H.323, SIP et MGCP.

Les deux protocoles les plus utilisés actuellement dans les solutions VoIP présents sur le marché sont le H.323 et le SIP[2].

2 Protocole H.323

2.1 Description générale du protocole H.323

Le standard H.323, fournit depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Télécommunications Union) pour les réseaux qui ne garantissent pas une QoS (Quality of service), tels que FastEthernet et Token Ring. Il est présent dans plus de 30 produits. H.323 concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. Il traite également de l'interfaçage entre le LAN(Local Area Network) et les autres réseaux.

Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclue H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switched Telephone Network).

Plus qu'un protocole, H.323 crée une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

• Les messages de signalisation sont ceux envoyés pour demander la mise en relation de deux clients, qui indique que la ligne est occupée ou que le téléphone sonne, etc. Avec H.323, la signalisation s'appuie sur le protocole RAS (Registration/Admission/Status) pour l'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel.

• La négociation est utilisée pour se mettre d'accord sur la façon de coder les informations à échanger. Il est important que les téléphones (ou systèmes) utilisent un langage commun s'ils veulent se comprendre. Il s'agit du codec le moins gourmand en bande passante ou de celui qui offre la meilleure qualité. Il serait aussi préférable d'avoir plusieurs alternatives de langages. Le protocole utilise pour la négociation de codec est le H.245.

• Le transport de l'information s'appuie sur le protocole RTP (Real-time Transport Protocol) qui transporte la voix, la vidéo ou les données numérisées par les codecs. Les messages RTCP (Real-time Transport Control Protocol) peuvent être utilisés pour le contrôle de la qualité, ou la renégociation des codecs si, par exemple, la bande passante diminue.

Une communication H.323 se déroule en cinq phases : l'établissement d'appel, l'échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource reservation Protocol), l'établissement de la communication audio-visuelle, l'invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.) et enfin la libération de l'appel[3].

2.2 Rôle des composants

La figure 1.2 représente l'infrastructure H.323 qui se repose sur quatre composants principaux : les terminaux, les Gateways, les Gatekeepers, et les MCU (Multipoint Control Units).

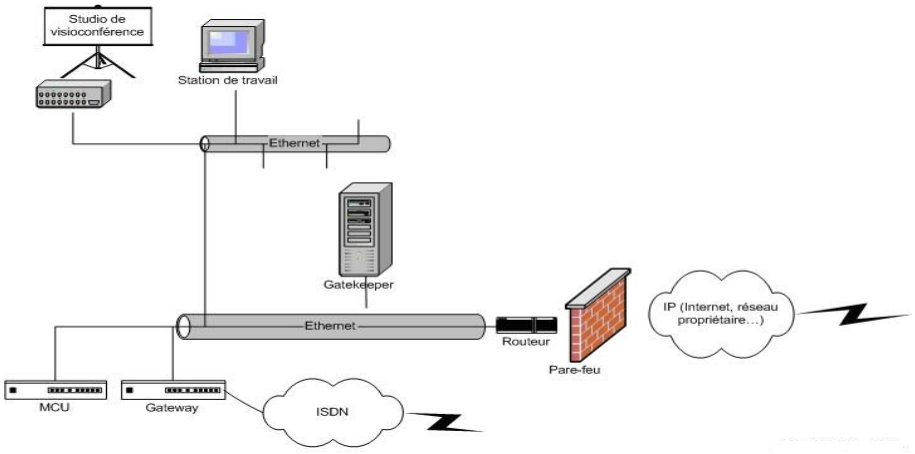

FIGURE 1.2 – Les composants de l'architecture H.323[3].

• **Les terminaux H.323 :** Le terminal peut être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet. Le minimum imposé par H.323 est qu'il mette en œuvre la norme de compression de la parole G.711, qu'il utilise le protocole H.245 pour la négociation de l'ouverture d'un canal et l'établissement des paramètres de la communication, ainsi que le protocole de signalisation Q.931 pour l'établissement et l'arrêt des communications. Le terminal possède également des fonctions optionnelles, notamment, pour le travail en groupe et le partage des documents. Il existe deux types de terminaux H.323, l'un de haute qualité (pour une utilisation sur LAN), l'autre optimisé pour de petites largeurs de bandes (28,8/33,6 kbit/s – G.723.1 et H.263).

• **Gateway ou les passerelles vers des réseaux classiques (RTC, RNIS, etc.) :** Les passerelles H.323 assurent l'interconnexion avec les autres réseaux, ex : les modems H.324, les téléphones classiques, etc. Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les medias (multiplexage, correspondance des débits, transcodage audio).

• **Gatekeeper ou les portiers :** Dans la norme H.323, Le Gatekeeper est le point d'entrée au réseau pour un client H.323. Il définit une zone sur le réseau, appelée zone H.323 (voir figure 1.3), regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dès l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe, obtenu auprès de son Gatekeeper de rattachement.

Le Gatekeeper a pour fonction :

1. La translation des alias H.323 vers des adresses IP, selon les spécifications RAS (Registration/Admission/Status).
2. Le contrôle d'accès, en interdisant les utilisateurs et les sessions non autorisés.
3. La gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées. Concrètement, une fraction de la bande passante est allouée à la visioconférence, pour ne pas gêner les applications critiques sur le LAN et le support des conférences multipoint adhoc.

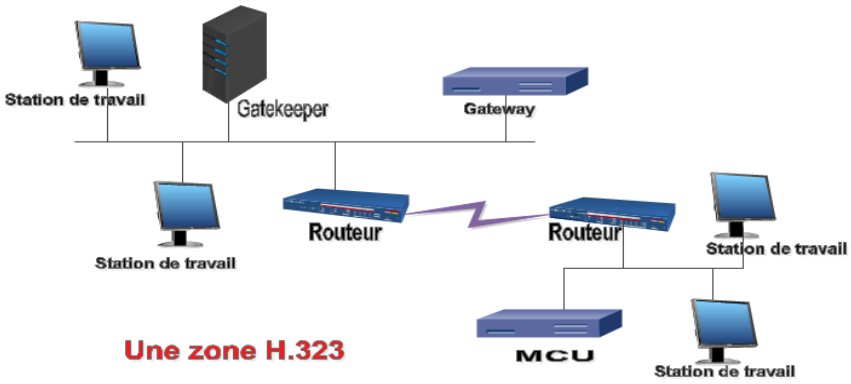

FIGURE 1.3 – La zone H.323.

• **Les MCU (Multipoint Control Unit) :** Les contrôleurs multipoint appelés MCU offrent aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints (MP). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées. Mais le MC ne traite pas directement avec les flux audio, vidéo ou données, c'est le MP qui se charge de récupérer les flux et de leurs faire subir les traitements nécessaires. Un MC peut contrôler plusieurs MP distribués sur le réseau et faisant partie d'autres MCU[3].

2.3 Avantages et inconvénients de la technologie H.323

La technologie H.323 possède des avantages et des inconvénients [4]. Parmi les avantages, nous citons :

• **Gestion de la bande passante :** H.323 permet une bonne gestion de la bande passante en posant des limites au flux audio/vidéo afin d'assurer le bon fonctionnement

des applications critiques sur le LAN. Chaque terminal H.323 peut procéder a l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue).

• **Support Multipoint :** H.323 permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.

• **Support Multicast :** H.323 permet également de faire des transmissions en multicast.

• **Interopérabilité :** H.323 permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications, les paramètres (les codecs, le débit...) sont négociés de manière transparente.

• **Flexibilité :** une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones. . .) qui peuvent partager selon le cas, de la voix de la vidéo et même des données.

Les inconvénients de la technologie H.323 sont :

• La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse.

• Comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité.

3 Protocole SIP

3.1 Description générale du protocole SIP

Le protocole SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF (Internet Engineering Task Force) qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants, en encapsulant des messages SDP (Session Description Protocol). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange. Cependant le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audio et vidéo. SIP remplace progressivement H323.

SIP est le standard ouvert de VoIP, interopérable, le plus étendu et vise à devenir le standard des télécommunications multimédia (son, image, etc.). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas seulement destiné à la VoIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo[3].

3.2 Caractéristique du protocole SIP

Pour l'établissement de la session, notre choix est porté sur le protocole SIP. De ce fait, une explication approfondie de ses différents aspects et caractéristiques est nécessaire. Ses principales caractéristiques sont[18] :

• **Fixation d'un compte SIP :** Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique. Par exemple, si un utilisateur d'un service de voix sur IP dispose d'un compte SIP et que chaque fois qu'il redémarre son ordinateur, son adresse IP change, il doit cependant toujours être joignable. Son compte SIP doit donc être associé à un serveur SIP (proxy SIP) dont l'adresse IP est fixe. Ce serveur lui allouera un compte et il permettra d'effectuer ou de recevoir des appels quelques soit son emplacement. Ce compte sera identifiable via son nom (ou pseudo).

• **Changement des caractéristiques durant une session :** Un utilisateur doit pouvoir modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en (voix uniquement) peut être modifié en (voix + vidéo).

• **Différents modes de communication :** Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci.

- **Mode Point à point :** Il s'agit d'un «unicast », qui correspond à la communication entre deux machines.
- **Mode diffusif :** Il s'agit d'un « multicast », qui correspond à la communication entre plusieurs utilisateurs via une unité de contrôle MCU.
- **Combinatoire :** combine les deux modes précédents. Plusieurs utilisateurs interconnectés en multicast via un réseau à maillage complet de connexion.

Gestion des participants : Durant une session d'appel, de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement, en étant

transférés ou en étant mis en attente (cette particularité rejoint les fonctionnalités d'un PABX par exemple, où l'appelant peut être transféré vers un numéro donné ou être mis en attente).

Négociation des médias supportés : Cela permet à un groupe durant un appel de négocier sur les types de médias supportés. Par exemple, la vidéo peut être ou ne pas être supportée lors d'une session.

Adressage : Les utilisateurs disposant d'un numéro (compte) SIP, disposent d'une adresse ressemblant à une adresse mail (sip :numéro@serveursip.com). Le numéro SIP est unique pour chaque utilisateur.

Modèle d'échange : Le protocole SIP repose sur un modèle Requête/Réponse. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La liste des requêtes échangées est la suivante :

- **Invite :** Cette requête indique que l'application (ou utilisateur) correspondante à l'url SIP spécifié est invité à participer à une session. Le corps du message décrit cette session (par ex : média supportés par l'appelant). En cas de réponse favorable, l'invité doit spécifier les médias qu'il supporte.
- **Ack :** Cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête invite.
- **Options :** Un proxy server en mesure de contacter L'UAS (User Agent Server) appelé, doit répondre à une requête « Options » en précisant ses capacités à contacter le même terminal.
- **Bye :** Cette requête est utilisée par le terminal de l'appelé à fin de signaler qu'il souhaite mettre un terme à la session.
- **Cancel :** Cette requête est envoyée par un terminal ou un proxy server à fin d'annuler une requête non validée par une réponse finale comme, par exemple, si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête Ack, alors elle émet une requête Cancel.
- **Register :** Cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL TO par le serveur auquel il est relié.

Codes d'erreurs : Une réponse à une requête est caractérisée, par un code et un motif, appelés respectivement code d'état et raison phrase. Un code d'état est un entier codé sur 3 digits indiquant un résultat à l'issue de la réception d'une requête. Ce résultat est précisé

par une phrase, textbased (UTF-8), expliquant le motif du refus ou de l'acceptation de la requête. Le code d'état est donc destiné à l'automate gérant l'établissement des sessions SIP et les motifs aux programmeurs. Il existe 6 classes de réponses et donc de codes d'état, représentées par le premier digit :

- **1xx** = Information - La requête a été reçue et continue à être traitée.
- **2xx** = Succès - L'action a été reçue avec succès, comprise et acceptée.
- **3xx** = Redirection - Une autre action doit être menée afin de valider la requête.
- **4xx** = Erreur du client - La requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur.
- **5xx** = Erreur du serveur - Le serveur n'a pas réussi à traiter une requête apparemment correcte.
- **6xx** = Echec général - La requête ne peut être traitée par aucun serveur.

3.3 Rôle des composants

Dans un système SIP, il existe deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy).

L'UAS (User Agent Server) : Représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue, elle renvoie une réponse au nom de l'utilisateur.

L'U.A.C (User Agent Client) : Représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes.

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 1.4).

Les URI SIP : Sont très similaires dans leur forme à des adresses email sip :utilisateur@domaine.com. Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI.

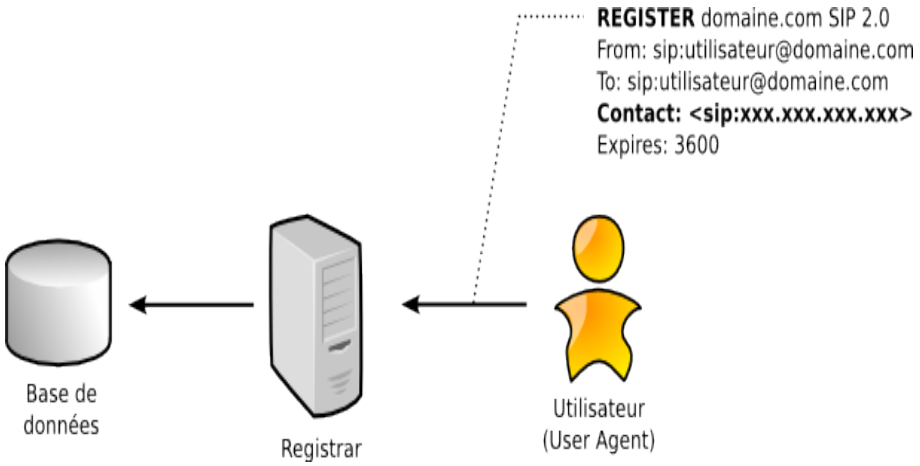

FIGURE 1.4 – Enregistrement d'un utilisateur[5].

Un Proxy SIP sert d'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 1.5 montre les étapes de l'interrogation du proxy la base de données.

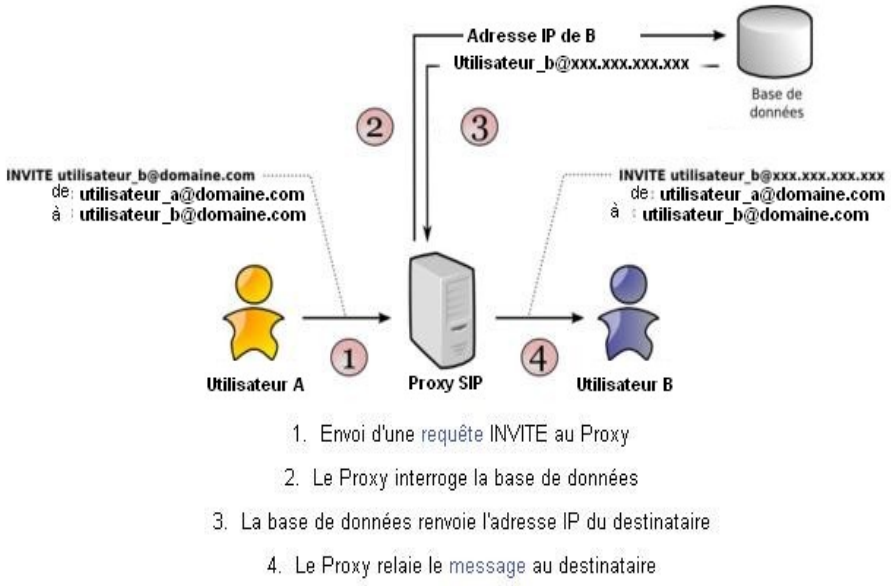

FIGURE 1.5 – Principe du protocole SIP[5].

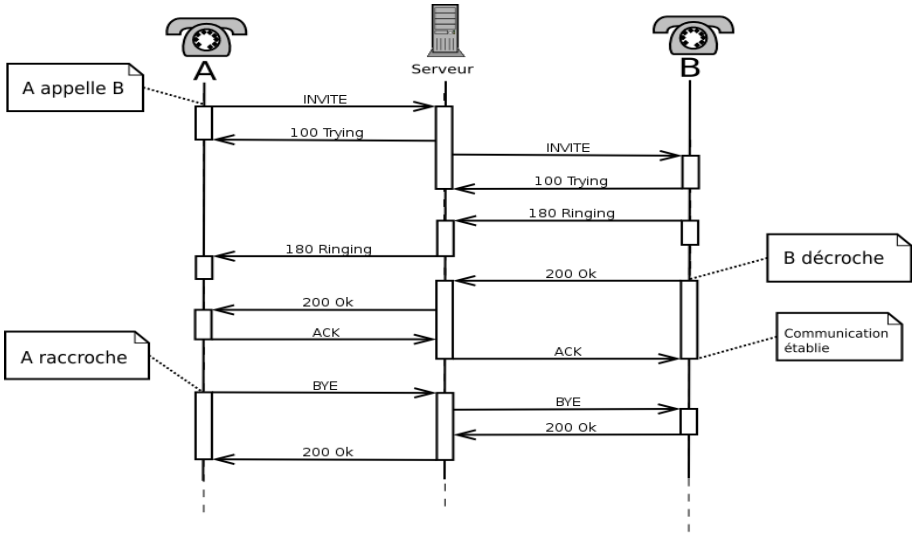

FIGURE 1.6 – Session SIP à travers un proxy[6].

Le Proxy se contente de relayer uniquement les messages SIP pour établir, contrôler et terminer la session (voir figure 1.6). Une fois la session établie, les données, par exemple un flux RTP pour la VoIP, ne transitent pas par le serveur Proxy. Elles sont échangées directement entre les User Agents.

3.4 Avantages et inconvénients

Les principaux avantages du protocole SIP [5][6] sont :

- **Ouvert :** Les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- **Standard :** L'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.
- **Simple :** SIP est simple et très similaire à http.
- **Flexible :** SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).
- **Téléphonie sur réseaux publics :** Il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.
- **Points communs avec H323 :** L'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur

le réseau. Un autre inconvénient est le faible nombre d'utilisateurs ; en effet SIP est encore peu connu et peu utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau.

4 Protocoles de transport

Nous décrivons deux autres protocoles de transport utilisés dans la voix sur IP, à savoir RTP et le RTCP [7].

4.1 Le protocole RTP

4.1.1 Description générale de RTP

RTP (Real time Transport Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF, afin de faciliter le transport temps réel de bout en bout, des flots donnés audio et vidéo, sur les réseaux IP. RTP est un protocole qui se situe au niveau de l'application et qui utilise les protocoles sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP, ce qui permet d'atteindre plus facilement le temps réel. Les applications en temps réels, comme la parole numérique ou la visioconférence constitue un véritable problème pour Internet. Une application en temps réel, exige une certaine qualité de service (QoS) que RTP ne garantie pas du fait qu'il fonctionne au niveau Applicatif.

De plus RTP est un protocole qui se trouve dans un environnement multipoint, donc on peut dire que RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint.

4.1.2 Les fonctions de RTP

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. Ceci de façon à reformer les flux avec ses caractéristiques de départ. RTP est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. Il est aussi un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de[19] :

•Mettre en place un séquencement des paquets par une numérotation et ce afin de permettre ainsi la détection des paquets perdus. Ceci est un point primordial dans la reconstitution des données. Mais il faut savoir quand même que la perte d'un paquet n'est pas un gros problème si les paquets ne sont pas perdus en trop grands nombres.

Cependant il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte.

•Identifier le contenu des données pour leurs associer un transport sécurisé et reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur).

• L'identification de la source c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast l'identité de la source doit être connue et déterminée.

• Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation). Ces trames sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement.

4.1.3 Avantages et inconvénients

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

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

4.2 Le protocole RTCP

4.2.1 Description générale de RTCP

Le protocole RTCP (Real-time Transport Control Protocol) est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP.

Le protocole RTP utilise le protocole RTCP, qui transporte les informations supplémentaires suivantes pour la gestion de la session.

Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS. Ces rapports comprennent le nombre de paquets perdus, le paramètre indiquant la variance d'une distribution (plus communément appelé la gigue : c'est à dire les paquets qui arrivent

régulièrement ou irrégulièrement) et le délai aller-retour. Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS.

Parmi les principales fonctions qu'offre le protocole RTCP, nous citons :

- **Une synchronisation supplémentaire entre les médias :** Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérées et suivre des chemins différents.

- **L'identification des participants à une session :** En effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.

- **Le contrôle de la session :** En effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

- **SR (Sender Report) :** Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (gigue), etc.). Ces rapports sont issus d'émetteurs actifs d'une session.

- **RR (Receiver Report) :** Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.

- **SDES (Source Description) :** Carte de visite de la source (nom, e-mail, localisation).

- **BYE :** Message de fin de participation à une session.

- **APP :** Fonctions spécifique à une application.

4.2.2 Avantage et inconvénient du protocole RTCP

Le protocole de RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanant sur une session et ces participants. Par contre il fonctionne en stratégie bout à bout. Et il ne peut pas contrôler l'élément principal de la communication "le réseau ".

5 Points forts et limites de la voix sur IP

Différentes raisons peuvent pousser les entreprises à s'orienter vers la VoIP comme solution pour la téléphonie. Les avantages les plus marqués sont [2] :

• **Réduction des coûts :** En effet le trafic véhiculé à travers le réseau RTC est plus couteux que sur un réseau IP. Réductions importantes pour des communications internationales en utilisant le VoIP, ces réductions deviennent encore plus intéressantes dans la mutualisation voix/données du réseau IP intersites (WAN). Dans ce dernier cas, le gain est directement proportionnel au nombre de sites distants.

• **Standards ouverts :** La VoIP n'est plus uniquement H323, mais un usage multi-protocoles selon les besoins de services nécessaires. Par exemple, H323 fonctionne en mode égale à égale alors que MGCP fonctionne en mode centralisé. Ces différences de conception offrent immédiatement une différence dans l'exploitation des terminaisons considérées.

• **Un réseau voix, vidéo et données (à la fois) :** Grâce à l'intégration de la voix comme une application supplémentaire dans un réseau IP, ce dernier va simplifier la gestion des trois applications (voix, réseau et vidéo) par un seul transport IP. Une simplification de gestion, mais également une mutualisation des efforts financiers vers un seul outil.

Les points faibles de la voix sur IP sont :

• **Fiabilité et qualité sonore :** Un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels la qualité de la reproduction de la voix du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques. De plus, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert) sans être en mesure de savoir si des paquets ont été perdus et à quel moment.

• **Vol :** Les attaquants qui parviennent à accéder à un serveur VoIP peuvent également accéder aux messages vocaux stockés et au même au service téléphonique pour écouter des conversations ou effectuer des appels gratuits aux noms d'autres comptes.

- **Attaque de virus :** Si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système.

Conclusion

La VoIP représente la solution la plus rentable pour effectuer des conversations. Ce qui rend son évolution évidente.

La téléphonie IP est une bonne solution en matière d'intégration, fiabilité et de coût. La voix sur IP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. Chaque standard possède ses propres caractéristiques pour garantir une bonne qualité de service. En effet, le respect des contraintes temporelles est le facteur le plus important lors de transport de la voix.

Malgré que la normalisation n'a pas atteint la maturité suffisante pour sa généralisation au niveau des réseaux IP, il n'est pas dangereux de miser sur ces standards vu qu'ils ont été acceptés par l'ensemble des professionnels de la téléphonie sur IP.

Dans le chapitre qui suit, nous procèderons à la présentation de l'organisme d'accueil.

Chapitre 2

Etude de l'éxistant

Introduction

L'opportunité de migrer de la téléphonie classique vers la téléphonie IP, a offert plusieurs avantages pour les entreprises, et leurs a permis de bénéficier de nouveaux services, tels que la vidéoconférence et la transmission des données.

Dans ce chapitre, nous allons commencer par la présentation de l'EPB (Entreprise Portuaire de Bejaïa), et procéderons à l'analyse des conditions permettant l'implémentation de la VoIP.

1 Présentation de l'organisme d'accueil

Le port de Bejaia joue un rôle très important dans les transactions internationale vu sa place et sa position géographique. Aujourd'hui, il est classé 2ème port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié ISO 9001.2000 pour l'ensemble de ses prestations, et à avoir ainsi installé un système de management de la qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail [15].

FIGURE 2.1 – Port de Bejaïa[15].

1.1 Histoire de la ville et du port

Au cœur de l'espace méditerranéen, la ville de Bejaïa possède de nombreux sites naturels et vestiges historiques, datant de plus de 10 000 ans, ainsi qu'une multitude de sites archéologiques, recelant des trésors anciens remontant à l'époque du néolithique.

Bejaïa joua un grand rôle dans le bassin méditerranéen. Grâce au dynamisme de son port, la sécurité de la région, la bonne politique et les avantages douaniers, Bougie a su attirer beaucoup de puissants marchands.

Dans l'antiquité, Amsyouen, habitants des flans surplombant la côte, ne fréquentaient la côte que pour pêcher. Les premières nefs qui visitèrent les abris naturels furent phéniciennes, ils y installèrent des comptoirs.

La Saldae romaine leur succéda, et devint port d'embarquement de blé. Ce n'est qu'au 11ème siècle que la berbère Begaïeth, devenue Ennaciria, prit une place très importante dans le monde à l'époque. Le port de Béjaïa devint l'un des plus importants de la Méditerranée, ses échanges étaient très denses. L'histoire retiendra également à cette époque, que par Fibonacci de Pise, fils d'un négociant pisan, s'étendirent dans le monde à partir de Béjaïa, les chiffres aujourd'hui universellement utilisés.

La réalisation des ouvrages actuels du port débuta en 1834, elle fût achevée en 1987. C'est en 1960 que fût chargé le 1er pétrolier au port d'Algérie.

Le port de Bejaïa aujourd'hui est réputé mixte ; hydrocarbures et marchandises générales y sont traitées. L'aménagement moderne des superstructures, le développement des infrastructures, l'utilisation de moyens de manutention et de techniques adaptés à l'évolution

de la technologie des navires et enfin ses outils de gestion moderne, ont fait évoluer le Port de Bejaïa depuis le milieu des années 1990 pour être classé aujourd'hui second port d'Algérie[15].

1.2 Historique de l'EPB

Le décret n° 82-285 du 14 Août 1982 publié dans le journal officiel n° 33 porta création de l'Entreprise Portuaire de Bejaïa ; entreprise socialiste à caractère économique ; conformément aux principes de la charte de l'organisation des entreprises, aux dispositions de l'ordonnance n° 71-74 du 16 Novembre 1971 relative à la gestion socialiste des entreprises et les textes pris pour son application à l'endroit des ports maritimes.

L'entreprise, réputée commerçante dans ses relations avec les tiers, fut régie par la législation en vigueur et soumise aux règles édictées par le sus mentionné décret. Pour accomplir ses missions, l'entreprise est substituée à l'Office National des Ports (ONP), à la Société Nationale de Manutention (SO.NA.MA) et pour partie à la Compagnie Nationale Algérienne de Navigation (CNAN). Elle fut dotée par l'Etat, du patrimoine, des activités, des structures et des moyens détenus par l'ONP, la SO.NA.MA et de l'activité Remorquage, précédemment dévolue à la CNAN, ainsi que des personnels liés à la gestion et aux fonctionnements de celles-ci.

En exécution des lois n° 88.01,n° 88.03 et n° 88.04 du 02 Janvier 1988 s'inscrivant dans le cadre des réformes économiques et portant sur l'autonomie des entreprises, et suivant les prescriptions des décrets n° 88.101 du 16 Mai 1988, n° 88.199 du 21 Juin 1988 et n° 88.177 du 28 Septembre 1988, l'Entreprise Portuaire de Bejaïa ; entreprise socialiste ; est transformée en Entreprise Publique Economique, Société par Actions (EPE-SPA) depuis le 15 Février 1989, son capital social fut fixé à Dix millions (10.000.000) de dinars algérien, actuellement, il a était augmenté à 3.500.000.000 de DA.

1.3 Situation Géographique

Le port est situé dans la baie de la ville de Bejaïa, le domaine public artificiel maritime et portuaire est délimité suite à l'arrêté n° 93/1015/DRAG, de Monsieur le Wali de Bejaïa, ainsi :

- Au nord par la route nationale n° 9.
- Au sud par les jetées de fermeture et du large sur une longueur de 2.750 m.
- A l'est par la jetée Est.
- A l'ouest par la zone industrielle de Béjaïa.

1.4 Vision, missions, valeurs et activités de l'EPB

- **Vision**

  - Piloter le développement du port en augmentant le trafic et les parts de marché.
  - Offrir des installations compétitives, sécuritaires et de classe mondiale.
  - Satisfaire pleinement les besoins et les attentes des clients.
  - Garantir la fiabilité des services pour contribuer à la compétitivité des clients.

- **Missions**

  - Promouvoir le développement économique et être un outil de facilitation des échanges internationaux.
  - Contribuer de façon marquante à la prospérité de la ville.
  - Garantir l'efficacité, l'efficience, la transparence et la facilité opérationnelle des procédures, ce doit être un port facile pour les opérateurs de l'hinterland.
  - Motiver et valoriser les salariés et prendre des engagements envers eux, car ils sont le principal atout.

- **Valeurs**

  - Valorisation et engagement des potentiels.
  - Gestion éthique et professionnelle.
  - Orientation et efficience vers le client.
  - Responsabilité sociale et environnementale (RSE).

- **Activités**

Les principales activités de l'entreprise sont :

  - L'exploitation de l'outillage et des installations portuaires.
  - L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.
  - L'exercice du monopole des opérations d'acconage et de manutention portuaire.
  - L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.
  - La police et la sécurité portuaire dans la limite géographique du domaine public portuaire.

1.5 Projets de l'EPB

a) Schéma directeur de développement du port

Le schéma de développement à long terme qu'a inscrit le port de Bejaïa permettra sans doute de renforcer les capacités commerciales du port et améliorer ses perfor-

mances logistiques, d'autant plus que la nouvelle pénétrante reliera directement le port à l'autoroute Est Ouest.

L'aboutissement de ce schéma directeur de développement permettra de réinventer le port de Bejaïa et d'accroitre son efficacité dans la chaîne logistique de transport, il contribuera ainsi à la compétitivité de ses clients en fournissant des services efficaces couvrant leurs besoins en transport maritime, transport terrestre et services logistiques.

FIGURE 2.2 – Schéma directeur de développement du port[15].

b) Réalisation d'une nouvelle gare maritime

Le port de Bejaïa a inscrit, dans son programme d'investissement, l'opération de réalisation d'une nouvelle gare maritime répondant aux normes internationales. Cette nouvelle infrastructure va inévitablement améliorer les conditions d'escales et d'accueil des passagers et le transit de leurs véhicules.

Le projet, dont les travaux de réalisation ont été confiés à BATIMETAL, sera réalisé sur deux sites qui seront liés par deux passerelles :

- Le site 1 à l'extérieur du port sur 8 159,31 m2.
- Le site 2 à l'intérieur du port sur 18 973,22 m2.

FIGURE 2.3 – Nouvelle gare maritime du port[15].

2 Organisation de l'EPB

2.1 Présentation des différentes structures de l'EPB

L'EPB est organisé selon des directions fonctionnelles et opérationnelles [15] :

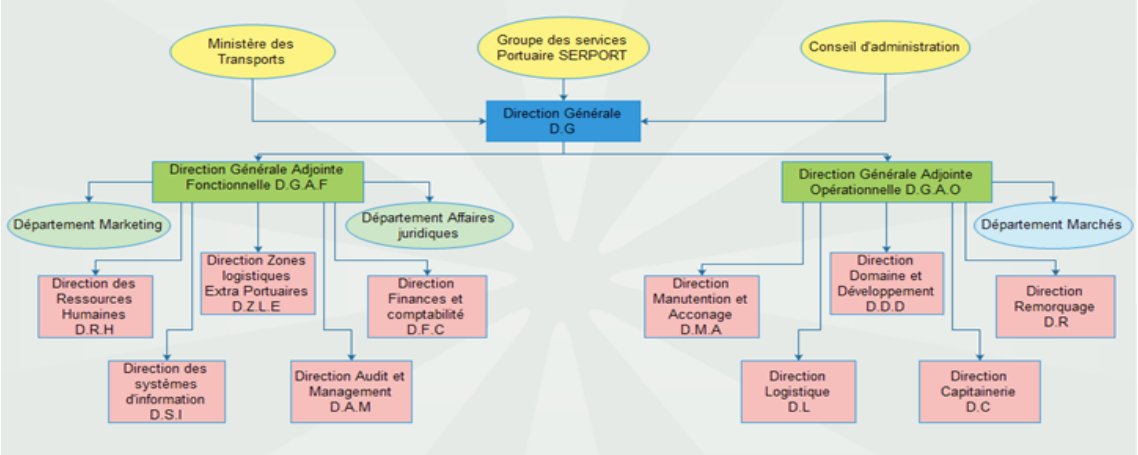

FIGURE 2.4 – Illustration de l'organigramme de l'EPB

2.1.1 Directions Générale Adjointe Opérationnelles (D.G.A.O)

a) Direction manutention et acconage (D.M.A) : Elle est chargée de prévoir, organiser, coordonner et contrôler l'ensemble des actions de manutention et d'acconage liées à l'exploitation du port.

b) Direction domaine et développement (D.D.D) : A pour tâches :

- Amodiation et location de terre pleins, hangar, bureaux, immeubles, installations et terrains à usage industriel ou commercial.
- Enlèvement des déchets des navires et assainissement des postes à quai.
- Pesage des marchandises (pont bascule).

c) Direction capitainerie (D.C) : : Elle est chargée de la sécurité portuaire, ainsi que de la bonne régulation des mouvements des navires, et la garantie de sauvegarde des ouvrages portuaires.

d) Direction remorquage (D.R) : Elle est chargée d'assister le pilote du navire lors de son entrée et de sa sortie du quai. Son activité consiste essentiellement à remorquer les navires entrants et sortants, ainsi que la maintenance des remorqueurs.

e) Direction logistique (D.L) : Elle consiste à gérer tout ce qui concerne le transport et le stockage des produits de l'entreprise : véhicules nécessaires au transport, fournisseurs de l'entreprise, entrepôts, manutention..., en optimisant leur circulation pour minimiser les coûts et les délais.

f) Département marchés : Les principaux rôles de département sont :
- Définir les besoins.
- Choisit la procédure de passation du marché.
- Choisit et hiérarchise les critères d'attribution du marché.
- Envoie l'avis de publicité.
- Signe et notifie le marché.

2.1.2 Directions Générale Adjointe Fonctionnelles (D.G.A.F)

Il s'agit des structures de soutien aux structures opérationnelles.

a) Direction générale (D.G) : Elle est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise.

b) Direction Audit et Management (D.M.I) : Elle est chargée de :
- La mise en œuvre, le maintien et l'amélioration continue du Système de Management Intégré (plans projets et indicateurs de mesure).
- L'animation et la coordination de toutes les activités dans le domaine HSE.
- La Contribution dans des actions de sensibilisation et de formation à la prévention des risques de pollution, à la protection de l'environnement, la santé des travailleurs et à l'intervention d'urgence.

c) Direction Finances et Comptabilité (D.F.C) : Elle est chargée de :
- La tenue de la comptabilité.
- La gestion de la trésorerie (dépenses, recettes et placements).
- La tenue des inventaires.
- Le contrôle de gestion (comptabilité analytique et contrôle budgétaire).

d) Direction Ressources Humaines (D.R.H) : Elle est chargée de prévoir, d'organiser et d'exécuter toutes les actions liées à la gestion des ressources humaines en veillant à l'application rigoureuse des lois et règlement sociaux. Elle assure les tâches suivantes :
- La mise en œuvre de la politique de rémunération, de recrutement et de la formation du personnel.

- La gestion des carrières du personnel (fichier).
- La gestion des moyens généraux (achats courants, parc automobile, assurances, ...etc.).

e) Direction des Systèmes d'Information (D.S.I) : Gère l'ensemble des systèmes d'information et de télécommunication de l'administration.

f) Direction Zones Logistiques Extra Portuaire (D.Z.L.E) : Il a pour objet de gérer les flux physiques, informationnels et financiers d'une organisation, dans le but de mettre à disposition les ressources correspondant aux besoins, et ce, aux conditions économiques et pour une qualité de service déterminées, dans des conditions de sécurité et de sûreté satisfaisantes.

g) Département Affaires Juridiques : Elle assure pour l'ensemble de l'institut une mission de conseil, d'expertise, de veille juridique ainsi que la défense de ses intérêts devant les juridictions.

h) Département marketing : Elle est chargée d'élaborer et de valider la stratégie commerciale, et de superviser et veiller à l'application des plans d'action à long et court terme de l'entreprise. Elle est dotée à cet effet des services suivants :

- Étude.
- Commercial.
- Projets nouveaux.
- Communication.

3 Le centre informatique de l'EPB

3.1 Présentation du centre informatique

Le centre informatique est une structure de l'EPB rattachée directement à la direction générale, elle a pour mission l'autorisation des métiers de l'entreprise portuaire de Béjaïa, et cela en mettant en place les logiciels et infrastructure nécessaire pour la gestion du système d'information.

L'EPB déploie des systèmes d'information pour accroître la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs. Le réseau local de l'entreprise apporte

aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseur et clients[15].

3.2 L'organisation humaine

Le centre informatique se compose de trois départements sous la coupe de l'assistant du PDG chargé du SI, chaque département est structuré en services comme le montre l'organigramme suivant.

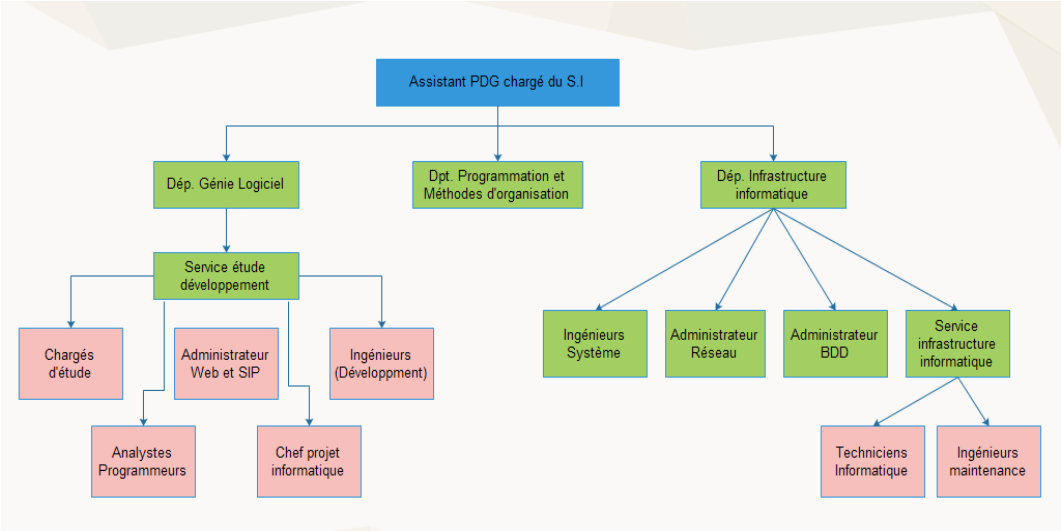

FIGURE 2.5 – Organigramme du département des systèmes d'informations

3.3 Stratégie de la DSI

Les principales stratégies du SI sont :

- Créer de la valeur métier.
- S'organiser pour produire mieux.
- Maîtriser les coûts.
- Réussir les projets.
- Rationnaliser l'architecture.
- Satisfaire les utilisateurs.

3.4 Le réseau local de l'EPB

Le réseau local de l'EPB permet aux différents postes de travail de s'échanger des informations, de se connecter vers l'extérieur et d'utiliser les applications hébergées en interne nécessaires à l'exécution des tâches quotidiennes des employées.

3.4.1 Architecture du réseau de l'EPB

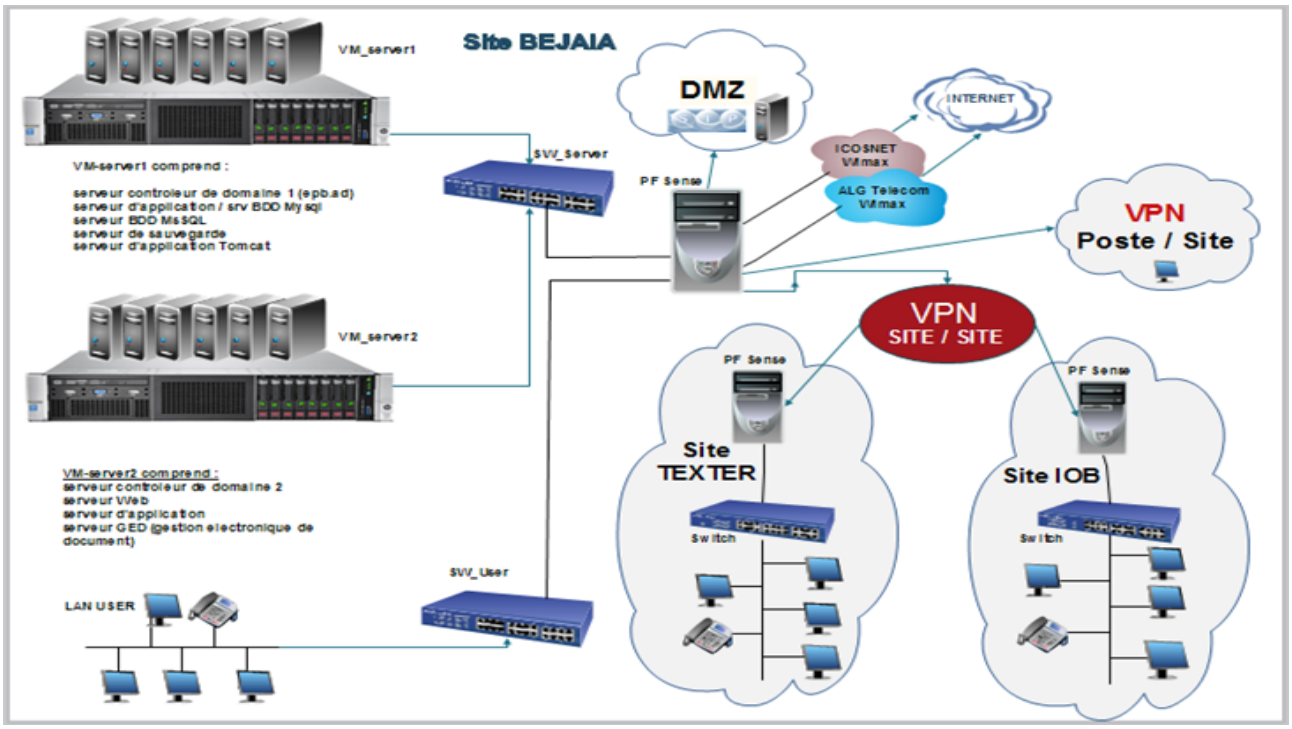

FIGURE 2.6 – Architecture du réseau informatique actuel de l'EPB[15].

Le réseau de l'entreprise portuaire de Bejaïa est d'une architecture client/serveur. L'armoire de brassage constitue l'essence même du réseau de l'EPB, elle contient les équipements réseau permettant aux employés de l'entreprise d'accéder à Internet et de faire de l'intranet. On y distingue plusieurs switchs où arrivent les câbles qui sont connectés aux différentes armoires de brassage de petite taille placées dans chaque étage des bâtiments, reliés aux prises murales où les employés connectent leurs ordinateurs. Les différents serveurs offrent des services aux différents postes clients.

- **Connexion internet :** L'entreprise portuaire de Béjaia s'est dotée de deux connections ALG telecom et ICOSNET. Cette dernière permet de se connecter à Internet haut-débit grâce à une antenne Outdoor qui communique par ondes hertziennes via une station de base au mont Gouraya .

- **Sécurité :** La sécurité est assurée par un par feu (pfsense) qui agit comme un filtre afin de définir les stratégies d'accès et les règles de routage déterminant la manière dont les clients accèdent à internet.
- **Data center (Salle serveur) :** Le data center est le cœur du réseau, toutes les

activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des switchs, elle comporte les différents serveurs.

4 Evaluation du réseau de l'EPB

A l'heure des nouvelles technologies de l'information et des communications, une entreprise qui se veut compétitive ne peut pas s'en passer du secteur de communication, et pour l'EPB qui se veut être parmi les meilleures en Algérie et ensuite en Afrique, Il lui reste beaucoup à faire dans ce secteur, qui est du reste un secteur poumon du développement intégral d'une société moderne.

La communication entre différents services et divisions au sein de l'EPB se fait encore sous forme classique, le PABX analogique à l'heure actuelle où on parle de la convergence de services voix et données sur le même réseau, il serait étonnant que cette institution dispose d'un réseau informatique qui ne sert jusqu'à présent qu'à la transmission des données, et pourtant cette même infrastructure pouvait aussi faciliter l'ajout d'autres services tels que : les communications vocales.

Ce système de téléphonie (VOIP) offre toute une série d'avantages par rapport à la téléphonie classique, dite analogique ou numérique utilisée actuellement au sein de l'EPB. Parmi les avantages, nous pouvons citer : la simplification de l'installation et de la maintenance, l'organisation simple du télétravail, la réduction des coûts de télécommunication, le gain d'argent. Il offre aussi une plus grande flexibilité du système téléphonique de l'entreprise et plus de disponibilité pour les clients.

5 Propositions de solutions

Pour répondre aux objectifs que nous avons évoqués précédemment, nous proposons l'implémentation d'une solution VoIP, offrant aux agents de l'EPB, la possibilité d'effectuer les communications vocales sur le réseau unique voix et données, et voir même à l'extérieure via internet.

L'utilisation de la VoIP conduit à la réduction des coûts d'appels et cela est possible en utilisant un fournisseur de service VoIP pour les appels locaux et internationaux.

Donc, nous avons une seule infrastructure où nous pouvons connecter des télé-

phones directement à une prise (RJ45) du réseau informatique, cette prise peut être partagée avec un ordinateur adjacent et les téléphones logiciels peuvent être aussi installés directement sur le PC.

5.1 Architecture du nouveau réseau de l'EPB

L'architecture de la solution que nous avons proposée est représentée par la figure ci-dessous, elle est scindée en deux étapes

- Ajout de deux serveurs VoIP (VoIP 1, VoIP 2).
- Ajout d'un PFsense redondant.

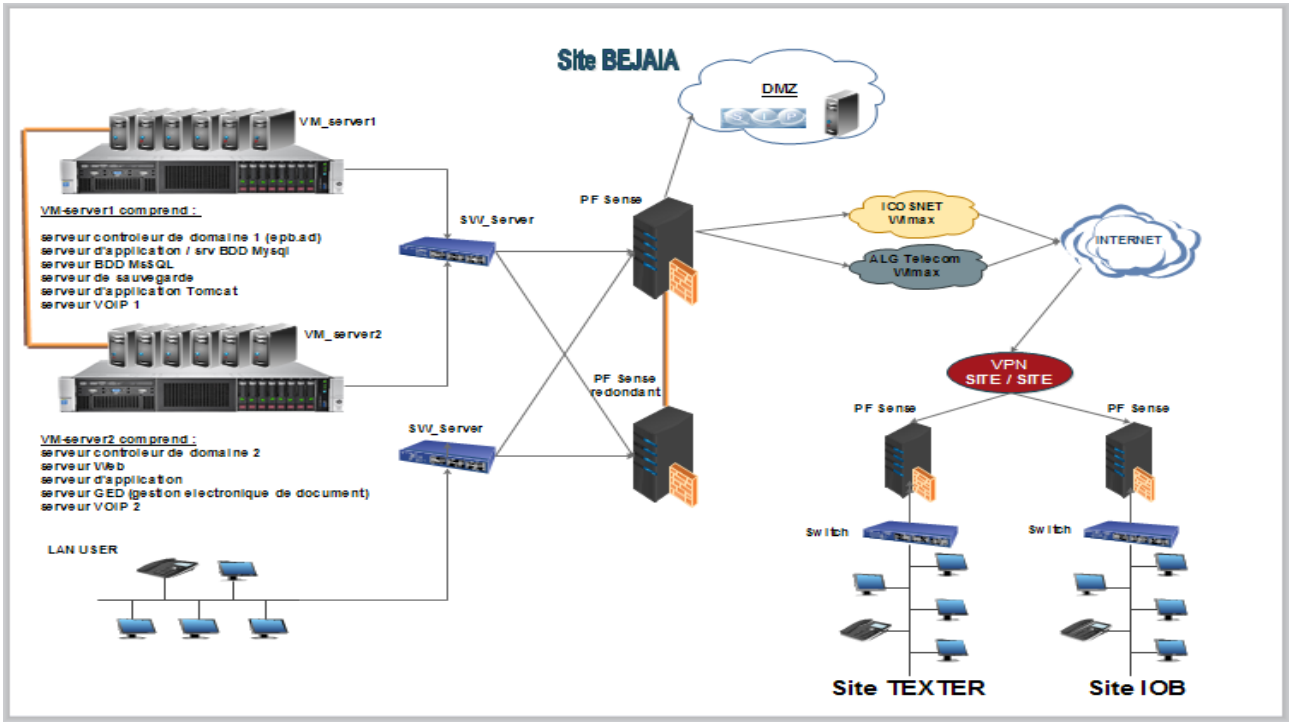

FIGURE 2.7 – Architecture du réseau informatique de l'EPB

Conclusion

Dans ce chapitre, nous avons fait la présentation de l'entreprise portuaire de Bejaïa (EPB), avec un accent particulier sur son réseau informatique, cadre choisi pour l'implémentation de la solution VoIP.

Dans le chapitre qui suit, nous allons procéder à l'installation et la configuration de la solution VoIP basée sur l'outil Asterisk.

Chapitre 3

Implémentation de la solution VOIP sous Asterisk

Introduction

Dans ce chapitre, nous allons proposer le modèle d'implémentation de la solution VoIP, au sein du réseau informatique de l'EPB. Après une étude des différentes solutions de VoIP qui s'offrent à nous, nous avons décidé d'implémenter la solution Asterisk.

Dans un premier temps, nous allons montrer les étapes d'installation et de configuration du logiciel Asterisk sous le système d'exploitation Linux, puis nous procèderons à la configuration de X-Lite qui est un téléphone VoIP softphone, freeware, et nous terminerons avec la mise en place d'un IVR (Interactive Voice Response) incluant notre base de données.

1 Présentation d'Asterisk

1.1 Définition

Asterisk est un autocommutateur téléphonique privé (PABX) open source pour systèmes UNIX. Il permet la configuration de la messagerie vocale, les files d'attente, les agents d'appels, les musiques d'attente, les mises en garde d'appels, la distribution des appels et la gestion de conférences.

Asterisk implémente les protocoles H.320, H.323 et SIP, ainsi qu'un protocole spécifique nommé IAX (Inter-Asterisk eXchange). Asterisk peut également jouer le rôle de registrar et de passerelle avec les réseaux publics. Il est utilisé par certains opérateurs comme cœur de réseau téléphonique du fait de son interopérabilité[10].

1.2 Intérêt du choix d'Asterisk

Asterisk joue un rôle important dans le monde de la téléphonie, c'est un commutateur privé, il a été conçu principalement pour sa compatibilité avec les équipements numériques et analogiques de la ToIP de base standard ainsi que pour son moindre coût. Mais aussi pour sa flexibilité. C'est un serveur qui évolue régulièrement en fournissant d'avantage de nouvelles fonctionnalités, il supporte touts les protocoles de la téléphonie et fonctionne sur plusieurs plateformes (Linux, Windows, Mac).

1.3 Ses principales fonctionnalités

Asterisk compte un nombre très élevé de fonctions permettant de répondre à la majorité des besoins en téléphonie, nous citons :

- Messagerie vocale.
- Conférence téléphonique..
- Répondeur vocal interactif
- Mise en attente d'appels.
- VoIP. . . etc

2 Installation d'Asterisk 13

Avant d'installer Asterisk, il faut préparer le système sous lequel nous installerons notre serveur. Pour cela, il faut installer tout d'abord les pré-requis nécessaires[8].

2.1 Détermination des pré-requis

Les pré-requis nécessaires pour que l'installation du serveur Asterisk s'accomplit avec succès sont :
$gcc, gcc++, bisondoxygen, curl, mlocate, lynx, tar, wget, nmap, bzip2, mod_ssl, crontabs, vixie-cron, libtool-ltdl, libtool-ltdl-devel, mysql-server, php-mysql, php-mbstring, php-mcrypt, flex, screen, libxml2, libtiff, phpmyadmin, build-essential, libxml2-dev, libncurses5-dev, linux-headers-`uname-r`, libsqlite3-dev, libssl-dev, libxml2-dev, libncurses5-dev, linux-headers-`uname-r`, libsqlite3-dev, uuid-dev, libjansson-dev, libssl-dev.$

2.2 Téléchargement des codes sources

Voilà les lignes de commandes nécessaires pour le téléchargement d'Asterisk et libpri identifie l'url. Après nous téléchargerons via la commande *wget*.

```
#cd /usr/src/
#wget http://downloads.digium.com/pub/asterisk/asterisk-13-current.tar.gz
```

2.3 Extraction des paquetages

Les paquetages téléchargés sont des archives compressés qui contiennent le code source, nous aurons besoin de les extraire, en utilisant la commande tar, avant de les compiler.

```
#cd /usr/src/
#tar zxvf asterisk-13-current.tar.gz
```

2.4 Compilation et installation

Asterisk est un serveur de téléphonie open-source permettant de disposer sur un simple PC les fonctions réservées aux PABX professionnel[17].

$\#cd\ /usr/src/Asterisk-13^{*}$	accès au dossier du Asterisk.
$\#make\ clean$	supprime les fichiers inutiles après installation.
$\#./configure$	construction d'un nouveau makefile..
$\#make\ menuselect$	exécution menuselect dans makefile.
$\#make$	compilation du code source.
$\#make\ install$	exécution de la partie install dans makefile.
$\#make\ samples$	

Makefile est un fichier qui contient les instructions à exécuter à partir des commandes, $./configure, make, makeinstall, makeconfig$, etc. chacune de ces commandes exécute le code approprié à elle dans ce fichier.

Dans le cas où nous voudrons bien lancer le serveur asterisk au démarrage du système, il faut exécuter après la compilation et l'installation des paquets, la commande suivante :

$\#make\ config$	charge le serveur Asterisk au démarrage du système.

Ainsi Asterisk est installé, il suffit maintenant de lancer le serveur et de se connecter à la console CLI (Command Line Interface) via la commande :

```
#asterisk -r
```

Pour arrêter et redémarrer le serveur asterisk, il suffit d'exécuter les commandes suivantes :

$CLI > core\ stop\ now$	arrêter le serveur asterisk.
$\#asterisk - c$	redémarrer le serveur asterisk.

3 Configuration d'Asterisk

3.1 Identification des fichiers de configuration

Une fois l'installation d'Asterisk est effectuée, plusieurs fichiers sont créés :

- **/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.
- **/var/run/asterisk.pid :** Fichier contenant le numéro du processus Asterisk en cours.
- **/var/spool/asterisk/outgoing/ :** Contient les appels sortants d'Asterisk.
- **/etc/asterisk/ :** Contient tous les fichiers de configuration.

Le dernier dossier nous intéresse, vu qu'il contient les fichiers de configuration du serveur Asterisk, parmi ces fichiers nous trouvons :

- **agents.conf :** Contient la configuration de l'utilisation des agents,cas d'un centre d'appel. Ceci nous permet de définir les agents et de leurs assigner des ID et des mots de passe.
- **asterisk.conf :** Définit certaines variables pour l'utilisation d'Asterisk. Il sert essentiellement à indiquer à Asterisk où chercher certains fichiers et certains programmes exécutables.
- **extensions.conf :** Configure le comportement d'Asterisk. C'est le fichier qui nous intéresse le plus dans ce travail.
- **iax.conf :** Configure les conversations VoIP en utilisant le protocole Inter-Asterisk Exchange (IAX).
- **rtp.conf :** Ce fichier de configuration définit les ports à utiliser pour le protocole RTP (Real-Time Protocol). Il faut noter que les numéros listés sont des ports UDP.
- **sip.conf :** Définit les utilisateurs du protocole SIP et leurs options.
- **zapata.conf :** Configure les paramètres de l'interface téléphonique Zapata.

3.2 Configuration des comptes users

Les utilisateurs que nous avons crée dans le fichier sip.conf, utilisent le protocole sip pour l'établissement de la connexion. Ces utilisateurs sont présentés ci-dessous :

```
[client]
type=friend      (spécifie le type d'utilisateu)
secret=123         (mot de passe)
host=dynamic       (spécifie l'adresse IP par laquelle l'utilisateur peut accéder à son compte)
username=client       (le nom de l'utilisateur)
context=default       (spécifie le type de routage à utiliser)
callerid=client « 061 »
mailbox=client@127.0.0.1

[standard]
type=friend
secret=123
host=dynamic
username=Standard
context=default
callerid=Standard « 101 »
mailbox=Standard@127.0.0.1

[DR]
type=friend
secret=123
host=dynamic
username=DR
context=default
callerid=DR « 201 »
mailbox=DR@127.0.0.1

[DSI]
type=friend
secret=123
host=dynamic
username=DSI
```

```
context=default
callerid=DSI « 301 »
mailbox=DSI@127.0.0.1
```

3.3 Configuration des extensions

```
[default]     (il faut saisir le nom du contexte entre crochet)
exten ⇒061,1,Dial (SIP/client,10,tr)  (la durée d'attente est 10 secondes si y'a pas de réponse)
exten ⇒101,1,Dial (SIP/standard,20,tr)
exten ⇒201,1,Dial (SIP/DR,20,tr)
exten ⇒301,1,Dial (SIP/DSI,20,tr)
```

Si l'appelant compose le numéro 301, il est mit en relation avec le poste dont le numéro est 301 qui utilise le protocole SIP, pareil pour les autres numéros.

Il existe d'autres options que nous pouvons ajouter dans le fichier extensions.conf, telles que la boîte vocale et le renvoi d'appel. La syntaxe du fichier est sous le format suivant :

Exten= extension, priorité, commande (paramètre)

- **Extension :** C'est généralement le numéro de téléphone ou le nom du client.
- **Priorité :** C'est un numéro qui indique la priorité de la commande, le serveur prend en considération la priorité de la commande en utilisant le numéro inscrit dans la syntaxe.
- **Commande :** C'est la commande qui peut exister, comme la commande dial (appel), voicemail (boîte vocale), etc.

Nous pouvons utiliser plusieurs options pour un seul numéro d'appel, nous pouvons mettre par exemple un transfert d'appel vers un autre numéro ou vers la boite vocale selon des priorités.

```
exten ⇒ 123,1,Answer
exten ⇒ 123,2,Playback                (répondeur)
exten ⇒ 123,3,Voicemail(9)        (9 est le numéro de la boîte vocale)
exten ⇒ 123,4,Hangup
```

Dans chaque ajout ou modification d'un client, il faut mettre à jour le serveur Asterisk en utilisant les commandes suivantes :

```
Localhost*CLI > sip reload
Localhost*CLI > dialplan reload
Localhost*CLI > reload
```

Les heures d'ouvertures de toutes les directions de l'EPB sont de : 8h00 à 16h du dimanche au jeudi. Les appels arrivants dans cette plage horaire uniquement peuvent être transférés à leur correspondant (DR, DSI), par contre le standard de l'EPB peut être joint à tout moment.

```
exten ⇒ 1,1,SayNumber(1)
exten ⇒ 1,2,Goto(default,101,1)

exten ⇒ 2,1,SayNumber(2)
exten ⇒ 2,n,GotoifTime(16 :01-13 :00|*|*|* ?fermer,s,1)
exten ⇒ 2,n,GotoifTime(*|fri-sat|*|* ?ferme,s,1)
exten ⇒ 2,n,Goto(default,301,1)

exten ⇒ 3,1,SayNumber(3)
exten ⇒ 3,n,GotoifTime(16 :01-13 :00|*|*|* ?fermer,s,1)
exten ⇒ 3,n,GotoifTime(*|fri-sat|*|* ?ferme,s,1)
exten ⇒ 3,n,Goto(default,201,1)
```

Les appels en dehors de la plage horaire d'ouverture, un message vocal sera prévu pour les informer des heures d'ouverture des directions de l'EPB.

```
exten ⇒ s,1,Background(/etc/asterisk/sounds/fermer)
exten ⇒ s,1,Background(/etc/asterisk/sounds/ferme)
```

4 Mise en place d'un IVR

Le serveur Asterisk considère l'IVR « Interactive Voice Response » comme toute autre application qui doit être déclarée dans le fichier /etc/asterisk/extensions.conf, et pour l'utilisation des messages vocaux, il faut placer les enregistrements sous le chemin /etc/asterisk/sounds.

4.1 Principe de fonctionnement

L'IVR est un ensemble de commandes permettant un échange continu entre le serveur et l'utilisateur ou l'appelant, cet échange est renforcé par des commandes externes à Asterisk, comme les commandes système ou autre application. Dans notre cas, c'est la mise en place d'un IVR pour la consultation des états des cargaisons stockées dans une base de données MySql, pour les clients de l'EPB.

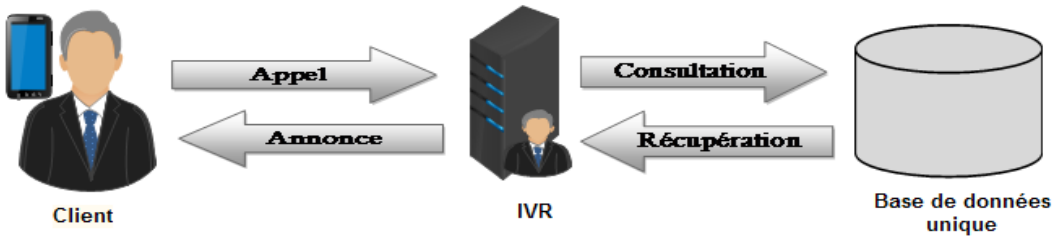

FIGURE 3.1 – Principe de fonctionnement d'un IVR

4.2 Mise en place de la base de données

Cette base de données va recueillir les principales informations relatives et nécessaires pour la récupération des informations et les annoncer automatiquement à l'appelant.
Pour la création, nous utilisons l'interface web de PhpMyAdmin ; un outil de gestion du serveur MySql.

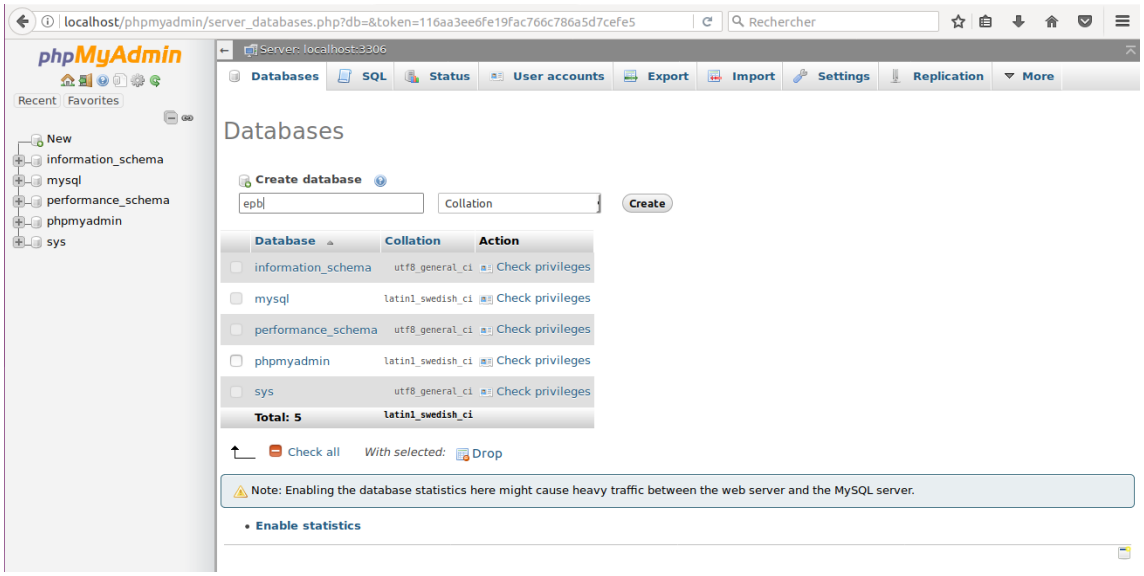

FIGURE 3.2 – Création de la base de données de l'EPB

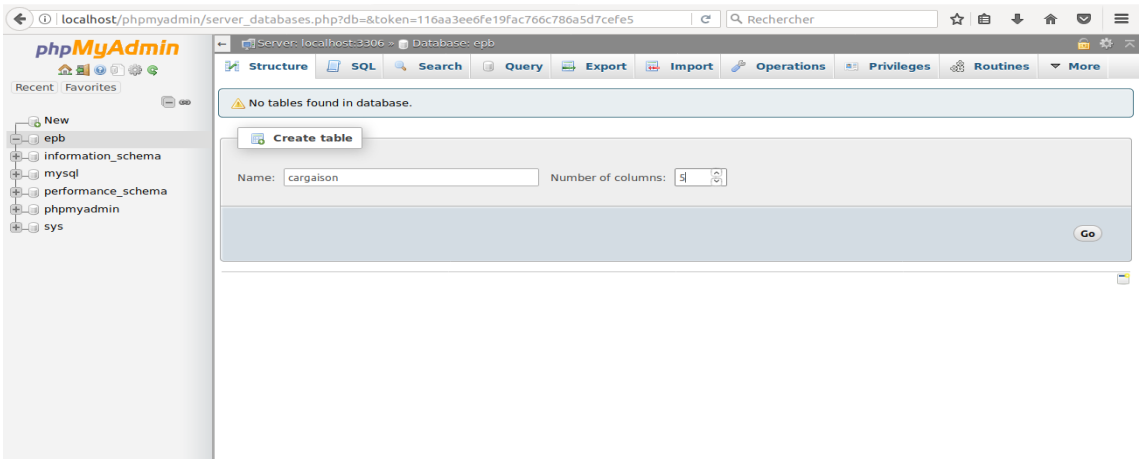

FIGURE 3.3 – Création de la table cargaison

La table cargaison contiendra 5 champs :

- **id :** id de la ligne à insérer dans la base de données.
- **nom :** nom d'utilisateur.
- **prénom :** prénom du client.
- **code :** Numéros du code qui sera la liaison entre l'utilisateur, l'IVR et la base de données.
- **etat_cargaison :** Il pendra une valeur de 1, si la cargaison n'est pas encore prête. une valeur de 2, si la cargaison est disponible. ' ', si le code est incorrect.

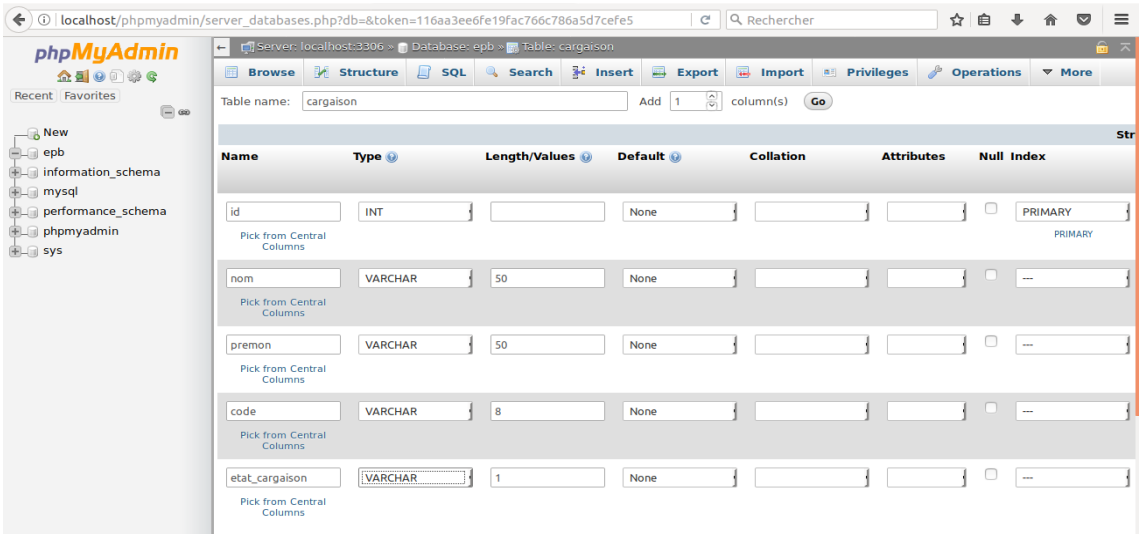

FIGURE 3.4 – Création des champs

4.3 Configuration de l'IVR

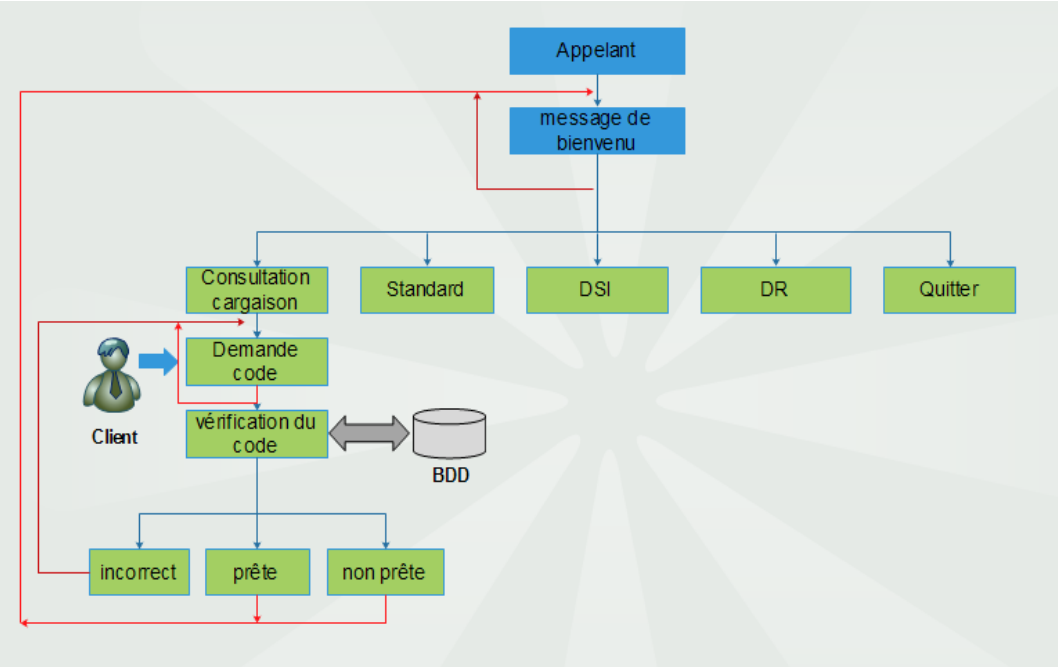

FIGURE 3.5 – Organigramme d'IVR

Ce diagramme représente l'acheminement d'un appel selon les informations saisies par l'appelant jusqu'à l'annonce du résultat.

Cette structure est reproduite dans le fichier de configuration /etc/asterisk/extensions.conf sous forme d'action à exécuter selon l'étape atteinte. Dans notre cas nous avons divisé cet IVR en deux grandes parties ; la première partie contiendra l'accueil et un menu de choix « bienvenu », la seconde contiendra le menu « consultation».

Accueil :

[Bienvenu] : Nom du menu principal.

exten ⇒ s,1,Ringing :

exten ⇒ s,2,Wait(2) : Définir le délais d'attente de saisie d'un choix.

exten ⇒ s,3,Background (/etc/asterisk/sounds/acceuil) : Lecture d'un enregistrement vocal en arrière plan.

exten ⇒ s,4,WaitExten(2) : Attente du saisie d'un choix.

exten ⇒ s,5,Goto(menu,s,3) : Si le temps d'attente de saisie est dépassé, l'appelant est renvoyé vers le début de ce menu.

Choix du service :

exten ⇒ 1,1,SayNumber(1)

exten ⇒ 1,2,Goto(default,101,1) : Lors de la saisie du digit 1, l'appelant peut joindre le standard.

exten ⇒ 2,1,SayNumber(2) exten ⇒ 2,2,Goto(default,201,1) : Lors de la saisie du digit 2, l'appelant peut joindre la DR.

exten ⇒ 3,1,SayNumber(3

exten ⇒ 3,2,Goto(default,301,1) : Lors de la saisie du digit 3, l'appelant peut joindre la DSI.

exten ⇒ 4,1,SayNumber(4)

exten ⇒ 4,2,Goto(consultation,s,1) : Lors de la saisie du digit 4, l'appelant sera orienté vers le menu/application du consultation de cargaison.

exten ⇒ 5,1,SayNumber(5)

exten ⇒ 5,2,Hangup() : Lors de la saisie du digit 5, fin de communication.

exten ⇒ i,1,Playback (/etc/asterisk/sounds/ invalid) : Lors de la saisie de n'importe quel autre digit, l'appelant recevra un message vocal l'informant que la saisie est invalide.

exten ⇒ i,2,Goto(bienvenu,s,3) : Suite de la ligne précédente qui va renvoyer l'appelant vers le début de ce menu.

Service de consultation de cargaison :

[consultation]

exten ⇒ s,1,Playback(/etc/asterisk/sounds/code) : Lecture d'un enregistrement vocal, dans ce cas la lecture ne peut pas être interrompue contrairement à la fonction Background.

exten ⇒ s,n,Read(code,,8,,,) : La fonction Read permet de lire les informations saisies par l'appelant, dans notre cas, nous allons lire les digits saisis jusqu'au 8 digits vu que le code contiens 8 chiffres.

exten ⇒ s,n,MYSQL(connect connid host user password bdd) : Connexion à la base de données.

exten ⇒ s,n,MYSQL(Query resultid $connid SELECT count(*) from cargaison where code=$code) : Sélectionner l'entrée contenant le champ code égale à la valeur de code saisie par l'appelant.

exten ⇒ s,n,MYSQL(Fetch fetchid $resultid etat) : Récupération de la valeur de l'état de cargaison.

exten ⇒ s,n,MYSQL(Clear $resultid) : Vidage des variables.

exten ⇒ s,n,MYSQL(Disconnect $connid) : Déconnexion de la base de données.
exten ⇒ s,n,GoToIf($["$etat" = "1"] ?consultation,p,1) : Si la valeur récupérée est égale à 1, la cargaison est prête et nous orientons l'appelant vers l'action p avec la priorité 1 dans ce menu.
exten ⇒ s,n,GoToIf($["$etat" = "2"] ?consultation,n,1) : Si la valeur récupérée est égale à 2, la cargaison n'est pas prêt et nous orientons l'appelant vers l'action n avec la priorité 1 dans ce menu.
exten ⇒ s,n,GoToIf($["$etat" = ""] ?consultation,r,1) : Si aucun résultat n'est récupéré nous orientons l'appelant vers l'action r avec la priorité 1 dans ce menu.
exten ⇒ p,1,Playback(/etc/asterisk/sounds/carg_pret) : Lecture d'un enregistrement indiquant que la cargaison est prête , puis donner la possibilité à l'appelant de choisir un autre service.
exten ⇒ p,2,WaitExten(2) : Suite de la ligne précédente et en attente d'un digit de la part de l'appelant.
exten ⇒ p,3,GoTo(bienvenu,s,3) : L'appelant est renvoyé vers le début de ce menu.
exten ⇒ n,1,Playback (/etc/asterisk/sounds/carg_n_pret) : Lecture d'un enregistrement indiquant que la cargaison n'est pas prête, puis donner la possibilité à l'appelant de choisir un autre service.
exten ⇒ n,2,WaitExten(2) : Suite de la ligne précédente et en attente d'un digit de la part de l'appelant.
exten ⇒ n,3,GoTo(bienvenu,s,3) : L'appelant est renvoyé vers le début de ce menu.
exten ⇒ r,1,Playback(/etc/asterisk/sounds/rcode) : Aucun enregistrement dans la base de données portant le code saisi par l'appelant et demande de ressaisir un code valide.
exten ⇒ r,2,GoTo(consultation,s,1) : Suite de la ligne précédante et orientation de l'appelant vers la ligne 2 de ce menu pour saisir un code.

5 Présentation de X-Lite

X-Lite est un softphone de CounterPath qui vous permet de faire des appels vocaux et vidéos VoIP, d'envoyer et de recevoir des messages instantanés, de partager des informations en ligne et d'échanger des fichiers [11].

FIGURE 3.6 – X-lite softphone[11].

5.1 Configuration de X-lite

Pour configurer le client X-Lite l'utilisateur « client » doit accéder au menu « Sip Account Setting » puis de ce menu vers le sous menu « Sip Account». Dans la fenêtre qui s'ouvre, il suffit de remplir les champs illustrés suivant l'utilisateur :

L'utilisateur client :

- Identifiant affiché pour l'utilisateur (Display Name) : client
- Identifiant servant a identifié l'utilisateur (User Name) : client
- Mot de passe associé (Password) : 123
- Nom sous lequel l'autorisation d'accès est possible (Authorization user name) : client
- Nom de domaine (Domain) : 192.168.1.109

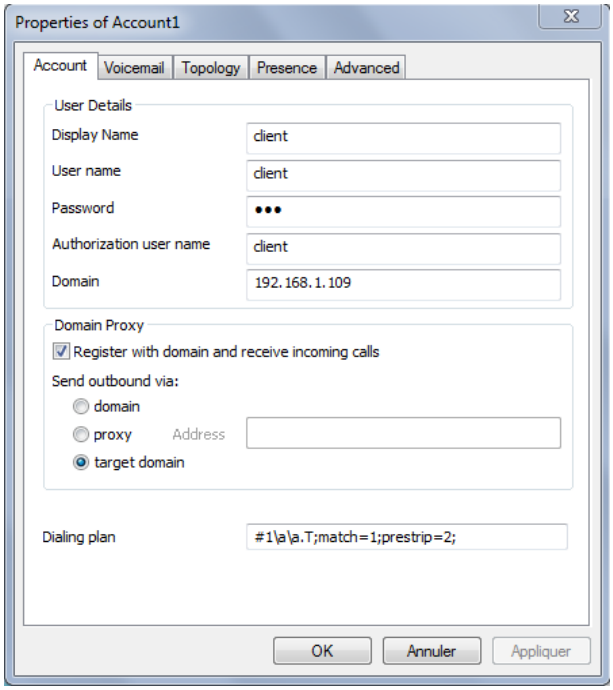

FIGURE 3.7 – Configuration du compte de l'appelant « client »[11].

Il est à noter qu'afin que l'authentification soit possible, ces valeurs doivent être conformes à celles saisies dans le fichier sip.conf du serveur Asterisk.

Une fois la configuration est achevée, le softphone se connectera automatiquement au serveur et s'enregistrera. Un message « Logged in » s'affichera, indiquant que les communications sont désormais possibles. Sinon, un message d'erreur explique le motif qui a fait échouer le processus[11].

Conclusion

Asterisk joue un rôle important au sein de l'entreprise où il facilite l'installation du réseau téléphonique et simplifie la gestion des appels entrants et sortants. Il est ouvert à tous, gratuit et simple à utiliser.

Dans le dernier chapitre, nous allons nous intéresser aux techniques, mécanismes et configurations à mettre en place afin de sécuriser la solution VoIP basée sur le serveur Asterisk.

Chapitre 4

Sécurisation de la solution VoIP

Introduction

Dans ce chapitre, nous allons nous intéresser aux techniques, mécanismes et configurations à mettre en place dans le but de sécuriser la solution VoIP basée sur le serveur Asterisk.

Ce chapitre se compose de deux grandes parties. Dans la première, nous présenterons le logiciel d'attaque Wireshark, ainsi que son mode de fonctionnement. Après, nous allons présenter également des scénarios d'attaques réalisés par ce logiciel. La deuxième partie, sera consacrée aux solutions implémentées pour sécuriser la solution déployée.

1 Architecture du réseau VoIP

La figure 4.1 montre l'Architecture adoptée au cours de la configuration de la solution de VoIP à base d'Asterisk.

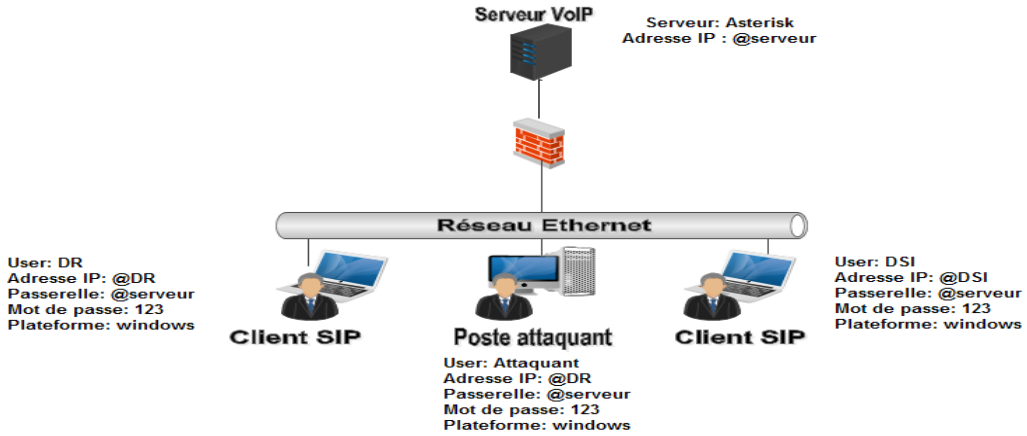

FIGURE 4.1 – Architecture VoIP

- Les deux utilisateurs SIP : Sont des machines sur lesquelles est installé le système d'exploitation windows et un client X-Lite.
- Poste attaquant : Dans le quel le système d'exploitation Linux est installé pour réaliser les attaques.
- Machine serveur : Sur laquelle est installé un système d'exploitation Linux, et le serveur de VoIP, Asterisk.
- Firewall : Un firewall software est installé dans la machine serveur pour limiter l'accès.

2 Attaques au niveau du protocole

Un appel téléphonique VoIP est constitué de deux parties : la signalisation qui instaure l'appel, et les flux de media qui transporte la voix. Les types d'attaques les plus fréquentes contre un système VoIP sont[9] :

2.1 Sniffing

Un reniflage (Sniffing) peut avoir comme conséquence, un vol d'identité et la révélation d'informations confidentielles. Il permet également aux utilisateurs malveillants perfectionnés de rassembler des informations sur les systèmes VoIP. Ces informations peuvent par exemple être employées pour mettre en place une attaque contre d'autres systèmes ou données.

2.2 Suivi des appels

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

2.3 Injection de paquet RTP

Cette attaque se fait au niveau du réseau LAN/VPN. Elle cible le serveur registrar, et a pour but de perturber une communication en cours. Pour réaliser cette attaque, l'attaquant doit être capable d'écouter le réseau afin de repérer une communication et ainsi repérer les timestamps des paquets RTP. Il doit aussi être capable d'insérer des messages RTP qu'il a généré ayant un timestamp modifié.

2.4 Le déni de service (DOS) : Denial of service

C'est, d'une manière générale, l'attaque qui vise à rendre une application informatique ou un équipement informatique incapable de répondre aux requêtes de ses utilisateurs et donc hors d'usage.Une machine serveur offrant des services à ses clients (par exemple : un serveur web) doit traiter des requêtes provenant de plusieurs clients. Lorsque ces derniers ne peuvent en bénéficier, pour des raisons délibérément provoquées par un tiers, il y a déni de service.

Nous allons montrer un exemple de l'attaque déni de service où l'attaquant utilise la requête « CANCEL ».C'est un type de déni de service lancé contre l'utilisateur. L'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL. Cette requête produit une erreur sur le dispositif de l'appelé et termine l'appel. Ce type d'attaque est employé pour interrompre la communication.

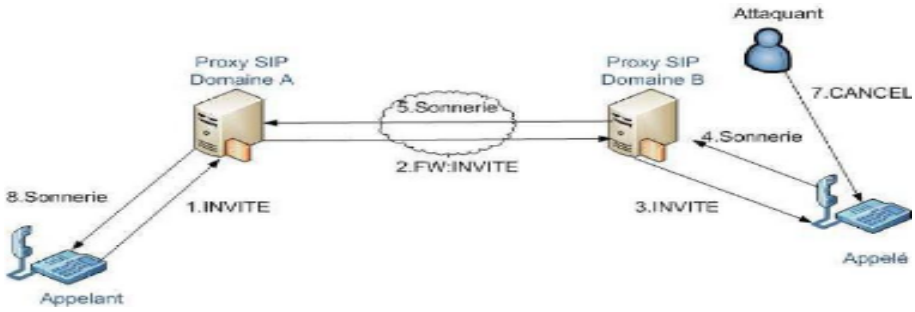

FIGURE 4.2 – Attaque DoS via une requête CANCEL[9].

La figure 4.2 montre un scénario d'attaque DoS CANCEL, l'utilisateur appelant initie l'appel, envoie une invitation (1) au proxy auquel il est rattaché. Le proxy du domaine A achemine la requête (2) au proxy qui est responsable de l'utilisateur appelé. Ensuite c'est le proxy du domaine B qui prend le relais et achemine la requête INVITE (3) qui arrive enfin à destination.

Le dispositif de l'appelé, quand il reçoit l'invitation, sonne (4). Cette information est réacheminée jusqu'au dispositif de l'appelant. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que l'appelé n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu.

2.5 Détournement d'appel (Call Hijacking)

Le Call Hijacking consiste à détourner un appel. Plusieurs fournisseurs de service VoIP utilisent le web comme interface permettant à l'utilisateur d'accéder à leur système téléphonique. Un utilisateur authentifié peut changer les paramètres de ses transferts d'appel à travers cette interface web. C'est peut être pratique, mais un utilisateur malveillant peut utiliser le même moyen pour mener une attaque.

2.6 L'écoute clandestine

L'eavesdropping est l'écoute clandestine d'une conversation téléphonique. Un attaquant avec un accès au réseau VoIP peut sniffer le trafic et décoder la conversation vocale.Des outils tels que VOMIT (Voice Over Misconfigured Internet Telephones) permettent de réaliser cette attaque. VOMIT convertit les paquets sniffés en fichier .wav qui peut être réécouté avec n'importe quel lecteur de fichiers son.

3 Attaques au niveau applicatif

• Les téléphones VoIP disposent d'une interface web de base souvent non protégée, permettant sa programmation à distance. L'assaillant après un scan et identification des terminaux, va pouvoir récupérer des informations essentielles (mots de passe, adresses ...) et détourner à son profit les comptes.

• Les téléphones et IPBX proposent des services qui parfois contiennent des failles de sécurité. Une fois exploitée, l'assaillant pourra prendre le contrôle de tout ou partie du système.

• La configuration ne prenant pas suffisamment en compte la sécurité : mot de passe évident, compte basique ... [12].

4 Les logiciels d'attaques

4.1 Wireshark

Wireshark est l'analyste de protocole réseau le plus utilisé au monde. Il vous permet de voir ce qui se passe sur votre réseau à un niveau microscopique dans de nombreuses entreprises commerciales et à but non lucratif, des organismes gouvernementaux et des établissements d'enseignement. Le développement de Wireshark se développe grâce aux contributions bénévoles des experts en réseau dans le monde entier et est la suite d'un projet lancé par Gerald Combs en 1998.

L'utilisation de Wireshark dans notre projet est pour la détection des vulnérabilités dans le réseau VoIP. Nous essayerons de capturer les paquets qui circulent, pour déterminer quelques informations telles que les adresses IP, les numéros de ports, et d'autres informations qui servent au piratage (vol d'identité, dénie de service, etc.). Ainsi que nous pouvons écouter une communication entre deux clients en décodant les paquets RTP (écoute clandestine) [13].

4.1.1 Captures de trames

Nous avons placé Wireshark sur une 3ème machine qui va jouer le rôle de l'attaquant. Elle va sniffer tout le trafic circulant dans notre réseau local. Nous avons lancé au début la capture des trames, ensuite nous allons initialiser une connexion entre deux utilisateurs SIP,« client » ayant comme adresse IP 192.168.43.75 et « DR » ayant comme adresse IP 192.168.43.7. Le résultat de la capture est le suivant :

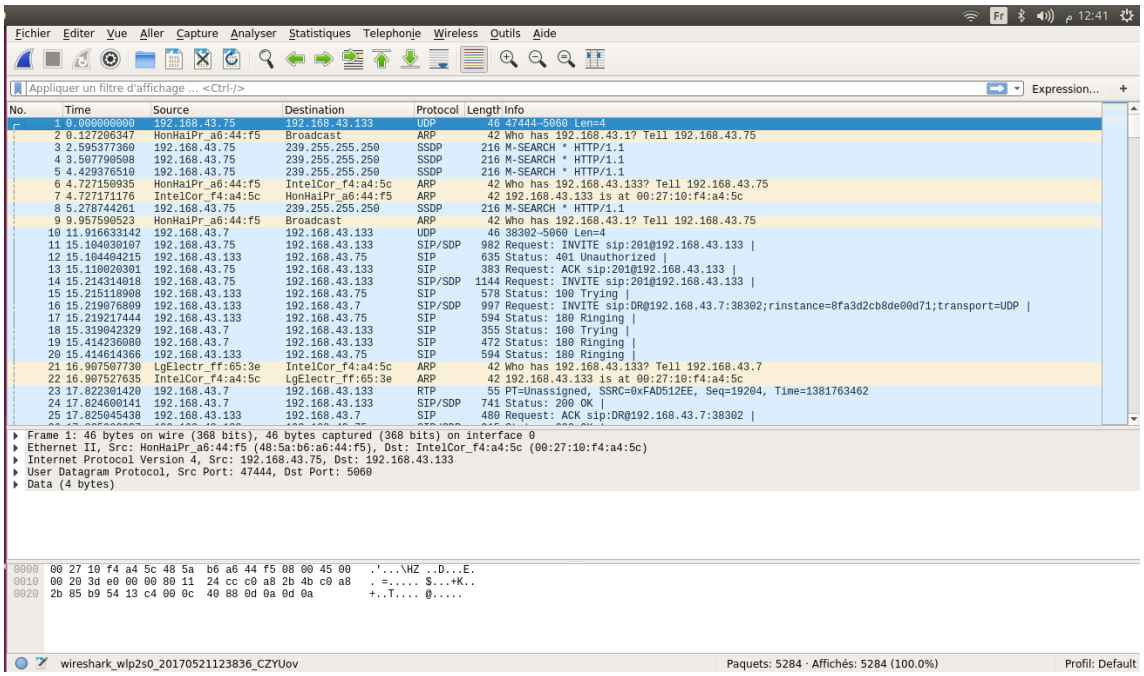

FIGURE 4.3 – Ecran de capture Wireshark

Comme nous pouvons le voir dans la figure 4.3, la conversation entre ces deux hôtes a été capturée. La fenêtre principale de Wireshark comprend deux grandes parties. Dans la première partie, nous voyons les différentes étapes de connexion entre les deux clients.

Dans la deuxième partie, qui est la plus intéressante, nous pouvons lire le contenu des paquets et donc collecter des informations indispensables pour effectuer une bonne attaque.

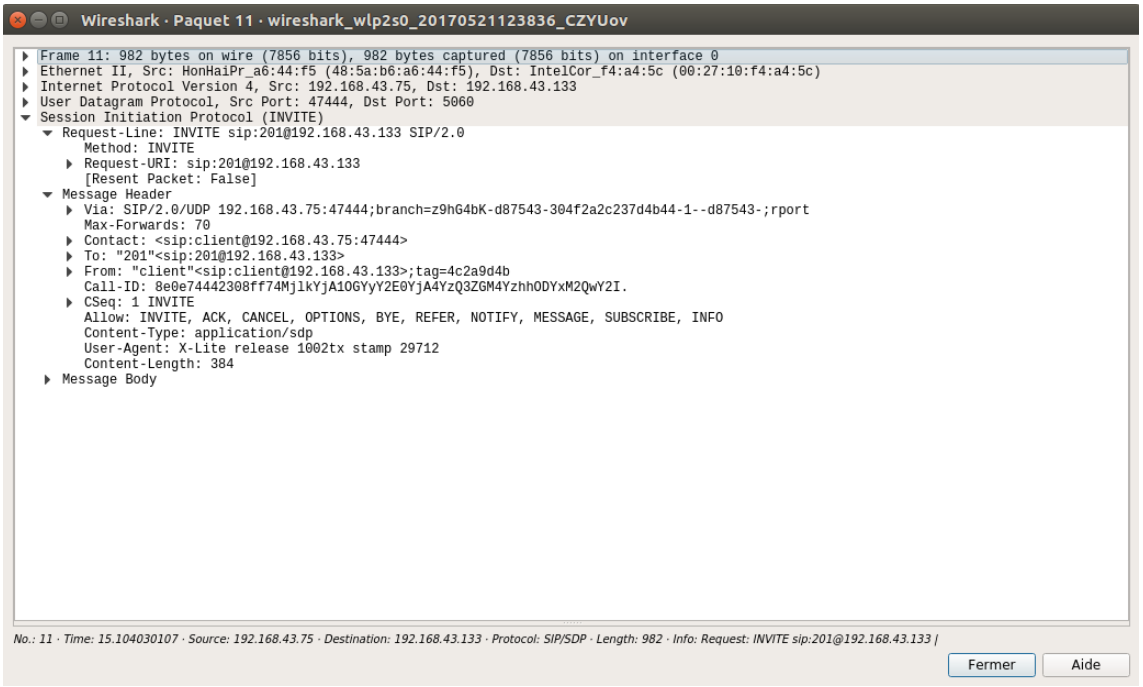

FIGURE 4.4 – Exemple de paquet contenant une requête INVITE

Dans la figure 4.4, le paquet que nous avons choisi à être examiner, est un paquet utilisant le protocole SIP,et contenant une requête INVITE. Cette requête contient des informations indispensables dans le cas où nous voulons effectuer une attaque basée sur le protocole SIP. Par exemple dans le cas où nous voulons exécuter une attaque de type DoS, en utilisant le protocole SIP, nous aurions besoin de connaitre le user agent. Dans cet exemple il n'est autre que le serveur Asterisk, l'adresse SIP de notre victime, son identité et d'autres paramètres.

4.2 Démonstration de l'attaque clandestine avec Wireshark

Nous utilisons Wireshark dans cette sous-section, pour conduire l'attaque d'écoute clandestine. Cette attaque consiste à capturer les trames circulant entre deux machines effectuant une conversation VoIP, et décoder par la suite les paquets afin d'écouter la conversation effectuée.

Le principe est le suivant. Un utilisateur nommé CLIENT ayant comme adresse IP 192.168.43.75 va appeler l'utilisateur nommé DR ayant comme adresse 192.168.43.7. Il faut savoir que ces deux utilisateurs utilisent un serveur Asterisk qui a été préalablement configuré pour effectuer leurs appels.

Avant cet appel, il faut tout d'abord activer Wireshark afin de sniffer le trafic. Il est installé sur une troisième machine qui n'est pas autorisée à passer des appels à travers le serveur Asterisk puisqu'elle n'est pas configurée dans les fichiers de ce dernier. Toutes ces machines sont installées sous le même réseau. Durant la capture nous pouvons voir les différentes phases d'appel, la signalisation et le transport des paquets.

A la fin de l'appel, nous aurions sniffé tous les paquets dont nous aurions besoin pour l'écoute clandestine, les paquets les plus importants sont ceux basés sur le protocole RTP vu qu'ils contiennent les conversations audio entre les deux clients comme l'indique la figure 4.5 :

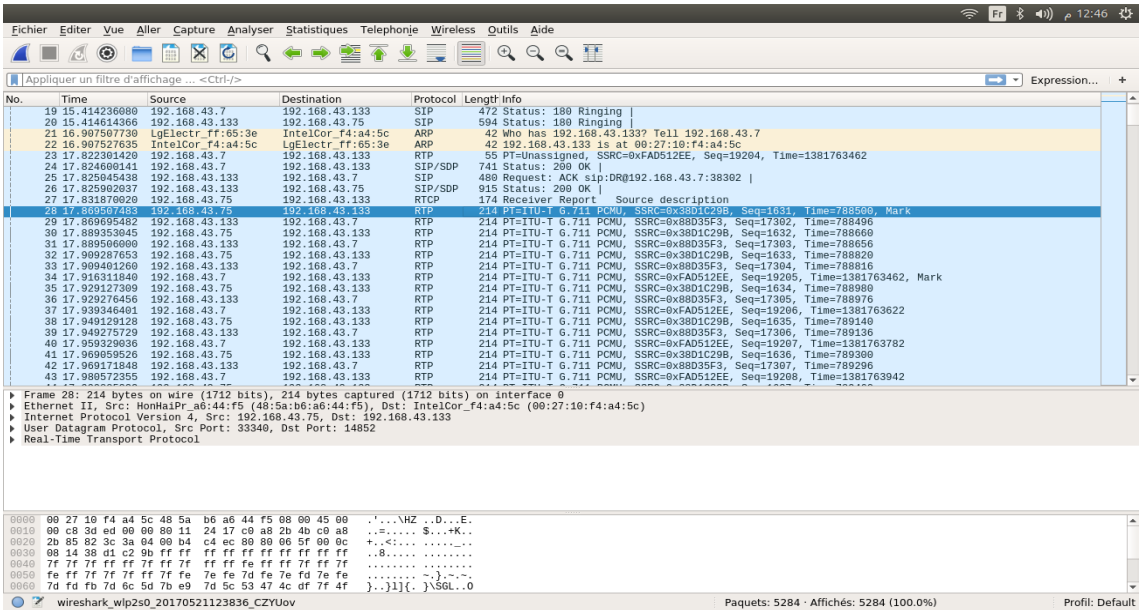

FIGURE 4.5 – Capture d'une communication téléphonique

Après avoir identifié les paquets RTP, nous allons maintenant procéder au décodage de l'appel. Dans le menu de Wireshark, nous cliquons sur le bouton «Telephony », puis ensuite le bouton « VoIP Calls » comme l'indique la figure 4.6.

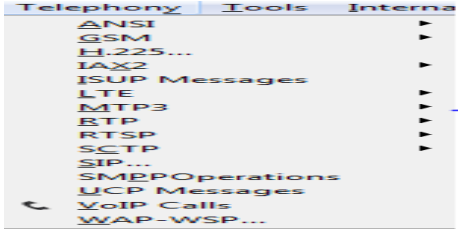

FIGURE 4.6 – Décodage : Bouton VoIP Calls

Une deuxième fenêtre s'ouvre (voir figure 4.7) contenant les communications dans les deux sens, de l'utilisateur qui a l'adresse : 192.168.43.75 vers 192.168.43.7, et inversement.

FIGURE 4.7 – Les communications téléphoniques détectées

Nous choisissons une des communications détectées et nous cliquons sur le bouton « Jouer Flux ». Maintenant que le décodage a abouti, nous pouvons aussi voir sur la figure 4.8 que le son est décodé et qu'il est prêt à être écouté.

Pour l'écoute, il faut choisir le parcours de la communication, plus précisément, il faut choisir la direction de la communication.

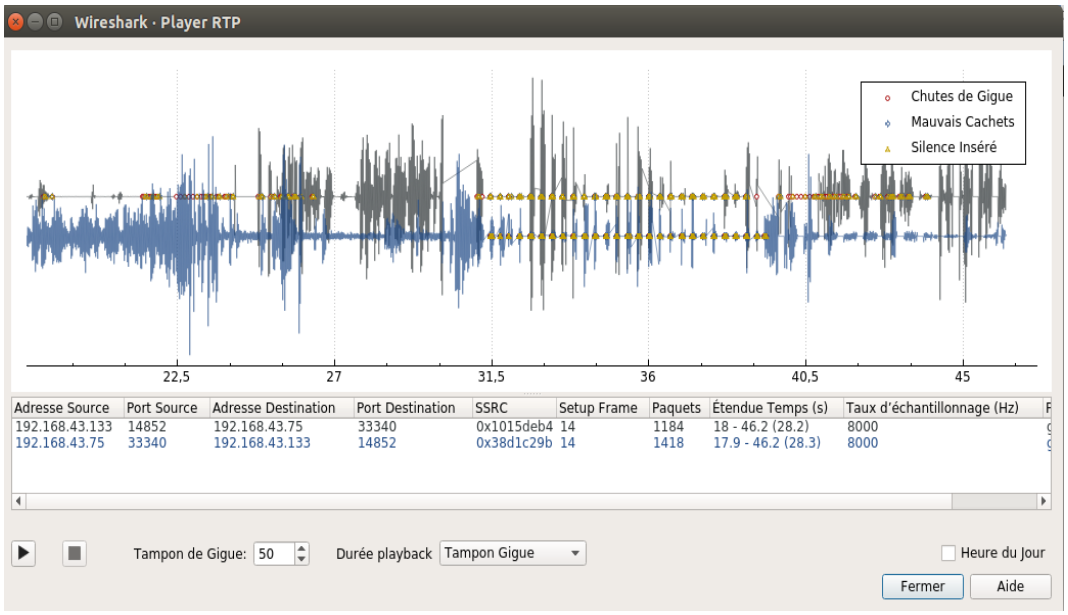

FIGURE 4.8 – Communication téléphonique décodée

5 Choix et implémentation des solutions

Pour se protéger contre l'attaque réalisée et même contre d'autres attaques similaires, nous avons choisi deux solutions qui peuvent aider à minimiser les menaces.

5.1 Solutions contre l'écoute clandestine

5.1.1 Mise en place de la solution VPN

Le VPN (Virtual Private Network) permet de véhiculer du trafic crypté grâce à des clés de cryptage, ce qui rend leur déchiffrage presque impossible. Un VPN permettra donc de contourner les attaques d'écoute clandestine.

L'outil que nous avons choisi pour la mise en place d'un VPN est OpenVPN. C'est un logiciel « open source » permettant de créer un réseau virtuel basé sur SSL. Il peut être utilisé afin de relier deux réseaux ou plus, via un tunnel chiffré à travers Internet. L'utilisation d'OpenVPN nécessite un client de ce dernier pour se connecter à son serveur.

• Installation d'OpenVPN

L'installation d'OpenVPN se fait grâce à la commande suivante :

```
#apt − get install openvpn easy − rsa
```

• Générations des certificats

Après installation, nous allons crée les certificats et les clés qui vont permettre aux clients et au serveur de s'authentifier, de telle sorte qu'aucune personne d'autre ne puisse se connecter au VPN. Nous allons se diriger vers le répertoire où se trouve les fichiers que nous allons configurer.

```
#mkdir /etc/openvpn/easy − rsa
#cd /etc/openvpn
#cp − r /usr/share/easy − rsa/*easy − rsa
```

Nous allons modifier les valeurs des variables d'environnement, afin de ne pas avoir à répéter les renseignements à fournir à la génération des clés, comme indiqué dans la figure 4.9.

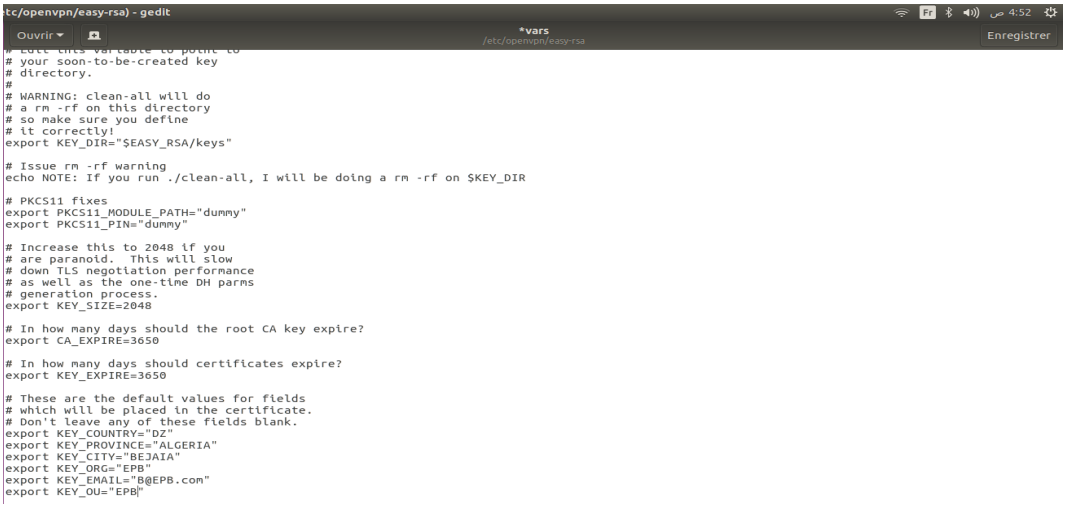

FIGURE 4.9 – Modification des valeurs des variables d'environnements

Une fois le fichier vars modifié, nous nettoierons le répertoire /keys et cela avant la génération des nouveaux certificats et la prise en charge des nouvelles variables, grâce à la commande suivante :

```
#../vars
#./clean − all
```

Nous passons maintenant à la création des certificats, mais avant tout, il faut commencer par créer l'autorité de certification, en tapant la commande suivante :

```
#./build − ca
```

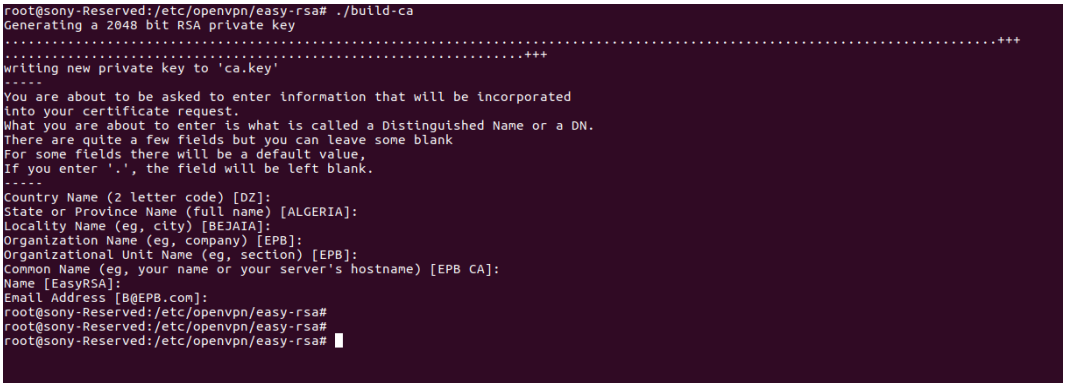

FIGURE 4.10 – Création du certificat d'autorité

Ce certificat est le certificat racine qui va ensuite nous permettre de créer le certificat serveur et les certificats clients. Maintenant, nous allons créer le certificat pour le serveur, grâce à la commande suivante.

```
#./build − key − server server
```

Le résultat de l'exécution de la commande est le suivant :

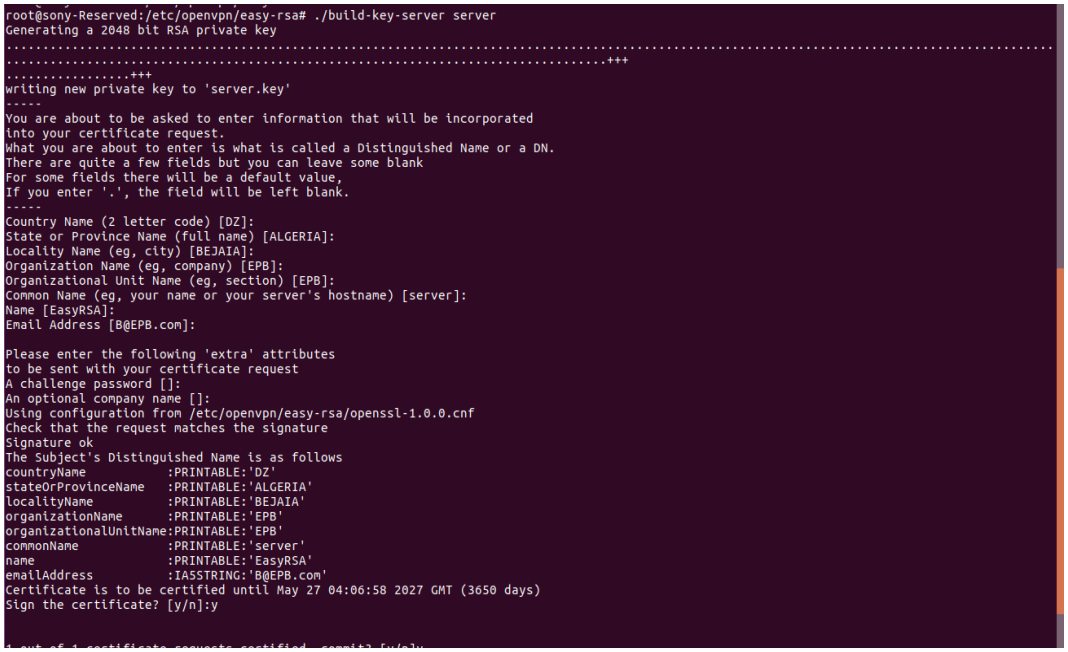

FIGURE 4.11 – Création d'un certificat pour le serveur

Maintenant, il faut créer le certificat pour le client grâce à la commande suivante :

```
#./build − key client
```

L'exécution de cette commande affiche le résultat suivant :

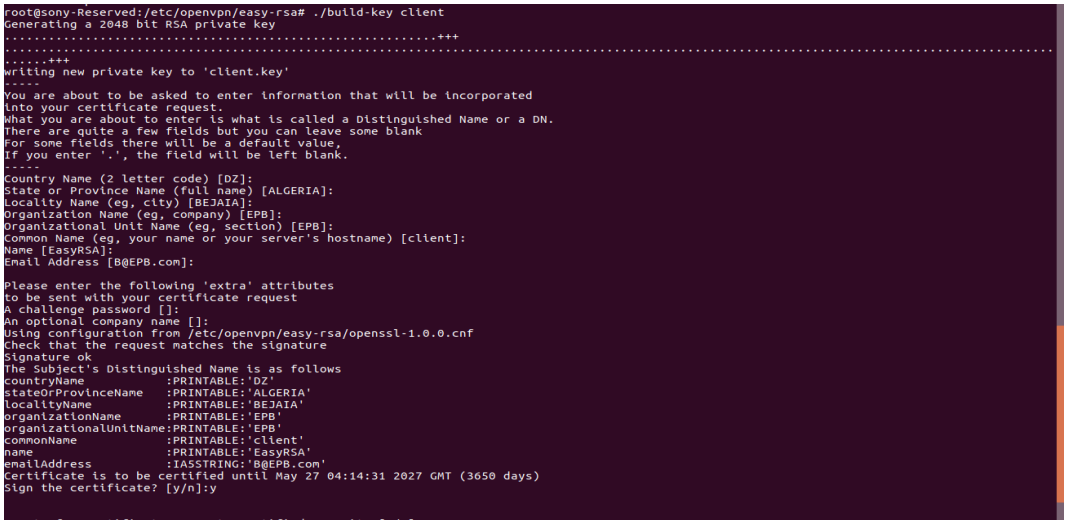

FIGURE 4.12 – Création du certificat client

A présent, il reste à créer les paramètres Diffie-helmann : Diffie-Hellman est un algorithme d'échange de clefs : il permet à deux personnes de mettre en place un système par lequel, elles pourront échanger les données de façon secrète. C'est le premier algorithme créé dans ce but, en 1976, par Whitfield Diffie et Martin E. Hellman [13]. La commande de création est la suivante :

$\#./build - dh$

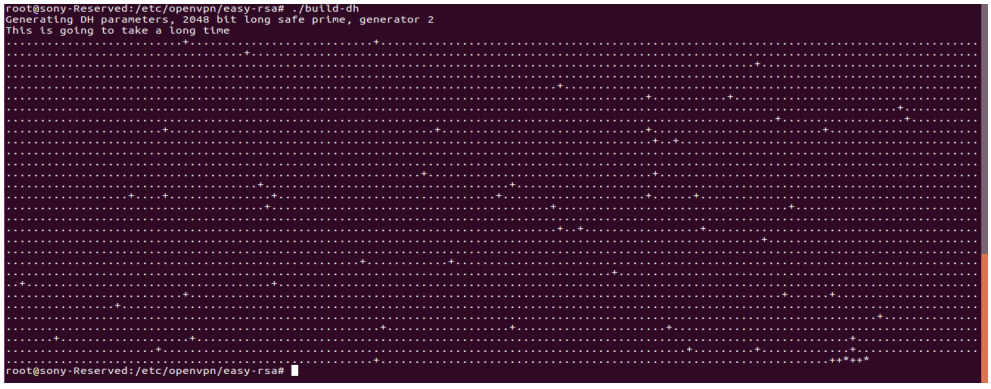

FIGURE 4.13 – Création des paramètres Diffie-helmann

Nous avons maintenant l'ensemble des informations cryptographiques dont nous avons besoin, pour configurer le VPN. Ensuite, il faut copier l'ensemble des informations cryptographiques que nous venons de générer dans le répertoire keys, dans le répertoire

/etc/openvpn crée par défaut à l'installation d'OpenVPN. La commande suivante est utilisée :

```
#cp Keys/*/etc/openvpn
```

• **Création d'un utilisateur OpenVPN**

Nous allons maintenant passer à la création d'un utilisateur ayant des droits restreints, qui sera chargé de lancer le service, de telle sorte que même si la machine s'est faite piratée, l'attaquant n'aura que les droits de cet utilisateur et pas ceux de root. Il faut créer un groupe d'utilisateur dans lequel, nous allons affecter l'utilisateur grâce à la commande suivante :

```
#groupeadd openvpn          (le groupe qu'on vient de créer se nomme openvpn)
Ensuite créer l'utilisateur
#useradd -d /dev/null -s /bin/false -g openvpn
```

• **Configuration et lancement du serveur**

En premier lieu, il faut copier le fichier server.conf se trouvant dans le répertoire /usr/share/doc/openvpn/examples/sample-config-files et le placer dans le répertoire suivant /etc/openvpn.

```
#cp server.conf/etc/openvpn
```

Par la suite, nous allons éditer ce fichier pour y positionner les variables pour la mise en place du VPN.

```
#Vi server.conf          (éditer les paramètres du fichier)
```

Les paramètres à modifier sont les suivants :

– **Dev tun :** Pour pouvoir utiliser OpenVPN en mode tunnel.

– **Server 10.8.0.0 255.255.255.0 :** Nous donnerons cette plage par défaut au serveur. A chaque fois qu'un client se connectera au VPN, le serveur lui attribuera une adresse IP contenue dans cette plage.

– **Comp-lzo** Bien vérifier en bas du fichier l'utilisation de la librairie lzo pour la compression des données.

– **User openvpn / group openvpn :** Utiliser l'utilisateur et son groupe que nous avons créé pour lancer le serveur.

Une fois les paramètres modifiés, nous allons sauvegarder et lancer le service par le

script contenu dans /etc/init.d. Le serveur est prêt à être utilisé. Nous passons alors à la configuration du coté client.

• **Configuration du client**

La configuration du client est simple. Il faut commencer par installer le client OpenVPN sur la machine. Ensuite il faut copier les fichiers suivants (Ca.crt, Client.crt, Client.csr et Client.key) qui se trouvent sous le répertoire /etc/openvpn du coté serveur.

Ensuite, il faut configurer le fichier client.conf afin qu'il puisse reconnaître le serveur grâce à l'ajout de la ligne suivante dans le fichier :

```
Remote 192.168.43.133 1194
```

C'est l'adresse du serveur et le port sur lequel va s'effectuer la connexion VPN. Maintenant le réseau VPN est prêt à être utiliser entre le serveur Asterisk et ses clients.

5.1.2 Chiffrement des appels avec SRTP et TLS

La sécurisation des appels est intéressante à mettre en place, pour protéger nos appels téléphoniques. Pour cela, nous allons chiffrer le flux SIP (signalisation) ainsi que le flux RTP (la voix). De cette manière, nous pouvons assurer la confidentialité[16].

• **Chiffrement SIP avec TLS(Transport Layer Security)**

Il va nous falloir créer des clés pour Asterisk et les clients profitant du chiffrement, Ensuite, nous devrons autoriser Asterisk à utiliser TLS pour les échanges SIP, puis nous devrons choisir les clients à sécuriser, Enfin, il faudra activer le chiffrement sur le poste de client, et lui fournir les fichiers de clé.Pour cela, nous créons un dossier qui contiendra les clés.

```
mkdir /etc/asterisk/keys
```

Le script permettant de créer les clés se trouve dans le dossier suivant :

```
cd /usr/src/asterisk/asterisk − 13.0.0/contrib/scripts/
```

Le script s'exécute comme ceci :

```
./ast_tls_cert −C asterisk.networklab.com −O "NetworkLab" −D /etc/asterisk/keys
```

Voici le détail des options :

• **C :** permet de spécifier le nom d'hôte du serveur Asterisk. A défaut d'un nom, vous

pouvez spécifier une adresse IP.
- **O :** permet de définir le nom de l'organisation.
- **D :** permet de spécifier le dossier de sortie.

A l'exécution du script, Nous avons un certificat self-signed pour l'autorité de certificat, un certificat pour le serveur Asterisk, une clé privée pour l'autorité de certificat et une pour Asterisk. Les fichiers PEM regroupent la clé privée et le certificat.

A présent, nous devons créer les clés et certificats pour les clients.

```
./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k /etc/asterisk/keys/ca.key -
C phone101.networklab.com -O "NetworkLab" -D /etc/asterisk/keys -o clients
```

Voici le détail des options :
- **m :** indique qu'il faut créer un certificat client.
- **c :** permet de spécifier le chemin vers le certificat de l'autorité de certificat.
- **k :** permet de spécifier le chemin vers la clé privée de l'autorité de certificat.
- **C :** permet de spécifier le nom d'hôte du poste du client. Il est possible de spécifier une adresse IP.
- **O :** permet de définir le nom de l'organisation.
- **d :** permet de spécifier le dossier de sortie.
- **o :** permet de choisir le nom de la clé à créer.

A présent, nous devons configurer Asterisk au niveau de fichier sip.conf, en apportons les modifications suivantes, pour autoriser l'utilisation de TLS.

```
[general]
tlsenable=yes
tlsbindaddr=0.0.0.0
tlscertfile=/etc/asterisk/keys/asterisk.pem
tlscafile=/etc/asterisk/keys/ca.crt
tlscipher=ALL
tlsclientmethod=tlsv1
```

Ensuite, nous devons autoriser les clients à utiliser TLS, en ajoutant la ligne transport=tls pour tous les clients concernés.

```
[client]
type=friend
secret=123
host=dynamic
username=client
context=default
callerid=client « 061 »
mailbox=client@127.0.0.1
transport=tls
```

• Chiffrement RTP avec SRTP

La première étape consiste à ajouter le support de SRTP à Asterisk.

– Téléchargement de la librairie SRTP.

```
cd /usr/src/
wget http://srtp.sourceforge.net/srtp-1.4.2.tgz
tar -xvzfsrtp-1.4.2.tgz
rm srtp-1.4.2.tgz
```

– Installation de la librairie SRTP.

```
cd srtp
./configure CFLAGS=-fPIC --prefix=/usr
make
make install
```

Pour qu'Asterisk prenne en charge SRTP, il nous faut le réinstaller

```
cd /usr/src/asterisk/asterisk-13.0.0/
make clean
./configure
make
make install
```

Ensuite,nous chargeons le module SRTP dans Asterisk.

```
asterisk −rv
module load res_srtp.so
```

A présent, il faut forcer l'utilisation de SRTP sur les clients voulus. Pour cela, nous ajoutons la ligne encryption=yes chez les utilisateurs concernés dans sip.conf.

```
[client]
type=friend
secret=123
host=dynamic
username=client
context=default
callerid=client « 061 »
mailbox=client@127.0.0.1
transport=tls
encryption=yes
```

Conclusion

Durant ce chapitre, nous avons parlé des différentes attaques que le réseau VoIP peut subir, parmi lesquelles nous avons cité « L'écoute clandestine », cette dernière peut se faire à l'aide du logiciel d'attaque « Wireshark ».

Afin d'éviter ce genre d'attaque, nous avons appliqué certaines mesures de sécurité, (SRTP, TLS et OpenVPN). Mais il faut savoir qu'il est impossible d'avoir une sécurité parfaite au niveau du réseau VoIP et sur tous les réseaux en général.

Conclusion générale

La VoIP est une technologie émergente qui tente plusieurs entreprises pour l'exploiter vu les avantages qu'elle présente.

En Algérie, cette technologie n'est pas encore très bien développée, vu l'absence des fournisseurs de VoIP. Cependant, il est possible de déployer quelques applications de cette technologie au sein des entreprises multi-sites, ce qui permettra de migrer les communications du réseau RTC vers le réseau IP.

Dans le premier chapitre, nous nous sommes intéressés à l'étude de cette technologie avec ses différents protocoles et standards. Au deuxième chapitre, nous avons fait une étude de l'existant de l'entreprise d'accueil avec un accent particulier sur son réseau informatique, cadre choisi pour la mise en œuvre de notre solution VoIP. Comme troisième chapitre, nous avons installé et configuré la solution VoIP, en utilisant le serveur Asterisk et deux utilisateurs x-lite. Et au dernier chapitre, nous avons effectué une attaque contre la solution installée, puis nous avons proposé et implémenté un mécanisme et un protocole pour la sécuriser.

Le but de notre projet est de réaliser une solution VoIP, afin de sécuriser le réseau mis en place. Pour cela, nous avons effectué une étude qui consiste à réaliser un scénario d'attaque sur le réseau et de voir ensuite les différentes vulnérabilités existantes, afin de sécuriser le réseau VoIP.

Pour conclure, nous tenons à ajouter que ce projet nous a était d'une expérience fructueuse et très bénéfique, car ce fût l'occasion d'enrichir nos connaissances et d'acquérir de l'expérience professionnelle. Cela nous a permis également de bien gérer et optimiser le temps dans le but d'en profiter au maximum.

Bibliographie

[2] J.Da Cunha, "VoIP et Asterisk/Trixbox", maitrise en systèmes distribués et réseaux, Université de Franche Comté, 2007-2008. consulté le 20 Mars 2017 à 15h45

[3] L.Ouakil, G.Pujolle, "Téléphonie sur IP", Eyrolles, Paris, 2008. consulté le 2 Avril 2017 à 10h10

[5] J.Luc Koch, B.Dalibard, "téléphonie sur IP", 2004. consulté le 4 Avril 2017 à 11h20

[7] G.Pujolle, "Les Réseaux", Eyrolles, Paris, 2003. consulté le 8 Avril 2017 à 10h30

[8] P.Sultan, "Asterisk : La téléphonie d'entreprise libre", Concevoir et développer son système de ToIP/VoIP, Eyrolles, 2009. consulté le 9 Avril 2017 à 13h11

[9] P.Thermos, A.Takanen, "Securing VoIP networks threats, vulnerabilities, and counter measures", Addison-Wesley, 2007.consulté le 14 Avril 2017 à 10h53

[17] S.Déon, "VoIP et ToIP Asterisk : La téléphonie sur IP",Eni, 2007. consulté le 17 Avril 2017 à 12h45

[18] J.P.Petit, O.Hersent, D.Gurle, "L'essentiel de la VoIP", Dunod, 2005. consulté le 11 Avril 2017 à 09h01

[19] T.Wallingford, "VoIP à 200%", O'Reilly, 2006. consulté le 29 Avril 2017 à 10h58

Webographie

[1] http ://www.frameip.com/voip/, Voix sur IP – VoIP. consulté le 19 Mars 2017 à 08h40

[4] http ://hi-tech-depanne.com/voip/. consulté le 26 Mars 2017 à 11h02

[6] www.rtcip.fr. consulté le 2 Avril 2017 a 11h19

[10] http ://www.open-source-guide.com. consulté le 5 Avril 2017 à 10h39

[11] http ://www.counterpath.com. consulté le 2 Avril 2017 à 09h27

[12] www.blog-des-telecoms.com. consulté le 13 Avril 2017 à 16h10

[13] www.wireshark.org. consulté le 17 Avril 2017 à 14h30

[14] fr.vikidia.org. consulté le 14 Avril 2017 à 15h10

[15] www.portdebejaia.dz. consulté le 18 Avril 2017 à 13h12

[16] www.networklab.fr. consulté le 2 Avril 2017 à 10h10

Résumé

La communication et le système de transmission de l'information sont devenus maintenant des moyens à grande importance. Et pour cela nous avons fait un tour sur l'une des plus importantes technologies de communication, c'est la voix sur IP, qui emploie le protocole Internet (IP) pour transmettre la voix comme paquets à travers un réseau IP. La VoIP est une bonne solution en matière d'intégration, de fiabilité, d'évolutivité et de coût. Dans notre projet, nous nous sommes intéressés à la protection de la solutions VoIP contre les attaques de sécurité. Ce travail a pour objectif : d'étudier les protocoles, les vulnérabilités et attaque sur la VoIP, afin de mettre en place une solution VoIP sécurisée basée sur le serveur Asterisk et le client X-Lite au sein de l'EPB.

Mots clés : VoIP, SIP, RTP, Asterisk, sécurité VoIP, IP

Abstract

Communication and the system of transmission of information have now become a means of great importance. Thus we have a look at one of the most important communication technologies is Voice over IP, which uses Internet Protocol (IP) to transmit voice as packets through an IP network. VoIP is a good solution for integration, reliability, scalability and cost. In our project, we are interested in protectingVoIP solutions against security attacks. The aim of this work is to study protocols, vulnerabilities and attack on VoIP, in order to implement a secure VoIP solution based on the Asterisk server and the X-Lite client within the EPB.

Keys words : VoIP, SIP, RTP, Asterisk, VoIP security, IP