**SOMMAIRE**

SOMMAIRE …………………………………………………………………………. …i

DEDICACES ……………………………………………………………………………ii

REMERCICEMENTS ………………………………………………....................……..iii

AVANT-PROPOS ………………………………………………………………………iv

LISTE DES FIGURES ………………………………………………………………….v

LISTE DES TABLEAUX ……………………………………………………………..vi

LISTE DES SIGLES ET ABREVIATIONS …………………………………………..vii

INTRODUCTION GENERALE ………………………………………………........…..1

PREMIERE PARTIE : CADRE THORIQUE ET METHOLOGIE ……………………3

DEUXIEME PARTIE : ETUDES DETAILS ET COMPARATIVES …………………8

TROISIEME PARTIE : PRESENTATIONS ET MISE EN PLACE DE LA SOLUTION………………………………………………………………………….….66

CONCLUSION GENERALE ………………………………………………………….100

BIBLIOGRAPHIE ……………………………………………………………………..101

WEBOGRAPHIE ………………………………………………………………….….102

TABLE DES MATIERES ………………………………………………………….….103

**DEDICACES**

Nous dédions ce mémoire :

A notre vieux père que je surnomme « l’homme fort de tous les temps » Gamal Hassan Nour et ma grande sœur que je surnomme aussi « Femme fort de tous les temps » Fatouma Gamal Hassan qui n’ont jamais cessé de nous conseiller, de nous soutenir financièrement et moralement.

A toute notre famille ; à nos frères, sœurs, tantes et nos oncles c’est par vos conseils que nous continuons à persévérer.

En particulier à Fatouma ma grand sœur, Hassan, Souad, Yasmin, Djama, Mariam, Alaleh, sans oublier Ali Hassan et à tous nos collègues, amis, connaissances que nous n’avons pas cité ;

Enfin nous le dédions à ma très chère mère qui ne pas la aujourd’hui Aicha Djama (Pais à son âme).

**REMERCIEMENTS**

Nous tenons à remercier tout premièrement le bon **Dieu** « tout puissant » lui qui nous donne le souffle de vie et nous fortifie tous les jours.

Je tiens aussi à exprimer ma profonde gratitude à tous mes remerciements les plus sincères à nos chers professeurs qui nous ont soutenus durant ces trois ans **: M.MASSAMBA LO, M. NGOR SECK** « l’amour de la programmation »**, M. Rachid, M.KARA SAMB, M. RACINE,**

**M.KHALIFA** notre encadreur qui s’est donné à fond pour nous à fin que nous achevons notre travail en beauté ainsi que nos autres professeurs que nous n’avons pas cité.

En suite à tous nos collègues avec qui nous avons partagé ces beaux moments ensemble.

**AVANT-PROPOS**

L’institut Supérieur d’informatique (ISI) est un institut qui forme dans le domaine de l’informatique.

Situe en plein cœur de Dakar, il offre des formations parmi lesquelles figure la filière Réseaux informatique.

La fin de cette formation est couronnée par l’obtention d’un diplôme professionnelle à la fin du 1er cycle (3ans).

L’institut Supérieur d’informatique qui offre encore des formations extraordinaire comme les formations des Cisco, Microsoft, oracle … etc, En plus c’est un centre des certifications pour prépare la certification Cisco international.

En outre, l’obtention de ce diplôme est conditionnée par la présentation et la soutenance d’un mémoire de fin première cycle d’étude. C’est dans cet ordre d’idée que le présent mémoire portant sur

« ETUDE ET MISE EN PLACE D’UN SYSTEME DE COMMUNICATION DE VOIP SECURISE » vous est présent

# LISTE DE FIGURES

[Figure 1:Topologie physique 10](#_Toc23152163)

[Figure 2:Topologie logique 10](#_Toc23152164)

[Figure 3 : Architecture selon les types des réseaux 11](file:///G:\memoireesss.docx#_Toc23152165)

[Figure 4 : Schéma d'un réseau post à post 11](#_Toc23152166)

[Figure 5 : Schéma d'un réseau client serveur 12](#_Toc23152167)

[Figure 6 : Schéma d'un réseau en bus 13](#_Toc23152168)

[Figure 7 : Schéma réseau d'une topologie en étoile 14](#_Toc23152169)

[Figure 8 : Schéma réseau d'une topologie en anneau 14](#_Toc23152170)

[Figure 9 : Schéma réseau d'une topologie maillée 15](file:///G:\memoireesss.docx#_Toc23152171)

[Figure 10 : Les constituants du Câble STP 17](#_Toc23152172)

[Figure 11 : Les constituants du Câble UPT 18](#_Toc23152173)

[Figure 12 : Schéma d’un réseau LAN 21](file:///G:\memoireesss.docx#_Toc23152174)

[Figure 13 : Wide Area Network (WAN) 22](#_Toc23152175)

[Figure 14 : Modèle OSI 23](#_Toc23152176)

[Figure 15 : Model TCP/IP 26](file:///G:\memoireesss.docx#_Toc23152177)

[Figure 16 : Codage et encodage 32](#_Toc23152178)

[Figure 17 : force brute 48](file:///G:\memoireesss.docx#_Toc23152179)

[Figure 18 : Authentifier nom et mot passe 55](#_Toc23152180)

[Figure 19 : Authentifier par SSL 56](#_Toc23152181)

[Figure 20 : Architecteur de notre réseau 68](#_Toc23152182)

[Figure 21 : L’IP-Phone 69](file:///G:\memoireesss.docx#_Toc23152183)

[Figure 22 : Soft Phone 70](file:///G:\memoireesss.docx#_Toc23152184)

[Figure 23 : Zoiper 70](#_Toc23152185)

[Figure 24 : Les serveurs IP PBX ATCOM 71](file:///G:\memoireesss.docx#_Toc23152186)

[Figure 25 : SWITCH 71](file:///G:\memoireesss.docx#_Toc23152187)

[Figure 26 : Exemple d’une architecture Interne et Externe d’une plateforme ASTERISK 72](#_Toc23152188)

[Figure 27 :la mise à jour du système 73](#_Toc23152189)

[Figure 28 : les Prérequis 74](#_Toc23152190)

[Figure 29 : L’installation PJSIP 74](#_Toc23152191)

[Figure 30 : Décompresse de pjprojetc-2.9.tar.bz2 74](#_Toc23152192)

[Figure 31 : Déplace dans le répertoire pjprojetc-2.9.tar.bz2 75](#_Toc23152193)

[Figure 32 : Préparations de Package 75](#_Toc23152194)

[Figure 33 : Les Dépendances sont remplies 75](#_Toc23152195)

[Figure 34 : Installation de bibliothèques 75](#_Toc23152196)

[Figure 35 : Vérification bibliothèques 75](#_Toc23152197)

[Figure 36 : Déplacement de build 75](#_Toc23152198)

[Figure 37 : Téléchargement d’asterisk 75](#_Toc23152199)

[Figure 38 : Décompression le répertoire asterisk 76](#_Toc23152200)

[Figure 39 : déplacement dans le répertoire 76](#_Toc23152201)

[Figure 40 : L’installation de la prise en charge du format MP3 76](#_Toc23152202)

[Figure 41 :Exécute du script 76](#_Toc23152203)

[Figure 42 : Les paquets à la compilation 76](#_Toc23152204)

[Figure 43 : l’installation des package manquant 76](#_Toc23152205)

[Figure 44 : l’installation asterisk terminer 77](#_Toc23152206)

[Figure 45 : Active de la fonction de format\_MP3 78](#_Toc23152207)

[Figure 46 : Module complémentaires pour la fonction format\_mp3 78](#_Toc23152208)

[Figure 47 : les exemples de fichier de configuration 78](#_Toc23152209)

[Figure 48 :Démarrage de asterisk 78](#_Toc23152210)

[Figure 49 : Le droit de propriété des répertoires 79](#_Toc23152211)

[Figure 50 : redémarrage de serveur et lancement de serveur asterisk 79](#_Toc23152212)

[Figure 51 : Fin d’installation d’asterisk dans notre serveur centos7 79](#_Toc23152213)

[Figure 52 : Fichier de configuration 79](#_Toc23152214)

[Figure 53 : Création d’un utilisateur 80](#_Toc23152215)

[Figure 54 : Configuration d’extension utilisateur 80](#_Toc23152216)

[Figure 55 : Fichier de configuration de Voice mail 81](#_Toc23152217)

[Figure 56 : Configuration de boite vocale 81](#_Toc23152218)

[Figure 57 : Configuration des appels simultanée 81](#_Toc23152219)

[Figure 58 : Activation des touche de transfère 81](#_Toc23152220)

[Figure 59 : Activation du transfert pour les utilisateurs 82](#_Toc23152221)

[Figure 60 : Parking d’appels 82](#_Toc23152222)

[Figure 61 : inclure parkedcalls 82](#_Toc23152223)

[Figure 62 : vidéo conférences 83](#_Toc23152224)

[Figure 63 : les conférences avec xlite 85](#_Toc23152225)

[Figure 64 : capture avec Wireshark sans la sécurité 87](#_Toc23152226)

[Figure 65 : : les paquets qui contient une requête INVITE 88](#_Toc23152227)

[Figure 66 : Capture d’une communication téléphonique 89](#_Toc23152228)

[Figure 67 : Décodage: Bouton VoIP Calls 89](#_Toc23152229)

[Figure 68 : Communication téléphonique détectés 90](#_Toc23152230)

[Figure 69 : Communication téléphonique décodé 90](#_Toc23152231)

[Figure 70 : installation des dépendance 91](#_Toc23152232)

[Figure 71 : l’installation d’openvpn 91](#_Toc23152233)

[Figure 72 : Déplacement dans le répertoire 3 91](#_Toc23152234)

[Figure 73 : Initialisation de pki 91](#_Toc23152235)

[Figure 74 : build-ca 91](#_Toc23152236)

[Figure 75 :build-serveur 92](#_Toc23152237)

[Figure 76 : build-client 92](#_Toc23152238)

[Figure 77 : Gen-dh 92](#_Toc23152239)

[Figure 78 : GenKey Secret 92](#_Toc23152240)

[Figure 79 : se déplace dans le serveur 92](#_Toc23152241)

[Figure 80 : Activation de routage 92](#_Toc23152242)

[Figure 81  : Configuration d’openvpn cote serveur 93](#_Toc23152243)

[Figure 82 : L’installation d’openvpn sur le client 96](#_Toc23152244)

[Figure 83 : Connexion de client vers le serveur 98](#_Toc23152245)

[Figure 84 : Copier les clés et certificat dans les clients 98](#_Toc23152246)

[Figure 85 : l’adresse de vpn de notre serveur 99](#_Toc23152247)

[Figure 86 : compresse 99](#_Toc23152248)

[Figure 87 : copier de fichier dans le répertoire 99](#_Toc23152249)

[Figure 88 : connexion au vpn au client 99](#_Toc23152250)

# LISTE DE TABLEAUX

[Tableau 1 : Matrice de chiffrement de Vernam …43](#_Toc23075307)

[Tableau 2 : Chiffrement ROT13 44](#_Toc23075308)

[Tableau 3 : les logiciels open source de la Voip 63](#_Toc23075309)

# LISTE DES SIGLES ET ABREVIATIONS

**A**

ATM: Asynchronous Transfer Mode.

**D**

DHCP: Dynamic Host Configuration Protocol

DSP: Digital Signal Processor,

**F**

FXS: Foreign exchange Subscriber,

FXO: Foreign exchange Office

**I**

IAX: Inter-Asterisk exchange.

IP: Internet Protocol.

IPBX: Internet Protocol Private Branch exchange

IMAP: Internet Message Access Protocol.

**L**

LAN Local Area Network.

LDAP Lightweight Directory Access Protocol

**M**

MGCP: Media Gateway Control Protocol.

MD5 : Message Digest.

MIC Modulation par Impulsion et Codage.

MTP Message Transfert Part (partie transfert du message).

MCU Multipoint Control Unit.

**N**

NAT: Network Address Translation,

**P**

PABX: Private Automatic Branch exchange.

POP: Post Office Protocol

PBX: Private Branch exchange.

PROM: Programmable Read Only Memory.

PABX-IP: Private Automatic Branch exchange IP.

PSTN: Public Switched Telecommunication Network.

P2P: Peer to Peer.

**Q**

QoS: Quality of service.

**R**

RSA : Rivest Shamir Adleman,

RTC : le Réseau Téléphonique Commuté

RNIS : Réseau numérique à intégration de services.

RAM: Random Access Memory.

RTCP: Real-time Transfert Control Protocole.

RTP : Real Time Protocol

RCX : Réseau de Connexion.

RDN Relative Distinguished Name.

**S**

SIP: Session Initiation Protocol.

SMTP: Simple Mail Transfert Protocol.

SSH: Secure Socket Layer

**T**

ToIP : Téléphonie sur IP

**V**

VoIP : Voice over IP = Voix sur IP

**W**

WAN : Wide Area Network, ou réseau étendu.

# INTRODUCTION GENERALE

De nos jours, les gains des entreprises et des administrations publiques sont influencés par le système de communication qu'elles possèdent par le billet des dépenses téléphoniques qui prennent une grande charge. La voix sur IP était initialement pour l’établissement d'une connexion circulaire entre les clients ou des entreprises dont la signale vocal codée de façon analogique. Depuis quelques années, la technologie VoIP (Voice Over Internet Protocole) commence à intéresser les entreprises, surtout celles de services comme les centres d’appels. Les couts généraux de l’infrastructure de réseau VoIP (Voice Over Internet Protocole) sont réduit et plus très important pour les entreprise.

La voix sur IP est un moyen de communication gratuit avec les nouvelles technologies permettant de transmettre les données ou les voix sur un réseau numérique ou sur l’internet. La voix sur IP est une de solution gratuit qui géré la communication entre clients d’un entreprises avec les différentes protocoles des réseaux avec leurs fonctionnements. La communication sur IP nous offre plusieurs solutions et des avantages au sein de l’entreprise qui implémenté cette solutions pour des raisons communications, Mais il faut des efforts pour innover et essayons des réduire les failles et les inconvénients qui existe encore. Le principe de voix sur IP est de faire circule sur l’internet, grâce protocole IP et aussi sur les réseaux RTC, les paquets de données à des échantillons de voix numérisée.

Comme cette technologie est base sur la téléphonie sur IP, elle est toutefois affectée par les vulnérabilités des attaque qui menacent la sécurité de protocole qui sont implémente sur notre réseaux et l’infrastructure réseaux sur la quelle quand va déployée. Cette dernière est le majeur problème pour les entreprises. Certaines attaques sur les réseaux Vo IP, comme les attaques de déni services, Les vols d’identité, peuvent causse des pertes catastrophique et énorme pour les entreprises. La VoIP (Voice Over Internet Protocole) offre des nombreuses nouvelles possibilités aux opérateurs et utilisateur qui bénéficie d’un réseau base sur IP.

La sécurité sur Vo IP est une nécessite et obligatoires pour les entreprise qui ont implémenté cette solution pour diminuer et réduire, au maximum, les risques des attaques la Vo IP. Il faut même se protège contre tout ce que est malveillant qui peut risquer perte donnée ou des intercepté les communications A vers B ou les contraires.

Pour déployée une solution Vo IP on doit assurer qu’elle va couvrir tout l’infrastructure d’un réseau comme les équipements et aussi la gestion de communications des utilisateurs, et aussi couvrir toutes le système d’exploitation sur les quels sont installés ces outils, le protocole signalisations et le transport de données.

Par contre les inconvénients d’utilise un service VoIP (Voice Over Internet Protocole), et aussi la perdre de la connexion si on le utilise pas une connexion internet haut débit stable. Alimentation de téléphonie qui joue un rôle important dans cet domine, atteintes d’alimentation n’affectent pas les lignes téléphonie traditionnelle à moins que la téléphonie nécessite une alimentation. Alors les utilisateurs peuvent utilise leur téléphonie classique au lieu de utilise une téléphonie sur VoIP (Voice Over Internet Protocole). Et en plus on peut manier un ordinateur portable ou fixe qui utilise sa batterie physique pourrait maintenir la communication sur IP avec certaine temps pendant qu’il est stable, les autres désavantage pour le VoIP (Voice Over Internet Protocole) est la qualité de sonore, généralement il est diffèrent celui de téléphonie traditionnelles, et la qualité sonore dépend la connexion internet. Ainsi que l’utilisation de l’internet peut aussi entrainer sa mauvaise qualité des appels téléphonie.

Le travail que nous allons présenter a pour objectifs de réalisé une étude et mise en place d’un système de communications sur Vo IP sécurise. Pour finir nous avons réalisé un projet qui porte complète avec le serveur asterisk et le client X-lite. Et aussi pour la sécurité nous avons études les attaques et la vulnérabilité sur la VoIP (Voice Over Internet Protocole) ainsi que les configurations utilise pour sécurise de notre réseaux de communications.

Le but de notre études et mettre en place d’un système de communications sur la VoIP (Voice Over Internet Protocole), alors nous avons établiez une long rechercher pour écrit notre mémoire est qui compose en trois partie.

Dans un première partie nous allons introduit la voix sur IP est les objectifs ainsi que la problématique et un analyse complète et la pertinence de sujet et aussi la délimitation de sujet c’est-à-dire des explications claire et simple pour limite notre études dans cas ou notre sujet est bien spécifique. Le deuxième cas de notre projet a pour établir une étude détails comparatives consiste à présente les réseaux informatique ainsi que la technologie sur VoIP (Voice Over Internet Protocole) et tout ce que viens avec la sécurité de VoIP (Voice Over Internet Protocole) avec une étude comparatives des solutions. La troisième partie et toute dernière partie de notre projet nous allons faire une présentation et mise en place des solutions et l’architecteur de la solution est le fonctionnement des implémentations.

**PREMIERE PARTIE**

# Chapitre I : Cadre théorique

Dans ce chapitre consacré au cadre théorique. Nous l’aborderons à travers la problématique liée au sujet, suivis des objectifs, les hypothèses de recherches et la pertinence du sujet.

## **I.1 : Problématique**

Les plupart des entreprise ont des sérieux problèmes les communications et aussi téléconférence avec la téléphonie traditionnelles, mais ils devront change cette technologie car cette technologie est devenu obsolète et leur équipement et des composants avec leur entretien. Ils vraiment important pour les entreprise ou les centre des appels aujourd’hui des change ou anticipe de arrêt de l’utilisation du RTC pour bascule aux réseaux sur IP simple moins couteux. Au causse des changements de la technologie accès à la internet, ils seront généralement la simplicité et la facilite de leur réseaux sans oublie le bénéficier économies avec des possibilités de nouvelle générations est fonctionnalité.

La Communication sur VoIP (Voice over Internet Protocole) est un moyens autonome qui régler beaucoup problème liées à la communications d’un réseau téléphonie sur IP et en plus parlant du cout pour réalise cette technologie est vraiment formidable pour les entreprise qui veulent implémente cette solution qui est une solution libre. Cette technologie sur VoIP (Voice Over Internet Protocole) elle joue un rôle capital dans le domaine de télécommunications dans la vie des entreprises ou vidéo conférence, C’est la raison pour laquelle on aura toujours besoin de faire la communication sur VoIP. Mais le problème qui se pose est la communication blanche est quand l’appelant qui compose un numéro existant de téléphone et n’obtient pas à la destination de l’auteur personne alors il s’agit un communication blanche alors par conséquence l’utilisateur appelant est perdu car il ne sait pas si son appel est abouti ou pas par exemple si la bénéficiaire ou destinateur qu’il veut joindre est occupé ou si il ne décroche pas et aussi qu’il parle pas, décalage dans la conversation est lorsque le utilisateur A ou l’appelant fais un appel à un utilisateur B que le sons parviennent à chaque destinateur de l’appelle avec certaine temps de retarde ce pour cela que la communication devient lourd et pénible, le début et la fin des mots est occupé c’est-à-dire certaine communication ou conversation entre utilisateur A et B va pas arrive à la destination indique son difficilement audibles pour la cause de coupure, bruit et parasites ainsi que quand on peut dire dans notre communication y’a parasite pour savoir ce résultat le seul signe est que y’a trop de bruit très élevé c’est un l’indice qui nous révèle, problème de maintien de la conversation, le temps ou le utilisateur A communique à la utilisateur B que le fréquence de problème et la durée de la communique est limite dans une dure aléatoire mais ça dépasse le trois première la communication.

**Comment améliorer les moyens de communication au sein des entreprise et peut-elle influence sur la réduction des coûts des communications ?**

**Comment sécuriser la solution VoIP qui sera implémentée et d'améliorer la qualité de service ?**

## **I.2 : Objectifs**

### **I.2.1 : objectifs générale**

Objectif général de ce travail consiste mettre en place un système de communications VoIP est propos des solutions sécurité pour assure la sécurité est la performance de la communication.

## **I .2.2 : Objectifs spécifiques**

Nous sommes parvenus à imaginer qu'avec la réalisation de mise en place d'une plate-forme de Voix sur IP sur un réseau, nous espérant adapter la politique de communication des informations de celles-ci à la nouvelle technologie qui n'est rien que la téléphonie au travers d'un réseau « par paquets » offrant :

* Comprendre la téléphonie sur IP fonctionnement et utilité.
* Mettre en place une solution de communication VoIP.
* Gérer les appels entrant et sortant, téléconférence, messagerie instantanée et boit vocal interactives.
* Etudes de la sécurité au tour de la Voip.
* Mise en place de la sécurité pour sécurise le système de communications mis en place.

## **I.3 Pertinence de Sujet**

Dans ce dernier temps les entreprise ils sont séduit par la nouvelle technologie qui sont au point de facilite la vie numérique dans tous les cas. La technologie sur VoIP (Voice over internet protocole) est quelque chose de très impressionnent avec son capacités de transmission qui rendent possible la communication sur internet de protocole, généralement appel téléphone Internet. En plus la manière dont il fait le travailler est vraiment un référencé car il prend les vibrations vocale en signaux numérique compresse traduisent les paquets IP. La VoIP sur IP qui nous permet aussi bien la téléphonique depuis un micro-ordinateur que la téléphonique au niveau d’une entreprise. Asterisk est une bonne mécanique avec un système ouvert souple et flexible qui est en téléphonie l’équivalent d’apache, le serveur web le plus répandu dans le monde. Lorsque la technologie est numérise, il s’intègre autres technologie informatiques. Nous pouvons faire des configurations pour envoyer automatiquement un courriel ou des messages texte lorsque vous avez un message vocal, ou vous pouvez avoir des messages vocaux envoyés à votre adresse email. Entreprise de VoIP offre encore plus d’options de personnalise, surtout si vous avez plusieurs bureau. Vous pouvez transfère les appels d’un bureau à l’autre sans les appelants étant conscient de cela de l’avenir. La qualité de cette technologie est la rapidité la manière dont il gérer les transfère des appels est numérise le son de la voix et compressé selon le format du codec choisi puis insère dans le paquet IP, On sachant qu’il consomme une faible band passant appel sur IP. La voix sur IP est un moyen pour réduire la somme d’utilisation téléphonie pour l’utilisateur de l’entreprise.

# Chapitre II : Cadre Méthodologique

## **II.1 Délimitation de sujet**

Pour la délimitation de notre sujet VoIP est un système de communication dans un domaine très ample et dans cadre de notre travail nous nous intéresserons à la mise en place d’une nouvelle architecture réseaux et d’ un système de voix sur ip sous asterisk avec les améliorations de qualité de service et la flexibilité des appels sans perdre des paquets et l’implémentation d’une solution efficace et qui assure aussi la sécurité des appels, et gérer les appels entrant et sortant et les téléconférence, messagerie … etc.

## **II.2 hypothèses**

### **II.2.1 hypothèse 1**

Nous admettons que la Voix sur IP est le meilleur moyen pour pourvoir en même temps garantir une réduction de coût de communication et de pouvoir entreprendre une excellente utilisation au ressource de la Voix sur IP. ASTERISK est aussi la meilleure solution open source pour pouvoir réalise notre solution VOIP.

### **II.2.2 hypothèse 2**

Mise en place de chiffrements avec « openssl » pour chiffrer et signer le trafic VoIP.

## **II.3 LES DIFFICULTES**

Durant la période de rédaction du mémoire ainsi que celle de la réal station de notre solution la voix sur IP, nous avions eu quelques difficultés dont la principale était le manque de documents, mémoires ou autres portant sur le sujet traité ou similaire afin que nous ayons une idée claire de la méthodologie à suivre. L’autre grande difficulté était le temps insuffisant qui nous a été donné pour terminer l’analyse et la conception de la solution. Nous avons dû approfondir nos connaissances sur le sujet pour avoir une maitrise sur ses concepts. Pour répondre dans les délais fixés pour la réalisation, il nous a fallu allier conception de rédaction.

# DEUXIEME PARTIE

# Chapitre III : ETUDES DETAILLES

# Dans ce chapitre nous traiterons du cadre Etudes détaillés, c’est à dire nous parlerons des rappels réseau informatique et la technologie sur la voix sur IP et puis de les rappels sur la sécurité.

Les réseaux existent depuis longtemps, destinés à transporter de l’information, ils peuvent être classés en trois catégories, principales, selon le type et l’origine de cette l’information:

* Réseaux téléphoniques des opérateurs de télécommunications.
* Réseaux informatiques nés de posemètre de communique des ordinateurs.
* Réseaux de diffusion acheminant les programmes audiovisuels.

Chacune de ces catégories présente des caractéristiques, liées aux applications téléphone, informatique, et de vidéo transportées par les différents réseaux.

## **III.1 Rappel sur les réseaux informatiques**

Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations. On appelle noeud l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions ou équipements (un ordinateur, un routeur, un concentrateur, un commutateur).

Deux types d’entités communiquent au sein d’un réseau:

* **Les ressources matérielles**: ordinateurs, imprimantes qui sont des composantes de traitement, les modems, cartes réseaux, commutateurs, routeurs, câbles qui sont des composants de transmission.
* **Les ressources logicielles:** applications informatiques, bases de données.
* **Composants d’un Réseau :**

Les composants des réseaux se répartissent selon deux types:

* Les composants de traitement sont les entités produisant et/ou consommant les informations qui circulent sur le réseau (ordinateurs).
* Les composants de routage assurent la transition et la circulation des informations échangées entre les composants de traitement (câbles, commutateurs).

Architectures des réseaux: l’architecture d’un réseau comprend 3 parties:

* L’architecture physiquedéfinit la topologie physique d’interconnexion des composants du réseau.
* L’architecture logiquedéfinit la topologie de circulation de l’information. Elle peut être différente de l’architecture physique.
* L’architecture logicielledéfinit les logiciels assurant l’acheminement des données.

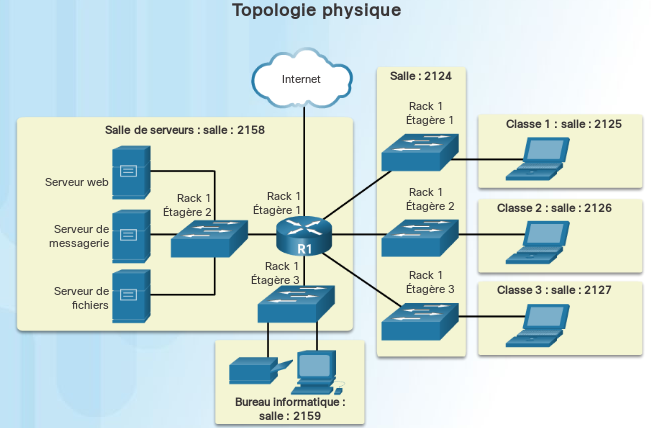


Figure 1:Topologie physique

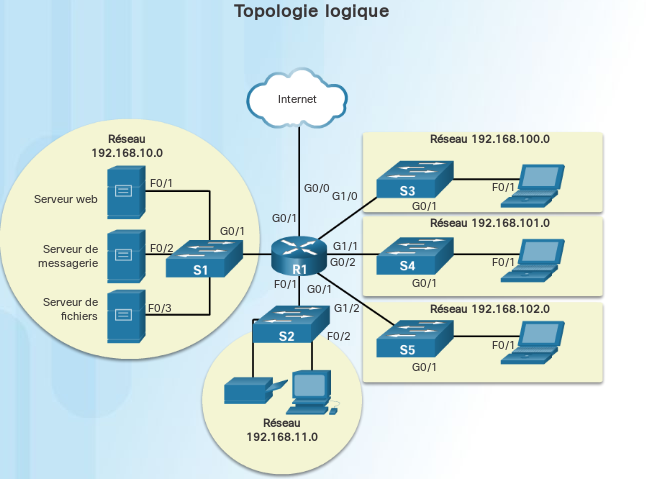


Figure 2:Topologie logique

Les diffèrent type de réseaux informatique est les suivants :

* **Les PAN :** Personal Area Network
* **Les LAN** : Local Area Network
* **Les MAN** : Metropolitan Area Network
* **Les WAN** : Wide Area Network
* **Les GAN** : Global Area Network

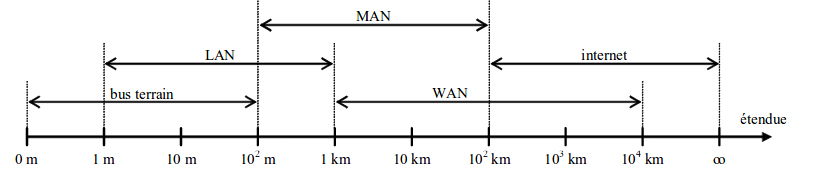


Figure  : Architecture selon les types des réseaux

* **CLASSIFICATION DE LES FONCTIONS ASSUMEES PAR LES ORDINATEUR**

Du point de vue architecture réseau, nous avons deux grandes catégories de réseaux : Réseau POSTE-à-POSTE (Peer to Peer) ;

Réseau serveur dédicacé ou client-serveur (server based).

* **Un serveur:** un ordinateur qui met se ressources et services à la disposition des autres. Il est, en général, du point de vue de ses performances, plus puissant que les autres.
* **Un client:** un ordinateur qui, pour l'exécution de certaines de ses applications fait appel aux ressources et services contenus dans le serveur.
* **Réseau poste-à-poste**

C'est un réseau sans serveur dédicacé, moins coûteux car ne nécessitant pas un serveur puissant et un mécanisme de sécurité très poussée. Chaque ordinateur connecté au réseau peut faire office de client ou serveur. En général, c'est un petit réseau de plus ou moins 10 postes, sans administrateur de réseau.



Figure  : Schéma d'un réseau post à post

Les avantages est l’implémentation moins couteuse, Ne requiert pas un système d'exploitation de réseau ; Ne requiert pas un administrateur de réseau dédié.

Les inconvénients des réseaux poste-à-poste moins de sécurise, chaque utilisateur doit former aux tache d’administrateur alors rend donc vite de l’administrateur très complexe.

* **Réseau à serveur dédicacé ou client serveur**

Dans une configuration client-serveur, les services de réseau sont placés sur un ordinateur dédié, appelé serveur, qui répond aux requêtes des clients. Un serveur est un ordinateur central, disponible en permanence pour répondre aux requêtes émises par les clients et relatives à des services de fichiers, d'impression, d'applications ou autres.

La plupart des systèmes d'exploitation de réseau adoptent des relations client-serveur. En règle générale, les ordinateurs de bureau agissent comme des clients, alors qu'un ou plusieurs ordinateurs équipés d'un logiciel dédié, qui sont dotés d'une puissance de traitement et d'une mémoire plus importantes assurent la fonction de serveurs. Les serveurs sont conçus pour gérer simultanément les requêtes de nombreux clients. La figure I.2 illustré ce réseau



Figure : Schéma d'un réseau client serveur

Les avantages d’un réseau client-serveur est garanti une meilleur sécurité et plus facile à administrer lorsque le réseau est entendu car l’administration est centralisée possibilité de sauvegarder toutes les données dans un emplacement central.

Les inconvénients l'utilisation d'un système d'exploitation de réseau, tel que NT, novelle Netware, Windows server 2003. Le serveur nécessite du matériel plus puissant, mais coûteux ; Requiert un administrateur professionnel ; Présente un point unique de défaillance s'il n'y a qu'un seul serveur ; si le serveur est en panne, les données de l'utilisateur risquent de ne plus être disponibles.

* **CLASSIFICATION SELON LA TOPOLOGIE RESEAU**

La topologie de réseau définit la structure du réseau. Elle représente l'interconnexion des équipements sur le réseau. Ces équipements sont appelés des nœuds. Les nœuds peuvent être des ordinateurs, des imprimantes, des routeurs, des ponts ou tout autre composant connecté au réseau. Un réseau est composé de deux topologies: physique et logique.

* **Topologies en bus**

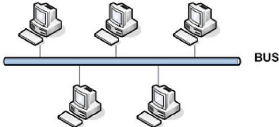
****

Figure  : Schéma d'un réseau en bus

Tous les équipements d'une topologie en bus sont connectés par un même câble, qui passe d'un ordinateur à l'autre, comme le ferait un bus qui traverse la ville. C'est pourquoi on parle souvent de bus linéaire. L'extrémité du segment de câble principal doit comporter un terminateur qui absorbe le signal lorsque ce dernier atteint la fin de la ligne ou du câble. En cas d'absence de terminateur, le signal électrique représentant les données est renvoyé à l'extrémité du câble, ce qui génère une erreur sur le réseau. La figure I.3 représente la topologie en bus.

* **Topologie en étoile**

La topologie en étoile est la plus utilisée sur les réseaux locaux Ethernet. Cette topologie ressemble aux rayons d'une roue de bicyclette. Elle est composée d'un point de connexion central. Il s'agit d'un équipement, comme un hub ou un commutateur, où tous les segments de câble se connectent. Chaque hôte du réseau est connecté à l'équipement central par son propre câble. La figure I.4 représente la topologie en étoile.

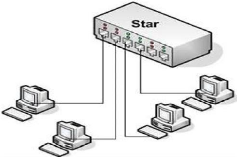


Figure  : Schéma réseau d'une topologie en étoile

**Topologie en anneau**

La topologie en anneau est également très utilisée pour la connectivité des réseaux locaux. Comme son nom l'indique, la forme de connexion des hôtes est celle d'un cercle ou d'un anneau. Contrairement à la topologie en bus, aucune de ses extrémités ne nécessite de terminaison. Le mode de transmission des données est différent de celui utilisé dans les topologies en étoile ou en bus. Une trame, appelée jeton, circule autour de l'anneau et s'arrête à chaque nœud. Si un nœud souhaite transmettre des données, il ajoute les données et les informations sur les adresses à la trame. La trame continue de circuler autour de l'anneau jusqu'à ce qu'elle trouve le noeud de destination. Ce dernier récupère alors les données dans la trame. L'avantage de cette topologie est qu'il n'y a pas de risque de collisions de paquets de données. La figure I.5 représente la topologie en anneau.

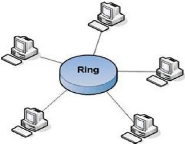


Figure  : Schéma réseau d'une topologie en anneau

* **Topologie maillée**

La topologie maillée permet de connecter tous les équipements, ou noeuds, entre eux afin d'obtenir une redondance et, donc, une tolérance aux pannes. Elle est utilisée sur les réseaux étendus (WAN) pour interconnecter les réseaux locaux, mais également pour les réseaux vitaux comme ceux utilisés par les gouvernements. La mise en œuvre de la topologie maillée est difficile et onéreuse. La figure I.6 représente la topologie maillée.

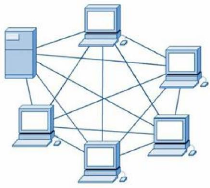


Figure  : Schéma réseau d'une topologie maillée

* **NORMES ET TECHNOLOGIES DES RESEAUX LOCAUX**
* **ETHERNET**

Les bases de la technologie Ethernet sont apparues dans les années 70, avec un programme appelé Alohanet. Il s'agissait d'un réseau radio numérique conçu pour transmettre les informations via une fréquence radio partagée entre les îles hawaïennes. Avec Alohanet, toutes les stations devaient suivre un protocole selon lequel une transmission sans reçu devait être retransmise après un court délai. Des techniques similaires permettant d'utiliser un support partagé ont été appliquées plus tard à la technologie filaire, sous la forme d'Ethernet. Ethernet a été développé dans l'objectif d'accueillir plusieurs ordinateurs interconnectés sur une topologie de bus partagée.

La première version d'Ethernet incorporait une méthode de contrôle de l'accès aux supports appelée CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Cette méthode d'accès a permis de résoudre les problèmes liés à la communication de plusieurs périphériques sur un support physique partagé.

* **TOKEN RING**

La société IBM est à l'origine de Token Ring, une architecture de réseau fiable basée sur la méthode de contrôle d'accès à passage de jeton. L'architecture Token Ring est souvent intégrée aux systèmes d'ordinateur central IBM. Elle est utilisée à la fois avec les ordinateurs classiques et les ordinateurs centraux. Il utilise la norme IEEE 802.5.

La technologie Token Ring est qualifiée de topologie en « anneau étoilé » car son apparence extérieure est celle d'une conception en étoile. Les ordinateurs sont connectés à un concentrateur central, appelé Unité d'Accès Multi Station (MSAU). Au sein de ce périphérique, cependant, le câblage forme un chemin de données circulaire, créant un anneau logique. L'anneau logique est créé par la circulation du jeton, qui va du port de l'unité MSAU à un ordinateur.

Si l'ordinateur n'a aucune donnée à envoyer, le jeton est renvoyé au port MSAU, puis en ressort par un autre port pour accéder à l'ordinateur suivant. Ce processus se poursuit pour tous les ordinateurs offrant une grande similarité avec un anneau physique.

* **FDDI (Fibre Distribution Data Interface)**

FDDI (Interface de Données Distribuées sur Fibre) est un type de réseau Token Ring. L'implémentation et la topologie FDDI est différente de celles d'une architecture de réseau local Token Ring d'IBM. L'interface FDDI est souvent utilisée pour connecter différents bâtiments au sein d'un campus universitaire ou d'une structure d'entreprise complexe. Les réseaux FDDI fonctionnent par câble en fibre optique. Ils allient des performances haute vitesse aux avantages de la topologie en anneau avec passage de jeton. Les réseaux FDDI offrent un débit de 100 Mbits/s sur une topologie en double anneau. L'anneau extérieur est appelé anneau primaire et l'anneau intérieur c'est anneau secondaire.

* **SUPPORTS ET EQUIPEMENT RESEAUX LOCAUX**
* **SUPPORT DE TRANSMISSION**

Les supports de transmissions peuvent être décrits comme le moyen d'envoi des signaux ou données d'un ordinateur à l'autre. Les signaux peuvent être transmis via un câble, mais également à l'aide des technologies sans fil. Nous traiterons les types de support suivants:

Cuivre : coaxial et paire torsadée ;

Verre : fibre optique ; Ondes : sans fil.

* **Câble à paire torsadé**

Le câble à paire torsadée est utilisé pour les communications téléphoniques et pour la plupart des réseaux Ethernet récents. Une paire de fils forme un circuit qui peut transmettre des données. Les paires sont torsadées afin d'empêcher la diaphonie, c'est-à-dire le bruit généré par les paires adjacentes.

Il existe deux types de pair torsadée: Paire torsadée blindée (STP) ;

Paire torsadée non blindée (UTP). 1. Paire torsadée blindée

Le câble à paire torsadée blindée (STP) allie les techniques de blindage, d'annulation et de torsion des fils. Chaque paire de fils est enveloppée dans une feuille métallique afin de protéger davantage les fils contre les bruits. Les quatre paires sont elles-mêmes enveloppées dans une tresse ou une feuille métallique. Le câble STP réduit le bruit électrique à l'intérieur du câble (diaphonie), mais également à l'extérieur du câble (interférences électromagnétiques et interférences de radiofréquences).La figure I.8 représente le câble blindé.

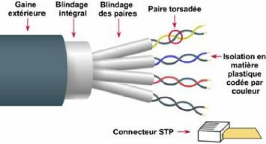


Figure  : Les constituants du Câble STP

* **Paire torsadée non blindée**

Le câble à paire torsadée non blindée (UTP) est utilisé sur différents réseaux. Il comporte deux ou quatre paires de fils. Ce type de câble compte uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal due aux interférences électromagnétiques et aux interférences de radiofréquences. Le câble UTP est le plus fréquemment utilisé pour les réseaux Ethernet. La figure I.9 représente le câble UTP.

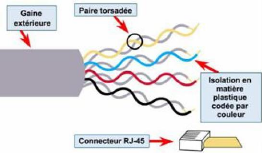


Figure  : Les constituants du Câble UPT

* **Le câble coaxial**

Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.

* **Câble à fibre optique**

Le câble à fibre optique est un de réseau capable d'acheminer des impulsions lumineuses modulées. La modulation de la lumière consiste à manipuler la lumière de telle sorte qu'elle transmette des données lors de sa circulation. Les fibres optiques comportent un cœur de brins de verre ou de plastique (et non de cuivre), à travers lesquels les impulsions lumineuses transportent les signaux.

Elles présentent de nombreux avantages par rapport au cuivre au niveau de la largeur de bande passante et de l'intégrité du signal sur la distance. Tandis que, le câblage en fibre est plus difficile à utiliser et plus couteuse que le câblage en cuivre.

* **Supports sans fil**

La communication sans fil s'appuie sur des équipements appelés émetteurs et récepteurs. La source interagit avec l'émetteur qui convertit les données en ondes électromagnétiques, puis les envoie au récepteur. Le récepteur reconvertit ensuite ces ondes électromagnétiques en données pour les envoyer à la destination. Dans le cadre de la communication bidirectionnelle, chaque équipement nécessite un émetteur et un récepteur. La plupart des fabricants d'équipements de réseau intègrent l'émetteur et le récepteur dans une même unité appelée émetteur-récepteur ou carte réseau sans fil. Tous les équipements d'un réseau local sans fil doivent être dotés de la carte réseau sans fil appropriée. Quatre normes de communications de données courantes s'appliquent aux supports sans fil à savoir:

**Norme IEEE 802.11** : la technologie de réseau local sans fil (WLAN), couramment appelée Wifi, utilise un système de contention ou système non déterministe basé sur un processus d'accès au support par accès multiple avec écoute de porteuse/évitement de collision (CSMA/CA).

**Norme IEEE 802.15** : la norme de réseau personnel sans fil (PAN), couramment appelée Bluetooth, utilise un processus de jumelage de périphériques pour communiquer sur des distances de 1 à 100 mètres.

**Norme IEEE 802.16** : la technologie d'accès couramment appelée Wi MAX (World wide Interoperability for Microwave Access) utilise une topologie point-à-multipoint pour fournir un accès à large bande sans fil.

Enfin La connaissance préalable d'une infrastructure réseau et différents matériels utilisé dans le réseau est une étape nécessaire pour acquérir la maitrise globale d'un environnement réseau. Ce chapitre vient de décrire les types de réseaux, les supports de transmission ainsi que les composants matériels qui les constituent.

**Personal Area Network (PAN)**

Pour permettre l’échange de données des appareils modernes comme notamment les smartphones, tablettes, ordinateurs portables ou les ordinateurs de bureau, ces derniers peuvent être connectés à un réseau adapté. Celui-ci peut être relié sous la forme d’un réseau personnel ou PAN (Personnal Area Network), on parle aussi de réseau domestique. Les techniques de transmission courantes sont l’USB ou le FireWire. Le réseau personnel sans fil (WPAN pour Wireless Personal Area Network) repose sur des technologies comme le Bluetooth, USB sans fil, INSTEON, IrDA, ZigBee ou Z-Wave.  Un réseau personnel sans fil qui peut être réalisé par l’intermédiaire du Bluetooth est appelé « Piconet ». Les WPAN et les PAN ne couvrent généralement que quelques mètres et ne sont pas adaptés pour connecter des appareils se trouvant dans des pièces ou bâtiments différents.

En plus de la communication de plusieurs appareils entre eux, un réseau personnel permet également la connexion à d’autres réseaux, généralement plus grands. On parle dans ce cas d’un Uplink ou de liaison montante. En raison de la portée limitée et d’un taux relativement faible de transfert de données, les PAN sont principalement utilisés pour relier des périphériques pour un usage récréatif. Les exemples typiques sont les écouteurs sans fil, les consoles de jeu et les appareils photo numériques. Dans le contexte de **l**’Internet des objets (idO, en anglais IoT Internet of Things), les WPAN sont utilisés pour la communication, le contrôle et la surveillance des applications à faible débit de données. Des protocoles comme INSTEON, Z-Wave et ZigBeee sont spécifiquement conçus pour la domotique.

**Local Area Network (LAN)**

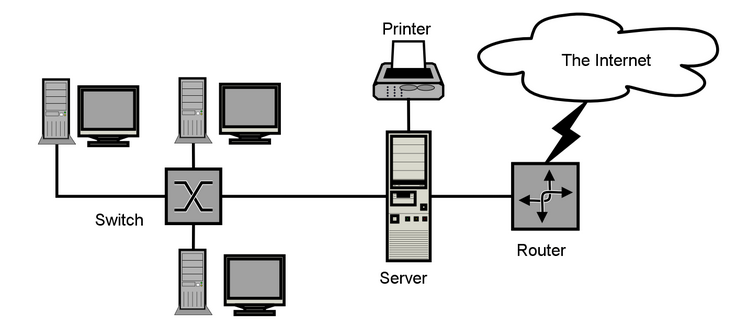
Si plusieurs ordinateurs doivent être réunis sur un réseau, cela se fait généralement sous la forme d’un réseau local ou LAN (acronyme de Local Area Network). Un tel réseau peut relier deux ordinateurs d’une maison ou alors plusieurs centaines d’appareils au sein d’une entreprise. Mais également des réseaux dans des institutions publiques comme les administrations, les écoles ou les universités sont généralement mis en œuvre sous la forme d’un LAN. Une norme commune très répandue pour les réseaux locaux câblés est le protocole Ethernet. Les autres technologies moins fréquentes et parfois obsolètes sont Arcnet, FDDI et Token Ring. La transmission de données est réalisée électroniquement surla base de câbles de cuivreou via des câbles de fibre optique.

Si plus de deux ordinateurs sont imbriqués ensemble dans un réseau local, des composants supplémentaires comme un hub (ou concentrateur), bridge (pont) ou un switch (commutateur réseau) sont nécessaires et agissent alors comme des éléments de couplage et des nœuds de distribution. Un LAN est conçu pour permettre un transfert rapide de grandes quantités de données. Selon la structure du réseau et du moyen de transmission utilisé, un débit de données de 10 à 1000 Mbit/s est courant. Les réseaux locaux permettent un échange d’informations confortable entre les différents périphériques qui sont connectés au réseau. Dans le contexte d’une entreprise, il est courant que plusieurs ordinateurs de travail partagent des serveurs de fichiers, des imprimantes réseau ou des applications sur le LAN.

Si un réseau local est implémenté par radio, on le nomme alors WLAN (Wireless local area network) ou réseau local sans fil. En France on utilise aussi couramment le terme de Wifi pour désigner un WLAN. Il n’y a pas vraiment de différences entre ces deux termes, Wifi est simplement une marque déposée de protocoles de communication sans fil. La base technique de la norme WLAN ou Wifi est définie par les normes du groupe IEE 802.11. Les réseaux locaux sans fil offrent la possibilité d’intégrer facilement des appareils dans un réseau domestique ou d’entreprise et sont compatibles avec un LAN Ethernet filaire. Toutefois, le débit des données est inférieur à celui d’une connexion Ethernet.

La portée d’un réseau LAN est tributaire de la norme utilisée et du support de transmission, pouvant être augmenté par l’amplificateur de signal, ce que l’on appelle un répéteur (de l’anglais repeater). Une plage de signal de plusieurs kilomètres est possible avec Gigabit Ethernet sur fibre optique.

Toutefois, les réseaux locaux couvrent rarement plus d’un complexe de bâtiments. Plusieurs LAN (Local Area Network) à proximité géographique peuvent se connecter à un MAN (Metropolitan Area Network) ou WAN (Wide Area Network).



**Métropolitain Area Network (MAN)**

Figure  : Schéma d’un réseau LAN

Un Métropolitain Area Network (MAN) ou réseau métropolitain, est un réseau de télécommunication à large bande qui relie plusieurs LAN géographiquement à proximité. Il s’agit en règle générale de différentes branches d’une société qui sont reliées à un MAN via des lignes loués. Les routeurs de haute performance et les connexions de fibres optiques hautes performances sont utilisés ce qui permet de fournir un débit de données beaucoup plus élevé que l’Internet. La vitesse de transmission entre deux nœuds éloignés est comparable à la communication dans un réseau local. L’infrastructure pour le MAN est assurée par les opérateurs de réseaux internationaux. En tant que réseau métropolitain, les villes câblées peuvent être intégrées dans les réseaux étendus : WAN (Wide Area Networks) et sur le plan international au niveau des GAN (Global Area Networks).

Metro-Ethernet est une technologie de transmission spéciale disponible pour le MAN qui peut être utilisé pour construire de puissants réseaux métropolitains (MEN ou Metro Ethernet Network) basés sur Carrier Ethernet (CE1.0) ou Carrier Ethernet (CE 2.0).

Une norme pour les grands réseaux de radio régionaux, que l’on nomme Wireless Metropolitan Area Network (WMAN) a été développée avec IEEE 802.16. La technologie connue sous le nom de WiMAX (Worldwide Interoperability for Microwave Access) permet de mettre en place ce que l’on appelle des bornes Wifi ou WLAN hotspots. Ce sont plusieurs points d’accès Wi-Fi travaillant ensemble dans différents endroits. La norme commune de transmission DSL est techniquement disponible que lorsque des câbles en cuivre ont été posés.

**Wide Area Network (WAN)**

Alors que les réseaux métropolitains relient des zones qui se trouvent proches les unes des autres dans des zones rurales ou urbaines, les WAN (Wide Area Network) ou réseaux étendus couvrent des vastes zones géographiques à l’échelle d’un pays ou d’un continent par exemple. En principe, le nombre de réseaux locaux ou d’ordinateurs connectés à un réseau étendu est illimité.

Alors que les réseaux locaux (LAN) et MAN peuvent être réalisés en raison de la proximité géographique des ordinateurs connectés ou des réseaux sur la base d’Ethernet, les réseaux étendus utilisent des techniques comme IP/MPLS (Multiprotocol Label Switching ), PDH (Plesiochrone Digitale Hierarchie), SDH (Synchrone Digitale Hierarchie), SONET (Synchronous Optical Network), ATM (Asynchronous Transfer Mode) et encore rarement l’obsolète X.25.

Les réseaux étendus sont généralement détenues par une organisation ou une entreprise et sont donc exploités en privé ou loués. En outre, les fournisseurs de services Internet utilisent des WAN pour connecter les réseaux locaux d’entreprises et les clients à Internet.

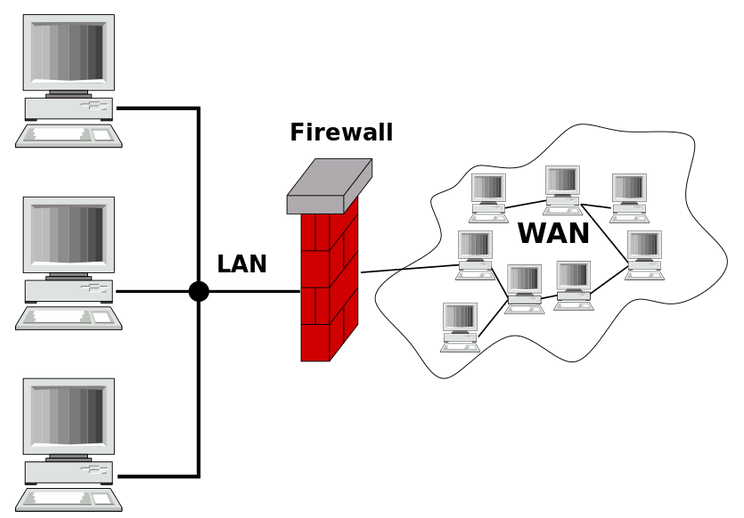


Figure 13 : Wide Area Network (WAN)

## **Global Area Network (GAN)**

Un réseau mondial comme Internet est aussi appelé GAN (Globe Area Network). Internet n’est cependant pas le seul réseau informatique de ce genre. Les entreprises actives au niveau international maintiennent également des réseaux isolés qui couvrent plusieurs WAN et connectent ainsi des ordinateurs d’entreprise dans le monde entier. Les GAN utilisent les infrastructures de fibre optique des réseaux étendus et combinent ces derniers avec descâbles sous-marins internationaux ou des transmissions par satellite.

Le modèle OSI (Open System Interconnexion) est un modèle générique et standard d’architecture d’un réseau en 7 couches, élaboré par l’organisme ISO en 1984. La mise en évidence de ces différentes couches se base sur les caractéristiques suivantes qui étaient recherchées par l’ISO :

* création d’une couche lorsqu’un niveau d’abstraction est nécessaire ;
* définition précise des services et opérations de chaque couche ;
* définition des opérations de chaque couche en s’appuyant sur des protocoles normalisés ;
* choix des frontières entre couches de manière à minimiser le flux d’information aux interfaces ;
* définition d’une couche supplémentaire lorsque des opérations d’ordre différent doivent être réalisées.

Dans le découpage en 7 couches, on distingue :

Les couches basses (1-4) : transfert de l’information par les différents services de transport ;

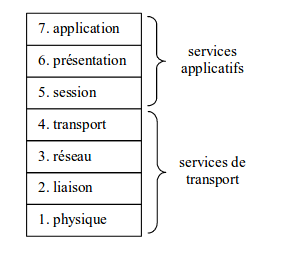
Les couches hautes (5-7) : traitement de l’information par les différents services applicatifs.

Figure  : Modèle OSI

**Physique**

La couche physique (physical (eng)) gère la communication avec l’interface physique afin de faire transiter ou de récupérer les données sur le support de transmission, qui peut être électrique, mécanique, fonctionnel ou procédural.

Ce sont les contraintes matérielles du support utilisé qui décident des objectifs à atteindre pour cette couche :

Conversion en signaux électriques, taille et forme des connecteurs, dimensions et position des antennes, etc.

Ex. : Interconnexion avec le support physique de transmission (paire torsadée, fibre optique, etc.), choix du codage (NRZ, Manchester, modulation AM, FM, etc.), procédure de paramétrage. S

Nb : Il est conceptuellement faux de considérer que le support physique de transmission lui-même appartient à cette couche.

**Liaison**

La couche liaison (liaison de données : datalink (eng)) s’occupe de la bonne transmission de l’information entre les nœuds via le support, en assurant la gestion des erreurs de transmission et la synchronisation des données.

Là aussi, le support de transmission conditionne les protocoles à mettre en œuvre.

Ex. : Gestion des erreurs (contrôles de parité, CRC, etc.), synchronisation (Xon/Xoff, CSMA/xx, etc.), multiplexage.

**Réseau**

La couche réseau (network (eng)) a en charge de déterminer le choix de la route entre les nœuds afin de transmettre de manière indépendante l’information ou les différents paquets la constituant en prenant en compte en temps réel le trafic. Cette couche assure aussi un certain nombre de contrôles de congestion qui ne sont pas gérés par la couche liaison.

Ex. : Techniques de commutation de données (circuits, paquets, etc.).

Nb : Dans les réseaux à diffusion, le routage est très simple, la couche réseau est donc minimaliste, voire inexistante.

**Transport**

La couche transport (transport (eng)) supervise le découpage et le réassemblage de l’information en paquets, contrôlant ainsi la cohérence de la transmission de l’information de l’émetteur vers le destinataire.

Ex. : Techniques de commutation par paquets, fragmentation.

**Session**

La couche session (session (eng)) gère une communication complète entre plusieurs nœuds, permettant ainsi d’établir et de maintenir un réel dialogue suivi (/ une session), pouvant être constitué de temps morts pendant lesquels aucune donnée n’est physiquement transmise.

Ex. : Une connexion HTTP avec suivi de navigation sur un même site web (usage des cookies), une connexion FTP.

**Présentation**

La couche présentation (présentation (eng)) a en charge la représentation des données, c’est-à-dire de structurer et convertir les données échangées ainsi que leur syntaxe afin d’assurer la communication entre des nœuds disparates (différences hardware et/ou software). Ex. : Codage des données (ASCII, Unicode, little-endian, big-endian, etc.), cryptage, compression.

**Application**

La couche application (application (eng)) est le point d’accès des applications aux services réseaux. On y retrouve toutes les applications de communication via le réseau communément utilisées sur un LAN ou sur internet :

Applications de transfert de fichiers, courrier électronique, etc.

Ex. : Navigateurs (HTTP), transfert de fichiers (FTP), clients email (SMTP).

Le modèle TCP/IP est dérivé de l'ARPANET et deviendra plus tard connus sous le nom de world wide internet. L'ARPANET était à la base un projet militaire de l'armée américaine dont le but était de connecter, via les lignes téléphoniques, une centaines d'universités et d'installations gouvernementales entre elles. L'objectif était de maintenir les communications coûte que coûte après une attaque nucléaire. Pour vous remettre dans le contexte, cette problématique à pris place pendant la guerre froide.

Il en découle un réseau basé sur le routage de paquets à travers une couche appelée Internet. La connexion de cette couche est de type connections less (sans connexion préalable) : tous les paquets transitent indépendamment les uns des autres et sont routés suivant leur contenu.

Le modèle TCP/IP est donc le modèle utilisé pour Internet.

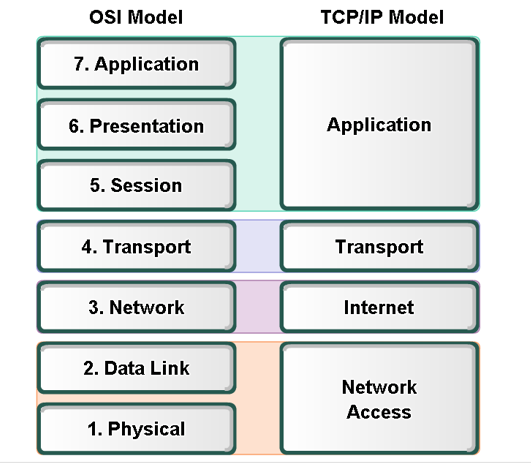
Le nom de modèle TCP/IP est étroitement lié à deux protocoles : le protocole TCP (Transmission Control Protocol) et le protocole IP (Internet Protocol). Ceci est en partie dû au fait que sont les deux protocoles les plus utilisés pour Internet.Voici une figure qui illustre la différence entre le modèle TCP/IP et le modèle OSI :

Figure  : Model TCP/IP

#### 

#### **La couches Host-to-Network**

Couche assez sombre, le modèle TCP/IP en dit peu sur cette couche excepté que l'hôte doit se connecter au réseau depuis certains protocoles de sorte à pouvoir envoyer des paquets IP à travers le réseau.

#### **La couche Internet**

Le but de cette couche est de permettre d'injecter des paquets dans n'importe quel réseau et de faire en sorte qu'ils arrivent à destination. Tous les paquets ne prendront pas le même chemin pour arriver à bon port, mais ceci n'est pas un problème. S'ils arrivent dans le désordre, un protocole, placé dans une couche supérieur, se chargera de les ordonner.

C'est dans la couche internet que sont défini le format officiel des paquets et son protocole : le protocole IP pour Internet Protocol. La fonction de la couche internet est de délivrer les paquets IP au bon endroit. Vous l'aurez compris, le routage des paquets est ici très critique et on souhaite éviter une éventuelle congestion.

On peut faire l'analogie avec la couche network du modèle OSI.

#### **La couche Transport**

Tout comme pour le modèle OSI, la couche de transport permet aux hôtes source et destination de faire une conversation. C'est dans cette couche-ci que sont définis deux protocoles end-to-end pour le transport :

* TCP (Transmission Control Protocol), protocole fiable qui nécessite une connexion entre la source et la destination. Le protocole permet de délivrer un flux d'octets, le tout sans erreurs. Le flux d'octets est d'abord découpé en messages, puis les passe les uns après les autres à la couche Internet. Le destinataire réassemble ensuite les messages reçus. Le protocole TCP dispose également de mécanismes de contrôle pour éviter qu'un émetteur trop rapide n'inonde un receveur trop lent.
* UDP (User Datagramme Protocol), protocole non-fiable qui ne nécessite pas de connexion préalable (sans négociation). Ce protocole ne dispose pas de mécanisme de contrôle de flux. Ce protocole est surtout utilisé dans une architecture de client-serveur voir de requête-réponse, pour la VOIP, les jeux en ligne, les appels vidéos. En effet on peut envoyer des plus grosses quantités de données d'un seul coup par rapport au TCP et on part du principe, lors de l'usage de l'UDP, que si on perd quelques paquets ce n'est pas trop grave. On préfère par exemple avoir une conversation téléphonique hachurée qu'avec du délai.

#### **La couche Application**

Le modèle TCP/IP n'a pas besoin des couches Session ni Presentation. La couche application contient des protocoles haut-niveaux : FTP pour le transfert de fichiers, SMTP pour les mails, HTTP pour le WWW, DNS pour les noms de domaine…

Le modèle TCP/IP et le modèle OSI ont beaucoup de points communs. Tous les deux sont basés sur le concept d'empilement de protocoles indépendants. De plus les différentes couches ont des systèmes de fonctionnement similaires.

* **La Similitudes**
* Les couches au-dessous de la couche de Transport sont des couches orientées vers les applications utilisateurs.
* Les couches au-dessus et y compris la couche de Transport sont là pour fournir un service de transport end-to-end et ce de manière indépendante de la manière de communiquer.

Note: des conclusions différentes seraient émises si nous comparions la stack de protocoles…

#### **La Différences**

* La chose la plus flagrante est le nombre de couches entre les deux modèles. Pour le modèle OSI, il y a 7 couches ; alors que pour le modèle TCP/IP nous sommes à seulement 4 couches.
* L'autre point est le type de connexion supporté. Le modèle OSI supporte à la fois les communications « connection » (communications sans connexion préalable) et les communications « connection-oriented » (connexion préalable) dans la couche réseau ; mais seulement une communication « connection-oriented » dans la couche de transport. Le modèle TCP/IP à contrario ne dispose que d'une communication « connectionless » dans la couche réseau mais des communications « connection-oriented » et « connectionless » dans la couche de transport.

## **III.2 Technologie sur Voip**

# Dans cette partie nous traiterons du cadre Etudes comparatives, c’est à dire nous parlerons des rappels réseau informatique et la technologie sur la voix sur IP.

Au cours dix dernière année, les augmentations des réseaux large band de la réduction couts des VOIP, c’est-à-dire la téléphonique sur IP et définie dérangent qui transforme les secteurs des télécommunications. Les services de la VOIP sont dormais acceptes par le grand fournisseur de service, et aussi le vecteur qui est impact par cette technologie et la réduction et bon communication établie, les opérateurs eux même font des économies en utilisant la technologie sur l’internet.

## **III .2 .1 Historie du téléphone**

En moins deux décennies, Voice Over Internet Protocol ou VoIP (VoIP) a révolutionné l'industrie des télécommunications. Alors que les téléphones cellulaires ont fait les titres dans lesquels progressivement évolué à partir de briques de poche cher supercalculateur, fond VoIP a contribué à briser les barrières dans la communication internationale, en fournissant une réelle alternative aux appels téléphoniques faite avec l'infrastructure de télécommunications traditionnelle et fournit presque universelle accès à des appels bon marché à ne importe qui avec un ordinateur et une connexion internet.

Le premier logiciel de VoIP reconnaissable a été lancé dans les premiers jours de la Internet moderne en 1995. Bien que primitive par les normes d'aujourd'hui, d'Internet VocalTec ' Le service téléphonique 'était révolutionnaire pour l'époque. Un succès parmi les premiers à adopter, Succès encouragé les fournisseurs de matériel de téléphonie par Internet, tels que Cisco Lucent et de développer leur propre entreprise de produits VoIP, destiné à remplacer Les solutions de téléphonie d'entreprise obsolète. Les utilisateurs domestiques, malheureusement, étaient entravée par les limites technologiques de l'époque; les vitesses de connexion lente et pauvres codecs audio de qualité étaient de sérieux obstacles qui ont dû être surmontés avant VoIP pourrait faire le saut vers le grand public.

Le l'arrivée de connexions Internet à large bande à des prix abordables dans la plupart des villes de l'Ouest de début des années 2000 a été cruciale pour la prolifération de la VoIP et de la téléphonie Internet services. Pour la première fois, les utilisateurs avaient suffisamment de bande passante à utiliser plus élevé la qualité codec approché la loyauté des appels téléphoniques ordinaires et pourrait les services VoIP se exécuter simultanément avec le navigateur, les programmes de messagerie instantanée et aussi des jeux sans leurs connexions Internet à une halte. La libération Dernières versions de Microsoft Windows et Mac OS ont aidé à surmonter bientôt la compatibilité matérielle et des maux de tête, avec un casque plug-and-play prennent très les tracas de chat vocal en ligne. La scène était prête pour une révolution; partout ce qui était nécessaire était le bon logiciel pour faire VoIP pour les masses.

Enfin le téléphone sur IP est actuellement un outil vraiment indispensable dans la télécommunication à travers l’internet surtout faire communiquer un ordinateur et un téléphone puis quand on a installé une application qui permet de faire de les appels entre un téléphone et ordinateurs.

* **Caractéristique de la voix sur IP**

Le protocole  IP a été conçu pour ne pas surcharger les réseaux. Il fournit uniquement les fonctions requises pour transférer un paquet d'une source à une destination en passant par un système interconnecté de réseaux. Ce protocole n'est pas destiné au suivi et à la gestion du flux de paquets. Ces fonctions sont effectuées par d'autres protocoles d'autres couches, si nécessaire.

Les principales caractéristiques du protocole IP sont les suivantes :

* **Sans connexion** – aucune connexion avec la destination n'est établie avant d'envoyer des paquets de données.
* **Acheminement au mieux (peu fiable) –** la livraison des paquets n'est pas garantie.
* **Indépendant du support –** le fonctionnement est indépendant du support transportant les données.

## **III.2 .2 Mode fonctionnement et protocole associe Voip**

## **III.2.2.1 PROTOCOLE TCP /IP**

TCP (Transmission Control Protocol) est un des principaux protocoles de la couche transport du modèle OSI. Il permet, au niveau des applications, de gérer les données en provenance de la couche inférieure du modèle (protocole IP). Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP. Le protocole TCP est un protocole orienté connexion, c’est-à-dire qu’il permet à deux machines qui communiquent de contrôler l’état de la transmission. Le protocole TCP permet principalement de:

* Remettre en ordre les datagrammes en provenance du protocole IP
* Vérifier le flux de données afin d’éviter une saturation du réseau
* Formater les données en segments de longueur variable afin de les remettre au protocole IP
* Permet aussi de multiplexer les données.

## **III.2.2.2 PROTOCOLE UDP**

Contrairement protocole UDP aux données où seul le débit global compte, il faut garantir pour la voix un flux le plus régulier possible. Pour ne pas ralentir le trafic, il faudrait utiliser des protocoles de transport simplifié, quitte à ne pas prendre en compte la gestion des erreurs (la voix est peu sensible à quelque erreurs contrairement aux données, mais la qualité perçue est très dépendante des fluctuations de délais dues aux congestions dans le réseau).

Ainsi le protocole UDP basé sur la même couche que TCP. Cependant, il présente des performances moyennes par rapport à TCP, car il permet l’envoi de paquets sans contrôle de réception.

## **III.2.2.3 PROTOCOLE RTP**

Le protocole est protocole qui a été développé par l’IETF, afin de faciliter le transport réel, de bout en bout, des flots de données audio et vidéo sur les réseaux IP. Le protocole RTP n’est pas un protocole réel de transfert, puisque son utilisation se fait généralement sur UDP ce qui permet d’atteindre plus facilement le temps réel.

Les applications temps réel comme la parole numérique ou la visioconférence constitue un véritable problème pour le réseau Internet. Plus généralement RTP permet:

* D’identifier le type d’information transporté
* D’ajouter des marqueurs temporels et des numéros de séquence à l’information transportée
* De contrôler l’arrivée à destination de paquets

## **III.2.2.4 PROTOCOLE RTP**

Le protocole RTCP est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. L’objectif de RTCP est de fournir différents types d’informations et un retour quant à la qualité de réception. Le protocole RTCP est un protocole de contrôle associé à RTP, il mesure les performances, il n’offre pas de garantie par contre. Pour cela, il faut, employer un protocole de réservation de type RSVP ou bien s’assurer que les liens de communication utilisés sont correctement dimensionnés par rapport à l’utilisation qui en est fait. Trois principales fonctions de RTCP:

* Fournir des informations sur la qualité de session
* Contrôler le débit auquel les participants à une session RTP transmettent leurs paquets RTCP
* Transmettre des informations de contrôle de session.

Le mot codec vient de « compression-décompression » (ou « codage-décodage » et désigne un procédé capable de numériser et compresser ou de décompresser un signal, analogique ou numérique. Aujourd’hui, le couple RTP/RTCP, s’utilise systématiquement dans les applications multimédias interactives, pour la téléphonie, la vidéo, les jeux vidéo et même les premiers simulateurs de réalité virtuelle. Ces protocoles applicatifs sont chargés de transporter une information multimédia en temps réel au travers d’un réseau IP. Cependant, ce couple de protocole n’est pas utilisé pour la réservation des ressources réseaux, ni pour fiabiliser les échanges, ni pour garantir les délais de transit puisque certains paquets peuvent être retardés. Le codec numérise et compresse la voix de l’émetteur, ainsi les données numériques sont encapsulées dans des paquets IP et acheminées vers le destinataire. A l’arrivée au destinataire, ce dernier, grâce au même codec décompresse et restitue le son (voir figure 15).

[](https://wikimemoires.net/wp-content/uploads/2011/03/encodage-decodage-voix.jpg)

Figure : Codage et encodage

Dans la communication par VoIP, la voix est traitée de la même manière que les autres données numériques transmises via le réseau Internet. Elle est d’abord captée par le microphone sous forme d’un signal analogique, puis envoyée via le réseau Internet. Ce signal analogique doit être converti en un signal numérique, puis il est ensuite comprimé par un codec. La voix est alors numérisée puis regroupée en paquets de données numériques, prêts à être transportées par le réseau via le protocole IP. L’IP «de l’anglais Internet Protocol» est un protocole spécifique au réseau Internet qui a été développé en 1973 aux USA à des fins militaires. Ce protocole assure la transmission des données numériques en fonction des adresses des réseaux qu’elles incluent.

Pour communiquer en VoIP, les correspondants peuvent utiliser les logiciels spécifiques. Ils ont besoin d’un ordinateur connecté à Internet, de microphones et de haut-parleurs. Ces logiciels permettent de communiquer librement entre deux ordinateurs connectés à Internet, mais donnent également la possibilité d’effectuer un appel payant vers un numéro téléphonique conventionnel. De plus des téléphones traditionnels peuvent également être branché a une passerelle IP ce qui a comme résultat de transformer cet appareil en téléphone VoIP.

* **Les protocoles de VoIP**
* **Protocoles de signalisation**

La signalisation dans un environnement VoIP active et coordonne les différents éléments de cet environnement afin qu’un appel puisse être effectué (et reçu). Cette signalisation consiste en l’échange de messages dans un environnement IP. Le format de ces messages dépend du protocole utilisé.

Ils permettent, entre autres, les fonctions suivantes:

* Ouvrir et fermer une session multimédia (voix, vidéo)
* Enregistrer des terminaux
* **H.323**

Le protocole historique de la VoIP est H322, son apparition (1996) a été une étape important du développement de VoIP. Les principales caractéristiques de H323 sont le suivant :

La communication mise en place est complément indépendante de l’architecture réseau qui l’achemine et de la couche application des terminaux ou du système d’exploitation des IPBX.

Les phases de mise en relation et de déconnexion sont elle aussi indépendantes des terminaux utilisés : H323 fournit les outils nécessaires à la coordination de la communication

H323 définit des standards pour la compression et la décompression d’un flux en temps réel. Jusqu’à la, ces procèdes étaient liés à chaque constructeurs, l’apparition de H323 permet donc à des équipements de constructeurs différents de communiquer entre eux.

Pour garantir la continuité d’une conversation IP ou d’un flux multimédia, H323 propose une gestion de la bande passante, de façon à réserver une bande passante suffisante à chaque communication, en limitant si besoin le nombre de liaison VoIP simultanées une architecture basée sur le protocole H323 s’appuie sur plusieurs éléments :

Les terminaux sont les éléments actifs permettant de capter ou d’émettre un son (téléphone IP, ordinateur équipe d’un client SIP …). Les Gateway (passerelles) sont des éléments chargés d’interconnecter le réseau IP au réseau téléphonique, et plus globalement d’interconnecter des réseaux de différentes natures. La spécificité d’une passerelle est de posséder au moins 2 interfaces : une carte réseau connectée au réseau local de l’entreprise et une interface téléphonique permettant d’accéder au réseau téléphonique (public ou interne à l’entreprise). Exemple : la passerelle permet à un terminal H323 d’appeler un terminal sur un autre réseau. Les gatekeepers (portiers) sont responsables de la translation entre un numéro de téléphone et une adresse IP. Ils gèrent également l’authentification et l’enregistrement des terminaux et peuvent éventuellement offrir un service d’annuaire. Dans tous les cas, la translation d’adresse est basée par un annuaire, local (directement héberge par le gatekeeper) ou centralisé (auquel s’adresse le gatekeeper). D’un point de vue technique, H323 n’est pas un protocole unique : il se décompose en trois protocoles élémentaires, chacun chargé d’une tache spécifique (on retrouve ici un principe de base de la programmation système : un programme ne réalise qu’une seule tache, mais il la réalise correctement et complément) : RAS (Registration, admission and statuts) est utilisé pour communiquer avec un gatekeeper : chercher si un gatekeeper est disponible, s’enregistre auprès de ce gatekeeper et lui soumettre une translation d’adresse.

* **Q931** : c’est le protocole crée initialement pour les réseaux RNIS qui est aussi utilisé par H323 pour établir une conversation entre deux terminaux différents : choix du codec, délai de transmission de la voix … On notera ici qu’un seuil codec est obligatoire en H323 ; le codec G711 (échantillonnage à 64kps, donc d’une qualité relativement peu élevée)

Une communication H323 se déroule en 5 phases  : quatre phases sont obligatoirement effectuée pour chaque appel abouti, et une phase (phase 4) peut être ajoute si l’appel doit être traite de manière particulière : transfert d’appel vers un autre poste vers une messagerie, gestion d’un menu vocal.

* **SIP**

Le protocole SIP (Session Initiation Protocol) a été publié pour la première fois par l’IETF en 1997, par la RFC 2543. Cette dernière un peu vague a été complétée au cours du temps pour finalement arriver en 2002 à la RFC 3261. SIP à l’origine était conçue pour être un protocole simple, mais afin d’offrir le même niveau de service que H323, Le protocole s’est enrichie, le rendant plus complexe, même si le principe de base reste, beaucoup plus simple que H323. Le SIP a longtemps été considéré comme le futur de la ToIP, il est en tout cas un des protocoles majeurs sur le marché.

* **IAX/IAX2**

Le protocole IAX (Inter-Astérisk eXchange) est issu du projet d’IPBX open source et de la communauté « Astérisk », tout comme le SIP, c’est un protocole de ToIP VoIP qui permet de communiquer entre client/serveur ou serveur/serveur.

La différence avec le SIP et le point fort de l’IAX, se base sur l’utilisation d’un [port UDP](http://www.frameip.com/entete-udp/) unique qui est le port « 4569 » qui permet de s’affranchir des [problématiques de NAT](http://www.frameip.com/nat/) dans votre système télécom.

Les fournisseur de service internet présentent également des offres intéressantes de téléphonie sur VoIP et continuent de développer leurs infrastructures numériques. Il est également possible de communiquer par voix sur IP grâce aux téléphones intelligents qui supportent cette technologie. Afin d’assurer la sécurité optimale des communications VoIP, il est recommandé d’opter pour un fournisseur qui garantit le chiffrement des données transférées et la protection à NIP. Il est également conseillé d’installer des logiciels de protection, ainsi qu’un coupe-feu spécifique à la VoIP.

## **III.3 RAPPELLE SUR LA SECURITE**

## **III.3 .1 Introduction**

La continuité de l’activité de l’entreprise appelle celle de son système d’information. Cette continuité ne peut être assurée que par la mise en place d’un moyen de protection apportant un niveau de sécurité adapté aux enjeux spécifiques de l’entreprise.

La sécurité des réseaux est devenue l’un des éléments clés de la continuité des SI (Système d’informations) de l’entreprise.

Comme toute composante critique, le réseau doit faire l’objet d’une politique de sécurité compte de tous les besoins d’accès et é change au réseau d’entreprise:

* accès distants
* échange des mails
* commerce électronique
* interconnexion des tierces parties
* **PRINCIPAUX OBJECTIFS** :

L'intégrité c'est-à-dire garantir que les données sont bien celles que l'on croit être.

La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.

La disponibilité, les services (ordinateurs, réseaux, périphériques, applications…) et les informations (données, fichiers…) doivent être accessibles aux personnes autorisées quand elles en ont besoin.

Le non répudiation, permettant de garantir qu'une transaction ne peut être niée.

L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

* **PROBLEME DE SECURITE :**

Problème dus à des failles notamment dans les protocoles de communication tout information circulant sur internet peut être capturée et enregistre et / ou modifier.

* **PROBLEME DE CONFIDENTIALITE ET D’INTEGRITE:**

Toute personne peut falsifier son adresse IP (spoofing) ce qui engendre une fausse identification.

* **LES DIFFERENTS ASPECTS DE LA SECURITE**

La sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

La sécurité physique, soit *la sécurité au niveau des infrastructures matérielles* : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnel.

La sécurité personnelle : la sensibilisation des utilisateurs aux Problèmes de sécurité.

* **LES CAUSES DE L’INSECURITE :**

On distingue généralement deux types d'insécurités :

L'état actif d'insécurité, c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur)

L'état passif d'insécurité, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose le système.

* **LES MENACES** :

La menace est définie comme étant une violation potentielle de la sécurité. Nous distinguerons les types de menace suivants :

La menace accidentelle : menace d'un dommage non intentionnel envers le SI. Cette menace peut découler d'une catastrophe naturelle (incendie, inondation, tremblement de terre,...), d'une erreur dans l'exploitation du SI (manipulation, saisie, ...) ou de pannes qu'elles soient matérielles ou de logicielles.

La menace intentionnelle ou délibérée : par opposition à la précédente, elle est le fait d'un acte volontaire.

La menace active : menace de modification non autorisée et délibérée de l'état du système. Si elle venait à se concrétiser le SI (Système d’information), ou ses informations, subiraient un dommage ou une altération bien réelle.

La menace passive : menace de divulgation non autorisée des informations, sans que l'état du système soit modifié. Une écoute de ligne ou une lecture de fichier sont des exemples de menaces passives.

* **LES VULNERABILITES :**

Les vulnérabilités: ce sont les failles de sécurité dans un ou plusieurs systèmes. Une vulnérabilité peut se définir comme une faiblesse ou une faille dans les procédures de sécurité, les contrôles administratifs, les contrôles internes d'un système, qui pourrait être exploitée pour obtenir un accès non autorisé à un SI, à un de ses services ou à des informations

Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

* **LES RISQUE :**

Un risque est un danger, un inconvénient plus ou moins probable auquel on est exposé dans un système d'information. Il est généralement admis que le risque est une fonction de la menace, des vulnérabilités et des contre-mesures (ensemble de mesures adoptées pour contrer les menaces et les failles).

* **LES ATTAQUES :**

Les attaques (exploits):elles représentent les moyens d'exploiter une vulnérabilité.

Les informations ou les systèmes d’informations d’une entreprise peuvent subir des dommages de plusieurs façons : certains intentionnels (malveillants), d’autres par accident. Ces événements seront appelés des « attaques ». Il existe quatre catégories principales d’attaque (L’accès, La modification, Le déni de service)

* **LES POLITIQUE DE SECURITE**

La politique de sécurité est l’expression de ces objectifs.

Elle indique l’ensemble des mesures à prendre, des structures à définir et l’organisation à mettre en place afin

D’empêcher (ou tout au moins freiner) la détérioration, l’utilisation anormale ou la pénétration des systèmes et réseaux ;

De détecter toute atteinte, malveillante ou non, à l’intégrité, la disponibilité et la confidentialité des informations. D’intervenir afin de limite les conséquences et, les cas échéant, poursuivre l’auteur du délit.

Il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes : Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.

Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés. Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.

Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

## **I.3.2 Cryptologie**

La cryptologie est un outil pour crypter du message en fonction du besoin des entreprises pour la sécurité des messages entrants et sortants alors la crypto est divisée en deux familles :

* **Cryptanalyse  pour percer les messages secrets.**

L’origine de la cryptographie remonte à 4000 avant J.C en Egypte pharaonique longtemps réservée aux communications militaires et diplomatiques mais depuis s’est largement vulgarisée.

Tous les algorithmes et protocoles inventés avant les années 70, ont été complètement cassées.

On se réfère à cette période en parlant de période de la cryptographie classique ou artisane (art des codes secrets): 4000 ans avant J.C jusqu'en 1975/76.

Dans les années 70, considérées comme le début de l'époque moderne, la cryptographie, devenue la science des codes secrets, s'est développée dans le monde civil surtout avec la prolifération des systèmes de communication et de nouveaux services des années 1990/2000: Internet, Commerce électronique. Cette nouvelle cryptographie est dite moderne par ce qu’entre autres:

Toutes ses branches ont connues une modélisation mathématique plus cohérente

Elle a produit des outils (algorithmes, protocoles,...) qui restent encore robustes malgré le développement des techniques de cryptanalyse. Elle prend en charge presque totalement tous les besoins de sécurité dans un schéma de communication son application dans le monde civil a permis le développement de nouveaux métiers ou services: commerce électronique, e-banking(terme de banque renvoie à deux conceptions.), consultation de données personnelles sur internet.

## **III.3.2.1 Cryptographie**

* **Définitions utiles**

Message clair : Le message originel que Mr Ndiaye veut envoyer à Mme Anne sans que personne d’autre qu’Anne ne puisse le lire

Clé Données (Nombre très grand) utilisé par un [algorithme de cryptage](http://www.netscape.ca/browser/netscape8/help/fr/glossary.html) pour chiffrer et déchiffrer des données

Chiffrer : transformer un message clair en un message codé qui n’est pas compréhensible sans avoir la clé de déchiffrement.

Déchiffrer : retrouver le message original avec la clé de déchiffrement.

Décrypter : retrouver le message original sans la clé de déchiffrement.

Algorithme de cryptage. Algorithme: une procédure bien définie qui:

D'abord prend en entrée une valeur, une donnée (élément ou partie d'un ensemble)

Ensuite exécute une suite finie de règles ou d'opérations (de calculs,...)

Enfin donne un résultat.

NB Il arrive qu'on considère une fonction (application) mathématique comme un algorithme.

Protocole : Description de l’ensemble du système : algorithmes de cryptage et décryptage, choix et utilisation des clés.

Information élément de connaissance: texte, son, image, vidéo,...

Traiter/manipuler une information: lire, écrire/modifier, effacer une information

Canal: moyen de transmission permettant de convoyer une information entre deux partenaires d'une communication; par exemple ligne téléphonique, fibre optique, moyen de communication sans fils.

Espion/adversaire/ennemie/attaquant: entité malveillante cherchant à agir illégalement sur un canal de communication dans le but de nuire: violer la confidentialité des données, intercepter et modifier les données, usurper l'identité d'une entité légitime, etc.

Canal non sûr: canal dans lequel un espion peut réaliser avec succès ses forfaits.

## **A Cryptographie symétrique**

La cryptographie symétrique (ou cryptographie à clé secrète) est la forme la plus ancienne de cryptographie. Ce chiffrement fonctionne en principe avec une clé secrète, bien qu’il existe certains chiffrements symétriques qui n’utilisent pas de clé, comme par exemple le chiffre de César. Dans le cas des chiffrements avec clé, le principe est le suivant : L’émetteur du message chiffre les données grâce à une clé. Cette clé est généralement une chaîne de caractères. Le message est chiffré et sans la clé il est quasi impossible (le niveau d’impossibilité dépend du niveau de protection du chiffrement utilisé ainsi que de la complexité de la clé utilisée) de retrouver le message d’origine. L’émetteur doit donc transmettre la clé aux personnes à qui il désire transmettre le message s’il veut que son message puisse être lu. Un système symétrique est un système construit avec une fonction ou un processus facilement réversible. Généralement on entend par systèmes symétrique les systèmes de chiffrement à clés sécrètes.

Dans un système symétrique, la clé secrète doit être partage entre les entités en communication d’où la nécessite d’avoir un canal sur.

Canal sur c’est se rencontrer, utilise la valise diplomatique et aussi utilise des technique de cryptographie non symétrique.

Maintenant les algorithmes de chiffrement symétrique sont utilisé pour rendre le service de confidentialité et sont compose de deux catégories : les algorithmes de chiffrements par bloc et les algorithmes de chiffrements par flux comme (DES, 3DES, LUCIFER, FEAL, RC4, RC5 …etc.).

Les méthodes ou technique pour utilise les systèmes symétrique sont plusieurs technique mais le plus essentielles sont les suivant Permutation(Transposition) Substitution (Tracer d’une permutation globale)

Chiffrement de Vernam ou One Time Pad(1918) Chiffrement par blocs, Chiffrement séquentiels ou par flux (ou flots).

## **A.1 les avantages et inconvénients Cryptographie symétrique**

Les avantages cryptographie symétrique est les algorithmes symétriques sont rapide (parce qu’ils utilisent de petits entiers et des opérations rapides.

En général, il semble que les algorithmes symétriques sont plus faciles à fabrique (plus nombreux !).

Le seul algorithme dont la sécurité est prouvée est un algorithme symétrique à savoir le chiffrement de Vernam.

## **A.1.1 Chiffrement de Vernam**

Le chiffre de Vernam ou encore l’algorithme à masque jetable est une méthode de chiffrement qui est théoriquement indéchiffrable. Toutefois, pour que cet algorithme fonctionne de façon optimale, les trois contraintes suivantes doivent absolument être respectées :

La clé doit être absolument aléatoire

La clé doit être de la même longueur que l’information à chiffrer

La clé ne doit être utilisée qu’une seule et unique fois (d’où le nom « chiffrement à masque jetable »).

Cet algorithme est une version améliorée des algorithmes de décalage simple (ou mono alphabétique). En effet, il inclut la notion de clé. Il est aussi une version améliorée du chiffrement de Vigenère qui fonctionne de la même façon, à la différence qu’il n’a pas les trois contraintes décrites précédemment, ce qui rend l’algorithme vulnérable.

Plutôt que d’avoir un seul décalage fixe, chaque caractère de la clé définit le décalage du caractère à chiffrer. On parle alors de chiffrement par substitution poly alphabétique. C’est pour cette raison que la clé doit avoir la même taille que le message à chiffrer et donc le chiffrement est réalisé par flot. Ainsi, un caractère n’aura pas la même valeur une fois chiffré, grâce à la clé.

Prenons l’exemple du message « LA\_CRYPTOGRAPHIE » chiffré avec la clé « FRIYL\_FTYBDGZWF\_ ». La première lettre du message à chiffrer est L (douzième lettre de l’alphabet) et la première lettre de la clé est F (sixième lettre de l’alphabet). Cela signifie que la nouvelle valeur de L dans ce cas-là sera R (L(12) + F(6) = R(18)). Il est assez aisé de chiffrer un message en s’aidant d’une matrice contenant les caractères de la clé et du message comme dans le tableau qui suit.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | \_ | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M N** | | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W X** | | **Y** | **Z** |
| \_ | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z |
| **A** | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ |
| **B** | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A |
| **C** | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B |
| **D** | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C |
| **E** | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D |
| **F** | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E |
| **G** | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F |
| **H** | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G |
| **I** | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H |
| **J** | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I |
| **K** | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J |
| **L** | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K |
| **M** | M N | | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L |
| **N** | N | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M |
| **O** | O | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | |
| **P** | P | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O |
| **Q** | Q | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P |
| **R** | R | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q |
| **S** | S | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R |
| **T** | T | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S |
| **U** | U | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T |
| **V** | V | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U |
| **W** | W X | | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V |
| **X** | X | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W |
| **Y** | Y | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | |
| **Z** | Z | \_ | A | B | C | D | E | F | G | H | I | J | K | L | M N | | O | P | Q | R | S | T | U | V | W X | | Y |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |

Tableau  : Matrice de chiffrement de Vernam

Par contre les inconvénients sont confidentialité de la clé secrète problème de partage de la clé à travers un canal sûr et problème de stockage de la clé, Durée de vie des clés assez courte, Peut des services de sécurité sont pris en charge par les systèmes symétrique par exemple : on ne peut déterminer qui entre les deux interlocuteurs légitimes, à chiffre un message.

## **A.2 Méthodes de Chiffrement**

## **A.2 .1 Chiffrement par flux**

Les algorithmes basés sur le principe de chiffrement par flot chiffrent ou déchiffrent un message à la volée. Leur fonctionnement se base sur un générateur de nombres pseudo-aléatoires et un mécanisme de substitution bit à bit. Les algorithmes se basant sur ce principe sont réputés rapides.

## **A.2 .2 Chiffrement par blocs**

Le chiffrement par blocs fonctionne différemment. Au lieu de prendre chaque bit un par un, les messages sont découpés en blocs (la taille des blocs dépend de la clé). Ensuite, chaque bloc est additionné à la clé et un traitement de type permutation, opération XOR ou autre est appliqué à chaque bloc.

## **A.3 Algorithmes**

## **A.3.1 ROT13**

Le chiffrement ROT13 (Rotate by 13 places) est une variante du chiffre de César, précédemment vu dans le chapitre consacré à l’histoire de la cryptographie. C’est un chiffrement à décalage fixe, et comme son nom l’indique, le décalage est de 13 positions. C’est donc un chiffrement par flot. Cela signifie que pour chiffrer ou déchiffrer un message, il faut substituer la lettre de base par celle qui se trouve 13 positions plus loin, comme dans le tableau de correspondance des caractères.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Position dans l'alphabet | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Alphabet | A | B | C | D | E | F | G | H | I | J | K | L | M |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|  |
| Position dans l'alphabet | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Tableau 2 : Chiffrement ROT13

Exemple : Ainsi, le chiffrement du message « La cryptographie » deviendra « Yn pelcgbtencuvr »

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L | A |  | C | R | Y | P | T | O | G | R | A | P | H | I | E |
| Y | N |  | P | E | L | C | G | B | T | E | N | C | U | V | R |

Pour décrypter le message, il suffit de refaire la même opération. En effet, l’alphabet est coupé en deux et contient 26 lettres (donc est un chiffre pair). En additionnant ou en soustrayant de 13 (soit la moitié), le résultat sera le même. Toutefois, la méthode « visuelle » a été présentée.

Mathématiquement parlant, ce qui a été expliqué reviendrai à dire cela (avec l’exemple de « La cryptographie ». La lettre L se trouve en 11ème Position dans l’alphabet. En lui additionnant 13, le résultat deviendra 24, ce qui va donc correspondre à la lettre de l’alphabet située en 24ème position, c’est-à-dire Y. Pour les lettres A et C qui suivent, le même traitement est appliqué. En revanche, pour la lettre R, qui est à la 17ème position dans l’alphabet, si on lui additionne 13, le résultat sera 30, or l’alphabet ne contient que 26 lettres.

Pour combler à ce problème il suffit d’utiliser l’opérateur modulo, qui permettra d’avoir le reste de la division par 26 et donc de retomber sur la bonne lettre.

## **B Cryptographie Asymétrique**

Les crypto systèmes une clé publique se subdivisent en deux catégories : les crypto systèmes déterministes et les crypto systèmes probabilistes. Un chiffrement est déterministes (applications) si un message donner est toujours chiffré de la même manière.

Donc, on a chiffrement déterministe si on parvient construire une application inversible droit (donc injective) et dont l’inverse est difficile à calculer pour eux qui ne connaissent pas la trappe c’est-à-dire qu’il soit une fonction à sens unique avec trappe.

Un chiffrement est probabiliste s’il n’est pas déterministe, plus précisément si la probabilité qu’un message soit chiffré de la même manière est très faible.

Les propriétés recherchées pour un crypto système clé publique :

Etre probabiliste si possible.

Etre simple à comprend et à mettre en œuvre

Etre efficient c’est-à-dire rapide, facile à implémenter sur diffèrent supports, consomme peu de ressource mémoire.

Etre résistant contre toutes les attaques connues :

Avoir une sécurité sémantique c’est-à-dire montre que l’algorithme est cassé et seulement si le problème difficile au quel il est relie, est résolue

Etre adapté de multiples applications (posséder la propriété d’homomorphie, être probabiliste).

On peut citer entre autres :

Un des grands inconvénients de cet algorithme est la taille du chiffre qui est constitué d’entier de même taille que n.

Son principal avant âge est sa sécurité sémantique car c’est un chiffrement bit par bit qui est sûr si le problème de la residousité quadratique est difficile.

La cryptographie est la discipline qui permet de protéger des messages. Si un message est intercepté, il devrait ne pas être compris ou ne pas être déchiffré facilement. Les premières traces de la cryptographie remontent au XVIème siècle avant J.-C. Depuis cette époque, elle n’a fait qu’évoluer. Si à ses débuts il était question de chiffrement symétrique, c’est-à-dire, avec une clé permettant de chiffrer et déchiffrer un message, depuis le milieu des années 70, une nouvelle méthode révolutionnaire de partage de messages est apparue avec des clés publiques : le cryptage asymétrique. Actuellement, ces deux types de cryptage sont utilisés conjointement. Les algorithmes asymétriques pour transmettre des clés de chiffrement et les algorithmes symétriques afin de chiffrer les données à protéger. Ce travail de rappelle de sécurité parle tout d’abord de l’histoire de la cryptographie. Ensuite, il décrit plusieurs algorithmes symétriques et asymétriques, ainsi que leur implémentation.

## **C Cryptographie Hybride**

Tout d’abord, La cryptographie hybride est un ensemble deux solutions de cryptographie asymétrique et la cryptographie symétrique.

Maintenant la Cryptographie asymétrique qui nous offre des garanties de la confidentialité, de l'authenticité, et de l'intégrité, mais c'est un système de chiffrement double, donc lent.

Le système symétrique est plus rapide, mais nous n'avons pas toujours l'occasion de transmettre la clé secrète par un moyen de transmission sécurisé.

Alors la cryptographie hybride qui nous donner les deux possibilités et leur avantage des deux systèmes :

La rapidité d’un système symétrique grâce à une clé secrète valide le temps du transfert de l’information, ou le temps d’une session.

La possibilité de transmettre la clé secrète par une crypto asymétrique.

En effet, un chiffrement hybride est rapide mais ne présente pas des faiblesses au niveau de la clé comme un chiffrement à clé publique. Mais un algorithme symétrique oblige à conserver la clé sur le disque dur ou sur une clé USB, C’est qui implique un risque qu’un pirate s’infiltre dans la mémoire de l’ordinateur ou du support USB pour avoir accès à la clé.

La plupart des systèmes hybrides fonctionnent de la manière suivant. Une clé aléatoire est générée pour l’algorithme symétrique. Elle varie généralement entre 128, 256, 512 bits selon les algorithmes. Les destinataires générés alors une clé publique est une clé privée, La clé publique sert à chiffrer la clé aléatoire. Réellement que ce dernière est courte, la chiffrer est rapide, alors que chiffrer le message avec un algorithme asymétrique aurait été bien plus long. Il ne reste plus qu’à envoyer les messages chiffré accompagné de la clé chiffrer correspondante. Le destinataire utilise alors sa clé privé pour déchiffrer la clé aléatoire. Avec cette dernière, il retrouve le message via un déchiffrement symétrique.

La plus classique de ces logiciels sont GnuPG (GNU Privacy Guard), dont le logo est ci-contre, et PGP (Pretty Good Privacy). Ces logiciels sont notamment très utilise pour sécuriser les envois des courriels. PGP depuis longtemps à gagne d’une grand popularité en raison de son efficacité et de son développeur, Philip Zimmerman. GnuPG s’est quant à lui fait une réputation en sa qualité d’algorithme stable et libre, inclus dans les systèmes d’exploitation libre. Il a également été intégré dans Mozilla Firefox, Thunderbird et bien d’autres logiciels libres.

## **III.3.2.2 Cryptanalyse**

Il s’agit de l’étude des mécanismes théoriques ou techniques visant à briser (casser) un algorithme de chiffrement, c’est-à-dire le fait de retrouver le message M à partir de C, sans connaître la clé K a priori. Dans certains cas, il s’agira également de retrouver cette clé K. On parlera d’attaque cryptanalytique.

Il en existe 4 grands types, chacun pouvant utiliser différentes techniques. Cette partie présentera ensuite quelques attaques souvent évoquées dans la littérature spécialisée dans le domaine de la cryptologie.

* **Les quatre attaques crytanalytiques**
* **Attaques sur le texte chiffre uniquement**

A partir d’un texte chiffré, on recherche le texte clair et/ou la clé. On procède par analyse de fréquence des lettres utilisées dans le texte chiffré. Cette technique ne fonctionne que pour la plupart des chiffrements classiques basiques, les seuls permettant l’utilisation de l’analyse de fréquence. On peut aussi également procéder par force brute pour briser de tels chiffrements.

* **Attaque à texte clair connu**

Etant donné un texte chiffré et un fragment de texte clair associé, on recherche le texte clair restant et/ou la clé. On utilise la technique dite de la cryptanalyse linéaire (1993) présentée rapidement dans la section suivante.

* **Attaque sur un texte clair sélectionné**

Etant donné la capacité de chiffrer un fragment de texte clair choisi arbitrairement, on recherche la clé par la technique de la cryptanalyse différentielle.

* **Attaque sur le texte chiffré uniquement**

Etant donné la capacité de déchiffrer un fragment de texte chiffré choisi arbitrairement, on recherche la clé.

* **Quelques autres techniques**
* **La force brute**

Le principe est ici de tester toutes les clés possibles de manière exhaustive. La limite maximale est donnée par T et N avec T représentant la taille de l’alphabet, N est la taille de la clé. Par exemple, pour une clé de 128 bits,

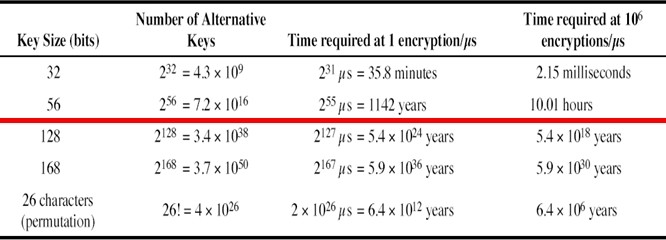
Il  y a 2 128 clés possibles. Cette technique n’est efficace que pour des textes

Figure  : force brute

Figure 16 : Force brute

Chiffrés avec une clé relativement courte. Sur la figure 13.1, la ligne rouge

Indique la limite actuelle conseillée. Une clé de 56 bits n’est plus à utiliser aujourd’hui si l’objectif premier est la confidentialité. Les algorithmes symétriques actuels utilisent en standard des clés variant entre 112 (3DES) et 256 bits (AES).

* **Attaque par dictionnaire**

Lorsque la clé est un mot (p.ex. un mot de passe), on peut tenter de court-circuiter la Force Brute. Le principe est ici d’utiliser un recueil de mots possibles (le dictionnaire), et de tester tous les mots de ce dictionnaire. Attention à bien distinguer les deux attaques : on teste tous les mots du dictionnaire mais celui-ci ne contient pas toutes les possibilités. Par exemple, on pourra y trouver "unie", "unir" et "unis", mais pas "unih" (pour autant qu’il s’agisse d’un dictionnaire de mots existant dans la langue française).

* **Analyse de fréquence**

Il faut toutefois que la taille de K soit inférieure à la taille de C, au risque de ne pas permettre l’unicité de la solution. Il faut aussi que le texte C soit suffisamment long pour être représentatif. Et enfin que l’algorithme utilisé soit une substitution simple (mono- ou poly alphabétique).

* **Cryptanalyse différentielle**

Il s’agit de l’étude (modélisation) des transformations subies par le message durant son passage dans l’algorithme de chiffrement. Le principe est de modéliser ce qu’une modification en entrée induira sur le résultat de l’algorithme.

* **Cryptanalyse linéaire**

Le but est d’effectuer une approximation linéaire de l’algorithme de chiffrement. Il n’y a ici aucune possibilité de choisir le texte clair à chiffrer, on dispose tout au plus d’un ensemble de couples (M, C).

Mi1 ⊕ Mi2 ⊕ . . . ⊕ Miu ⊕ Cj1 ⊕ Cj2 ⊕ . . . ⊕ Cjv = 0

avec Mi représentant le ieme bit de M = [M1, M2, . . . Mu] et Cj représentant le jeme bit de C = [C1, C2, . . . Cv]. Si c’est le cas, et selon la probabilité d’occurrence de l’expression, on peut déduire des faiblesses de l’algorithme (en termes de transformations aléatoires).

Définissons encore 2 termes :

Un cryptosystème est dit inconditionnellement sûr si le texte chiffré ne contient pas assez d’information pour retrouver le texte clair correspondant, peu importe la longueur du texte chiffré à disposition.

Un système est dit informatiquement sûr. Si le coût nécessaire au décryptement excède la valeur intrinsèque de l’information. Si le coût nécessaire au décryptement excède la durée de vie utile (durée de validité) de l’information Dans la pratique, on trouve très peu de systèmes du premier type. Beaucoup plus du second. Signalons enfin que la cryptanalyse et la cryptographie ont évolué conjointement. Comme dans de nombreux autres domaines, le jeu du chat et de la souris est bel et bien réel, même si la finalité de la cryptanalyse est souvent d’aider à la conception de meilleurs algorithmes.

## **III.3.2 Gestion des certificats et système authentification**

## **III.3.2.1 Gestion des Certificats**

* **Emission de certificats**

L'ensemble des standards et des services facilitant l'utilisation de la cryptographie à clef publique et des certificats X.509 v3 (Une norme spécifiant les formats pour les certificats à clé publique, les listes de révocation de certificat, les attributs de certificat) dans un environnement réseau est appelé *public key infrastructure* (PKI ou infrastructure à clef publique). La gestion de PKI est un sujet complexe qui dépasse le cadre de c’est document. Les sections qui suivent présentent quelques-uns des problèmes liés à la gestion de certificats qu'on retrouve dans les produits Red Hat.

De même, les différentes autorités de certification ont différentes procédures d'émission des différents types de certificats. Dans certains cas, la seule condition pourra être votre adresse électronique. Dans d'autres cas, un nom d'utilisateur et un mot de passe vous seront demandés. À l'autre bout de l'échelle, pour les certificats identifiants des personnes pouvant prendre des décisions importantes, le processus d'émission pourra requérir des documents notariés, une enquête de fond et un entretien personnel.

Selon les politiques de l'organisation, le processus d'émission des certificats peut soit être complètement transparent pour l'utilisateur, soit exiger une participation significative de l'utilisateur et des procédures complexes. En général, l'émission de certificats doit être flexible, ainsi les organisations peuvent les adapter à leurs besoins.

* **Certificats et annuaire de LDAP**

Le *Lightweight Directory Access Protocol* (LDAP) d'accès aux services d'annuaire propose une grande flexibilité pour la gestion des certificats d'une organisation. Les administrateurs systèmes peuvent stocker la plupart des informations requises par la gestion des certificats dans un annuaire compatible LDAP. Par exemple, une autorité de certification peut utiliser les informations contenues dans un annuaire pour préremplir un certificat avec les informations concernant un nouvel employé. L'autorité de certification peut niveler les informations de l'annuaire de nombreuses manières pour émettre les certificats un à un ou en groupe, en utilisant un éventail des différentes techniques d'identification en fonction de la politique de sécurité d'une organisation donnée. Les autres routines des tâches de gestion, telles que la gestion de clefs, le renouvellement ou la révocation de certificats, peuvent être partiellement ou pleinement automatisées à l'aide de l'annuaire. Les informations stockées dans l'annuaire peuvent également être utilisées en association avec les certificats pour contrôler l'accès aux différentes ressources disponibles sur un réseau en fonction des utilisateurs ou des groupes d'utilisateurs. L'émission de certificats et toutes les tâches de gestion des certificats font intégralement parties de la gestion des utilisateurs et des groupes d'utilisateurs. En général, les services d'annuaires performants sont une brique essentielle de toute stratégie de gestion des certificats. Red Hat*Directory Server* est pleinement intégré à Red Hat*Certificate System* afin de fournir une solution de gestion des certificats complète.

* **Gestion des clefs**

Avant d'émettre un certificat, la clef publique qu'il contient et la clef privée correspondante doivent être générées. Il est parfois plus utile d'émettre, pour une unique personne, un certificat et une paire de clefs pour les opérations de signature, et un second certificat et une paire de clefs pour les opérations de chiffrement. Séparer les certificats de signature et de chiffrement permet de conserver la clef de signature uniquement sur une machine locale, assurant ainsi un non répudiation maximale, et de sauvegarder la clef privée de chiffrement dans un endroit centralisé où elle peut être récupérée au cas où l'utilisateur perdrait la clef originale ou quitterait l'entreprise. Les clefs peuvent être générées par un logiciel client ou générées de façon centralisée par l'autorité de certification puis distribuées aux utilisateurs via un annuaire LDAP. Il y a plusieurs options entrant dans le choix du type de génération des clefs, locale et centralisée. Par exemple, la génération locale des clefs assure un non répudiation maximale, mais elle peut induire une plus grande participation de l'utilisateur lors des étapes d'émission. La flexibilité des possibilités dans la gestion des clefs est essentielle pour la plupart des organisations.

Le recouvrement de clef, ou la capacité de récupérer une sauvegarde des clefs de chiffrement suivant des conditions bien définies, peut être un point important de la gestion des certificats (selon l'utilisation des certificats par l'organisation). Les schémas de recouvrement de clefs mettent habituellement en œuvre un mécanisme de type *m sur n* : par exemple, *m* dirigeants d'une organisation sur *n* doivent donner leur accord, chacun contribuant à l'aide d'un code (ou d'une clef) personnel et spécial, avant que la clef d'une personne en particulier puisse être récupérée. Ce type de mécanisme assure que plusieurs personnes autorisées doivent donner leur accord avant qu'une clef de chiffrement puisse être récupérée.

* **Renouvellement et révocation de certificats**

Pour l’utilisation des certificats spécifie une période de temps pendant laquelle qu’il est valide. Les tentatives d'utilisation d'un certificat avant ou après la période de validité échoueront. Par conséquent, les mécanismes de gestion du renouvellement des certificats sont essentiels dans toute stratégie de gestion des certificats. Par exemple, un administrateur voudra être notifié automatiquement lorsqu'un certificat s'apprête à expirer, afin de compléter le processus de renouvellement approprié pendant le temps restant, sans gêner le détenteur du certificat. Le processus de renouvellement peut impliquer la réutilisation de la même paire de clefs publiques ou d'une nouvelle paire.

La révocation des certificats peut être gérée de différentes manières. Pour certaines organisations, il peut être suffisant de paramétrer les serveurs afin que le processus d'authentification inclue la vérification de la présence du certificat présenté dans l'annuaire. Lorsqu'un administrateur révoque un certificat, le certificat peut être automatiquement supprimé de l'annuaire et ainsi toutes les tentatives d'authentification échoueront, même si le certificat reste valide dans tous les autres domaines. Une autre approche implique la publication d'une *Certificates Revocation List* (CRL ou liste de certificats révoqués) dans l'annuaire à intervalles réguliers et la vérification de cette liste lors du processus d'authentification. Pour d'autres organisations, il sera peut-être préférable de vérifier directement l'autorité de certification émettrice chaque fois qu'un certificat est présenté pour une authentification. Ce processus est parfois appelé vérification de l'état d'un certificat en temps réel.

* **Autorités d'enregistrement**

Les interactions entre les entités identifiées par des certificats (parfois appelées entités finales) et les autorités de certifications (AC, pour *Certificates Authority*) sont un élément essentiel de la gestion des certificats. Ces interactions incluent les opérations telles que l'enregistrement de la certification, le recouvrement, le renouvellement ou la révocation de certificats, et la sauvegarde et le recouvrement de clefs. En général, une AC (Autorité de certification) doit être en mesure d'authentifier les identités des entités finales avant de répondre à leurs requêtes. De plus, certaines requêtes doivent être approuvées par un administrateur autorisé ou un gestionnaire afin d'aboutir.

## **III.3.2.2 Système Authentification**

* **Certificat identifiant une personne ou une entité**

Un certificat est un document électronique utilisé pour identifier un individu, un serveur, une entreprise ou toute autre entité et pour associer une clef publique à cette identité. Tout comme un permis de conduire, un passeport, ou tout autre moyen d'identification personnelle couramment utilisé, un certificat fournit généralement une preuve reconnue de l'identité de la personne.

Les certificats fonctionnent sur les mêmes principes que ces différents documents d'identité. Les autorités de certification (AC ou CA) sont des entités qui valident les identités et émettent les certificats. Elles peuvent être des tierces-parties indépendantes ou des organisations possédant leur propre serveur d'émission de certificats (tel que *Red Hat Certificate System*). Les méthodes utilisées pour valider une identité varient selon les politiques d'émission d'une AC (*Certificates Authority*) donnée tout comme les méthodes de validation des autres formulaires d'identification varient selon les organismes d'émission et leurs domaines d'application.

En général, avant d'émettre un certificat, une AC (*Certificates Authority*) doit utiliser ses procédures de vérification publiées pour un type de certificat afin de s'assurer que l'entité demandant le certificat est bien celle qu'elle prétend être.

Le certificat émis par l'AC lie une clef publique particulière au nom de l'entité qu'il identifie (tel qu'un nom d'employé ou de serveur). Les certificats aident à prévenir l'utilisation de fausses clefs publiques pour l'usurpation d'identité. Seule la clef publique certifiée dans le certificat fonctionnera avec la clef privée correspondante possédée par l'entité identifiée par le certificat. En plus de la clef publique, un certificat contient toujours le nom de l'entité qu'il identifie, une date d'expiration, le nom de son AC émettrice, un numéro de série et d'éventuelles autres informations utiles. Plus important, un certificat contient toujours la signature numérique de l'AC émettrice. La signature numérique de l'AC émettrice permet au certificat de fonctionner comme une *lettre d'introduction* pour les utilisateurs qui connaissent l'AC et lui font confiance mais qui ne connaissent pas l'entité identifiée par le certificat.

* **L'authentification confirme une identité**

L'authentification est le processus de confirmation d'une identité. Dans le contexte d'interactions entre les réseaux, l'authentification comporte l'identification confiante d'une partie par une autre. L'authentification sur les réseaux peut avoir plusieurs formes. Les certificats sont un moyen d'authentification. Les interactions entre les réseaux se font généralement entre un client, tel que le navigateur d'un ordinateur personnel, et un serveur, tel que le matériel et le logiciel hébergeant un site Web. L'authentification cliente se réfère à l'identification confiante d'un client par un serveur, c'est-à-dire, l'identification de la personne supposée utiliser le logiciel client. L'authentification serveur se réfère à l'identification confiante d'un serveur par le client, c'est-à-dire, l'identification de l'organisation supposée être responsable du serveur à une adresse réseau particulière.

Les authentifications cliente et serveur ne sont pas les seules formes d'authentification permises par les certificats. Par exemple, la signature numérique d'un courriel combinée au certificat identifiant l'expéditeur fournit une forte preuve que la personne identifiée par le certificat a bien envoyé le message. De même, une signature numérique dans un formulaire HTML combinée à un certificat identifiant le signataire peut fournir une preuve, après coup, que la personne identifiée par le certificat est d'accord avec le contenu du formulaire. En plus de l'authentification, la signature numérique assure, dans les deux cas, un degré de non répudiation, c'est-à-dire que la signature numérique rend difficile la négation ultérieure par le signataire des informations présentes dans le message électronique ou le formulaire.

L'authentification cliente est un élément essentiel de la sécurité réseau, sur les intranets ou les extranets. Les sections qui suivent présentes deux formes d'authentification cliente :

Authentification basée sur un mot de passe : Presque tous les serveurs permettent l'authentification cliente à l'aide d'un nom, ou pseudos, et d'un mot de passe. Par exemple, un serveur pour demander à un utilisateur de fournir un nom et un mot de passe avant de donner des droits d'accès à certaines parties du serveur. Le serveur maintient une liste des noms et des mots de passe ; si un nom particulier est dans cette liste, et que l'utilisateur fournit le bon mot de passe, le serveur donne des droits d'accès.

* **Authentification basée sur un certificat**

L'authentification basée sur les certificats est une étape du protocole SSL. Le client signe numériquement des données générées aléatoirement et envoie à la fois ces données signées et le certificat sur le réseau. Le serveur utilise les techniques de cryptographie à clef publique pour valider la signature et confirmer la validité du certificat.

* **L'authentification par mot de passe**

La figure 4 montre les étapes basiques mise en œuvre dans l'authentification d'un client à l'aide d'un nom et d'un mot de passe. Cette figure suppose que :

* L'utilisateur a déjà décidé de faire confiance au serveur, sans authentification ou sur la base d'une authentification de serveur via SSL.
* L'utilisateur a demandé une ressource contrôlée par le serveur.
* Le serveur demande une authentification client avant de donner les droits d'accès aux ressources demandées.

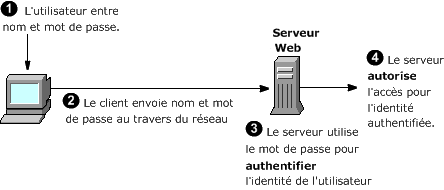


Figure  : Authentifier nom et mot passe

Avec cet arrangement, l'utilisateur doit fournir un mot de passe pour chaque serveur, et l'administrateur doit conserver les noms et les mots de passe de chaque utilisateur, généralement sur des serveurs distincts. Une implémentation propre ne mémorise pas les mots de passe en texte simple. À la place, il concatène le mot de passe avec une valeur aléatoire propre à chaque utilisateur (également appelée « salt » c’est un film qui est sortie vers 19 juillet 2010 à hollywood) et mémorise la valeur hachée du résultat avec le « salt ». Ceci rend plus difficile des attaques de force brute. Comme expliqué dans la section suivante, un des avantages de l'authentification par certificat est qu'elle peut être utilisée pour remplacer les trois premières étapes décrites à la figure 4 avec un mécanisme qui permet à l'utilisateur de fournir un seul mot de passe (qui n'est pas transmis à travers le réseau) et permet à l'administrateur de centraliser le contrôle de l'authentification des utilisateurs.

* **L'authentification par certificat**

La figure 5 décrit le fonctionnement d'une authentification client à l'aide des certificats et du protocole SSL. Pour authentifier un utilisateur auprès d'un serveur, Le client signe numériquement des données générées aléatoirement et envoie à la fois ces données signées et le certificat sur le réseau. Pour les besoins de cette discussion, la signature numérique associée aux données signées peut être considérée comme une preuve fournie par le client au serveur. Le serveur authentifie l'identité de l'utilisateur en se basant sur la force de cette preuve. Comme pour la figure 4, la figure 5 suppose que l'utilisateur a déjà décidé de faire confiance au serveur et qu'il a demandé une ressource, et que le serveur a demandé une authentification client lors du processus d'évaluation des droits à accéder à la ressource demandée.

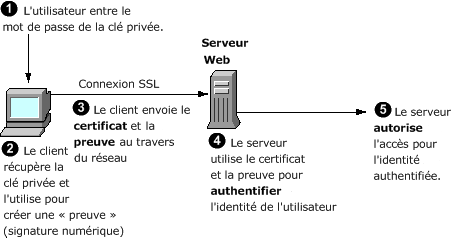


Figure  : Authentifier par SSL

Contrairement au processus décrit à la figure 4, celui de la figure 5 nécessite d'utiliser SSL. La figure 5 suppose également que le client possède un certificat valide qui peut être utilisé pour l'identifier auprès du serveur. L'authentification par certificat est généralement considérée comme préférable à l'authentification par mot de passe car elle est basée sur ce que l'utilisateur a (la clef privée) aussi bien que sur ce que l'utilisateur sait (le mot de passe qui protège cette clef privée). Cependant, il est important de remarquer que ces deux affirmations ne sont vraies que si aucune personne non autorisée n'a accès à l'ordinateur de l'utilisateur ou a son mot de passe, si le mot de passe de la base de données des clefs privées du logiciel client a été défini, et si le logiciel est paramétré pour demander le mot de passe à intervalles raisonnablement fréquents.

Ni l'authentification par mot de passe, ni l'authentification par certificat ne répondent aux questions de sécurité soulevées par l'accès physique à l'ordinateur d'un individu ou à ses mots de passe. La cryptographie à clef publique peut uniquement vérifier qu'une clef privée utilisée pour signer des données, correspond à la clef publique présente dans un certificat. Il est de la responsabilité de l'utilisateur de protéger physiquement son ordinateur et de conserver secret le mot de passe de sa clef privée.

**Voici les étapes décrites dans la figure 18 :**

* Le logiciel client, tel que le navigateur, maintient une base de données des clefs privées correspondantes aux clefs publiques publiées avec tous les certificats émis pour ce client. Le client demande le mot de passe de cette base de données la première fois qu'il a besoin d'y accéder lors d'une session donnée par exemple, la première fois que l'utilisateur essaie d'accéder à un serveur SSL qui requiert une authentification par certificat. Après avoir renseigné une première fois ce mot de passe, l'utilisateur n'en a plus besoin pour la durée de la session, même en accédant à d'autres serveurs SSL.
* Le client débloque la base de données des clefs privées, récupère la clef privée du certificat de l'utilisateur et utilise cette clef privée pour signer numériquement des données générées aléatoirement dans ce but en se basant sur des entrées du client et du serveur. Ces données et la signature numérique constituent une « preuve » de la validité de la clef privée. La signature numérique peut uniquement être créée avec la clef privée et peut être validée par la clef publique associée aux données signées, ce qui est réservé à la session SSL.
* Le client envoie le certificat de l'utilisateur et la *preuve* (les données générées aléatoirement signées numériquement) par le réseau.
* Le serveur utilise le certificat et la *preuve* pour authentifier l'identité de l'utilisateur (pour plus de détails sur ce fonctionnement, voir « [Introduction à SSL](https://developer.mozilla.org/fr/Introduction_%C3%A0_SSL) »).
* À ce moment, le serveur peut éventuellement exécuter des tâches d'authentification supplémentaires, comme vérifier si le certificat présenté par le client est stocké dans l'entrée de l'utilisateur d'un annuaire LDAP. Le serveur continu alors à évaluer si l’utilisateur identifié est autorisé ou non à accéder à la ressource demandée. Ce processus d'évaluation peut employer une variété de mécanismes standards d'autorisation, en utilisant éventuellement des informations présentes dans un annuaire LDAP, des bases de données d'entreprises, etc. Si le résultat de l'évaluation est positif, le serveur autorise le client à accéder à la ressource demandée.

Comme on peut le voir en comparant les figures 4 et 5, les certificats remplacent la portion de l'authentification correspondant à l'interaction entre le client et le serveur. Plutôt que de demander à l'utilisateur d'envoyer des mots de passe par le réseau à longueur de journée, l'ouverture de session unique demande une seule fois à l'utilisateur de saisir son mot de passe de base de données de clefs privée, sans l'envoyer par le réseau. Pour la suite de la session, le client présente le certificat de l'utilisateur pour authentifier l'utilisateur auprès de chaque serveur auquel il se connecte. Les mécanismes d'autorisation existants basés sur l'authentification de l'identité du l'utilisateur ne sont pas concernés.

* **Types de certificats**

Cinq types de certificats sont couramment utilisés avec les produits Red Hat :

* **Certificats de client SSL** : Utilisés pour identifier des clients auprès de serveurs via SSL (authentification client). Généralement, l'identité du client est présumée être la même que celle d'un être humain, tel qu'un employé dans une entreprise. Pour une description de la façon dont les certificats d'un client SSL sont utilisés pour l'authentification client. Les certificats d'un client SSL peuvent également être utilisés pour la signature de formulaires et comme composante d'une solution de l'ouverture de session unique. Par exemple une banque donne un certificat client SSL à l'un de ses usagers qui lui permet de s'identifier auprès du serveur de la banque et d'accéder à ses comptes. Une compagnie peut donner un certificat client SSL à l'un de ses nouveaux employés qui lui permet de s'identifier auprès du serveur de l'entreprise et d'obtenir accès aux ressources disponibles sur ce serveur.
* **Certificats de serveur SSL :** Utilisé pour identifier les serveurs auprès des clients via SSL (authentification serveur). L'authentification serveur peut être utilisée avec ou sans authentification client. L'authentification serveur est obligatoire lors de l'établissement d'une connexion SSL chiffrée. Par exemple les sites internet de commerce électronique (communément appelé e-commerce) supportent habituellement l'authentification serveur par certificat, au minimum, pour établir une session SSL chiffrée et assure les clients qu'ils traitent avec un site identifié comme étant celui d'une entreprise donnée. La session SSL assure que les informations personnelles renseignées par le client et transmises par le réseau, telles que son numéro de carte de crédit, ne seront pas aisément interceptées.
* **Certificats S/MIME** : Utilisés pour signer et chiffrer les courriels. Comme pour les certificats client SSL, l'identité du client est généralement présumé être la même que celle d'un être humain, tel qu'un employé d'une entreprise. Un certificat unique peut être utilisé comme certificat S/MIME et comme certificat SSL. Les certificats S/MIME peuvent également être utilisés pour la signature de formulaires et comme composante d'une solution de l'ouverture de session unique. Comme le exemple suivant une entreprise déploie des certificats combinés S/MIME et SSL dans l'unique but d'authentifier l'identité des employés, permettant ainsi la signature de messages et l'authentification de client SSL, mais pas le chiffrage des messages. Une autre entreprise émet des certificats S/MIME uniquement dans le but de signer et de chiffrer les messages de natures financière ou légale qu'elle envoie.
* **Certificats d'AC :** Utilisés pour identifier les autorités de certification (AC). Les logiciels client et serveur utilisent les certificats d'AC pour déterminer quelles autres certifications peuvent être de confiance. Comme exemple les certificats d'AC stockés dans communicateur déterminent quels autres certificats peuvent être utilisés pour l'authentification. Un administrateur peut implémenter certains aspects de la politique de sécurité de son entreprise en contrôlant les certificats d'AC stockés dans les communicateurs de chaque utilisateur.
* **Protocole SSL :** Le protocole *Secure Sockets Layer* (SSL) est un ensemble de règles gouvernant l'authentification serveur, l'authentification client et les communications encryptées entre des serveurs et des clients. SSL est largement utilisé sur Internet, particulièrement pour les interactions mettant en œuvre l'échange d'informations confidentielles telles que les numéros de cartes de crédit. SSL requiert un certificat SSL serveur, au minimum. Comme partie du processus de négociation, le serveur présente son certificat au client afin d'authentifier son identité. Le processus d'authentification utilise le chiffrement par clef privée et les signatures numériques pour confirmer que ce serveur est bien celui-ci qu'il prétend être. Une fois le serveur authentifié, le client et le serveur utilisent des techniques de chiffrement à clefs symétriques, ce qui est rapide, pour chiffrer toutes les informations qu'ils échangent pour le reste de la session et pour détecter toutes tentatives d'altération des données qui peuvent arriver. Les serveurs peuvent éventuellement être configurés pour demander l'authentification client aussi bien que l'authentification serveur. Dans ce cas, après le succès de l'authentification serveur, le client doit à son tour présenter son certificat au serveur afin d'authentifier son identité avant qu'une connexion SSL ne puisse s'établir.

Par conclusion, la certification électronique des clés publiques et des données associées des individus et des systèmes est une technique devenue de plus en plus indispensable en informatique, notamment du fait de l’expansion d’Internet et de la dématérialisation des documents. Tout serveur informatique, désirant communiquer de façon sécurisée avec des utilisateurs, utilise aujourd’hui le protocole SSL/TLS qui exige de posséder un certificat électronique.

Il est donc important pour les entreprises et les organisations de s’appuyer sur des infrastructures de gestion de clés (IGC), qui sont gérées soit directement, soit par des prestataires de services de certification électronique (PSCE). Gérer sa propre IGC est hors de portée des PME à cause de son coût ; celles-ci auront avantage à faire appel à des PSCE.

Des PSCE ainsi que des éditeurs de progiciels d’IGC existent depuis longtemps. La standardisation autour du standard PKIX de l’IETF devrait faciliter l’interopérabilité des différentes installations de ces infrastructures.

La généralisation des cartes à puce et des clés USB comme moyens de conservation des certificats et de leur clé privée, pour l’authentification, la signature et le paiement, augmentera le niveau de sécurité de l’authentification et, en même temps, nécessitera de mettre en œuvre de telles infrastructures.

La signature électronique et la sécurité associée pourront être mises à la disposition de tous dès que la carte nationale d’identité électronique verra le jour.

# Chapitre IV : Etudes Comparatives et le choix de les solutions

## **Introduction :**

Les plateformes de Voip (Voice Over Internet Protocol) avec la banalisation des réseaux hauts débit le nombre des applications possibles à considérablement augmenté. Le développement de la VoIPa entraîné les concepteurs de plates-formes de programmation à développer des API (Application Programming Interface) spécifiques à la voix sur IP. L’intégration de nouveaux besoins dans une plate-forme de développement permet d’attirer les concepteurs de logiciels qui doivent intégrer des fonctions de voix sur IP dans leurs applications.

## **IV.1 Etudes comparatives**

## **IV.1.1 Logiciels Propriétaires de la VoIP**

Les grands équipementiers de réseaux de télécommunications et informatique ainsi que divers éditeurs de logiciels proposent des solutions de téléphonie ou Voice sur IP basées sur leurs propres technologies, pour divers segments de marché(entreprises, opérateurs):

* **3CX**: logiciel propriétaire, protocole propriétaire
* **EyeP Communicator**: softphone commercial avec protocole standard ouvert SIP par eyeP Media
* **Gizmo Project**: logiciel propriétaire, protocole standard ouvert SIP
* **Google Talk**: logiciel propriétaire, protocole standard ouvert Jabber/Jingle
* **Microsoft** **NetMeeting** (abandonné): logiciel propriétaire, protocole standard ouvert H.323
* **Skype**: logiciel propriétaire, protocole propriétaire
* **Teamspeak** (audioconférence): logiciel propriétaire, protocole propriétaire.
* **Windows Live Messenge**r: logiciel propriétaire, protocole propriétaire
* **Yahoo! Messenger**: logiciel propriétaire, protocole propriétaire
* **DeskCallEVO**: logiciel propriétaire, protocole propriétaire

La Voix sur IP qui est proposée comme open source dans son domaine alors que certaines entreprises créent des applications basées la même de la solution asterisk ou permettent de communiquer ces logiciels ou utilisateurs qui rendent cette solution payant, Alors que asterisk propose la même chose mais gratuitement.

## **IV.1.2 Logiciels libres de la VoIP**

La désignation Open Source (Code source libre en français) s’applique aux logiciels dont la licence respecte des critères précisément établis par l’Open Source Initiative. Les principaux critères à respect sont :

* La libre distribution
* Un code source disponible
* Les travaux dérive possible

Pour les logiciels libre on va citez quelques logiciels open source et les plus populaires de la Voip.

* **IM :** Au niveau du bit IM est un client instantané bloqué, de croix-plate-forme de transmission de messages écrit utilisant des wxWidgets et est disponible pour Windows, Mac OS X et Linux. Il vient dans deux saveurs, personnel et professionnel. La version personnelle est libre mais limitée à utilisation personnelle/à la maison ; la version professionnelle fournit les réseaux IM privés pour des organismes de corporation, sans but lucratif et scolaires**.**
* **Brosix :** est un Instant Messenger puissant et facile à utiliser approprié aux entreprises et des individus qui cherchent à améliorer des communications, la productivité d'affaires et des rapports avec des associés et des clients. L'ensemble de Brosix de dispositifs riche satisfait la demande croissante d'affaires de la transmission de messages et de la collaboration instantanées bloquées.
* **X-Lite :** est un téléphone mou de VoIP de freeware de propriété industrielle qui emploie le protocole de déclenchement de session. X-Lite est développé par CounterPath. x-Lite soutient SRTP et bientôt ZRTP.  
  Il y a actuellement deux dégagements importants de X-Lite avec les interfaces radicalement différentes. X-Lite 2.0 pour le Mac et le Linux, qui emploie la vieille X-Pro base de code, et X-Lite 3.0 pour Windows qui emploie la base de code d'eyeBeam. X-Lite 2.0 est audio seulement. X-Lite 3.0 a l'acoustique, la vidéo, et la transmission de messages instantanée aussi bien qu'être présence-capable.
* **OpenH323**: Le projet OpenH323 vise à créer une exécution complète et interopérable du protocole de système de téléconférences d'ITU-T H.323 qui peut être employé par les réalisateurs personnels et par les utilisateurs commerciaux sans frais. Nous présentons dans le tableau ci-dessous les principales plate-formes open source utilisées dans la mise en œuvre de la VoIP:

|  |  |  |  |
| --- | --- | --- | --- |
| **Logiciels** | **Système d’exploitation** | **Flux** | **Protocole** |
| **Asterisk** | **Linux, Mac os** | **audio, vidéo** | **SIP, H.323, IAX** |
| **SFLPhone** | **Linux** | **audio, vidéo** | **SIP, IAX** |
| **Ekiga** | **Linux, Windows** | **audio, vidéo, chat** | **SIP, H.323** |
| **Jabbin** | **Linux, Windows** | **audio, chat** | **Jabber** |
| **KPhone** | **Linux** | **audio, vidéo, chat** | **SIP** |
| **Linphone** | **Linux, Windows** | **audio, vidéo, chat** | **SIP** |
| **SIP Communicator** | **Linux, Windows, Mac OS X** | **audio, vidéo, chat** | **SIP, Jabber** |
| **Mumble** | **Linux, Windows** | **audio** |  |
| **Twinkle** | **Linux** | **audio** | **SIP, IAX** |
| **QuteCom** | **Linux, Windows, Mac OS X** | **audio, vidéo, chat** | **SIP, Jabber** |

Tableau  : les logiciels open source de la Voip

## **IV.2 Choix de la solution**

## **IV.2.1 Choix d’Asterisk**

ASTERISK est une solution Fiable, libre et robuste, ASTERISK est sans doute la première solution open source de la VoIP. Nous l’avons donc retenu comme solution pour la réalisation de ce travail.

La solution proposée par le PABX Asterisk répond à toutes les attendes des administrateurs et utilisateurs de système de téléphonie voix sur IP. En effet, Asterisk est compatible avec la majorité des protocoles et codecs présent sur le marché. Les différents modèles d’installation proposés (service ou distribution) ont pour des avantages de faciliter une intégration rapide dans un réseau existant. La configuration du PABX et de ses modules est centralises et accessible depuis de nombreuses interface d’administration comme (web, wizard … etc). En fin, la facilité d’intégration, l’évolutivité, et la professionnalisation de ce système en font une solution concurrente pour les constructeurs du marché (Alcatel, Matra, Cisco).

## **IV.2.2 Présentation d’Asterisk**

Asterisk est un PABX logiciel libre de la Voip, multi plateformes. Il permet entre autres, la messagerie vocale, la conférence, les serveurs vocaux et la distribution des appels. Même implémente les protocoles H.323 et Sip ainsi qu’un protocole nommé IAX. Il permet la communication entre client et serveur ainsi qu’entre deux serveurs. Les avantages de cette solution est fiable et robuste, la simplicité d’utilisation, diminution des couts, open source.

## **IV.2.3 Fonctionnalités**

Asterisk offre un nombre important de fonctionnalités, permettant de répondre à l’ensemble des besoins en téléphonie d’une entreprise on peut citer:

* Stockage des appels entrants et sortants dans une base de données
* Statistiques de durée des appels
* Messagerie vocale
* Statistique des numéros composés …etc

Pour Conclure un peu les références de notre solution qui est asterisk pour implémenter, Les entreprises qui décident d’adopter la VoIP doivent le faire prudement, en mettant le facteur sécurité au premier plan et intègrer le fait que les dysfonctionnements logiciels sont actuellement très nombreux. De plus la vulnérabilité de cette technologie est certaine, les malveillances nombreuses.

Problèmes logiciels surtout, mais aussi failles de sécurité et déroutage d’appels handicapent cette technologie prometteuse. En effet cette technologie permet le passage du téléphone classique à l’ère informatique, s’interfaçant aux interfaces web, aux différents systèmes d’exploitation dont linux bien sûr, et de ce fait bénéficient de leurs avantages mais aussi des difficultés liées à l’informatique en général dont la sécurité bien sûr. Sur ce point il faut reconnaitre un niveau d’authentification faible et une abscence de procèdés de chiffrement non propriétaire.

Les défis à relever consistent à gérer les différents protocoles VoIP (SIP, H323 ou encore MGCP). En termes de sécurité, on constate que chaque équipementier a introduit des langages propres, on peut parler de « dialecte » pour chaque constructeur. Aussi, on rencontre encore des problèmes d’incompatibilité entre systèmes.

Il s'agit pour l'instant d'avertissements, puisque aucune attaque n'est encore à déplorer via la VoIP. Ce ne serait pourtant qu'une question de temps, assure le Communications Research Network. Par ailleurs, «s'il n'est pas corrigé, ce problème de sécurité de la VoIP aura aussi un impact sur la confiance du public», redoutent les experts. Pour le futur, nous n’allons pas vers la simplicité. Les sous-systèmes multimédia IP (IMS - IP multimédia Subsystem) arrivent avec les réseaux mobiles 3G et 4G en IP. Avec aussi des ouvertures pour les MVNO. Les firewalls seront complexes, voire impossible à mettre en oeuvre. Il faut s’attendre à des attaques passant des réseaux fixes aux réseaux mobiles et inversement...

**TROISIEME PARTIE**

# Chapitre V : Architecteur et Représentation de la solution

## **V.1 Introduction**

Asterisk est un autocommutateur téléphonique privée (PABX) open source pour les systèmes d’exploitation UNIX, il est publié sous licence GPL. Asterisk comprend un nombre très élevé de fonctions, tel que les appels téléphoniques, la messagerie vocale, les files d’attentes, les conférences, etc. Il implémente plusieurs protocoles H.320, H.323, SIP et IAX. Durant ce chapitre, on montrera les étapes d’installation et de configuration d’Asterisk sous le système d’exploitation Linux, ainsi que l’installation et la configuration de X-Lite qui est un téléphone VoIP softphone, freeware.

## **V.2 Architecteur du réseau Voip**

L’architecture adoptée au cours de la configuration de la solution de VoIP à base d’Asterisk.

* **Les trois clients SIP** : Sont des machines sur lesquelles installé le système d’exploitation linux ou windows et un client X-Lite, client Zoip
* **Poste attaquant** : Dans lequel on a installé Windows XP ou 7 pour réaliser les attaques.
* **Machine serveur** : la machine serveur sur laquelle installé un système d’exploitation Linux Centos ou debian, et leserveur de VoIP, Asterisk.
* **Firewall** :Un firewall software est installé dans la machine serveur pour limiter l’accès.

## **V.2.1 Architecteur complet**

Figure  : Architecteur de notre réseau

## **V.3 Représentation de la Solution**

Dans notre architecteur des réseaux sur VoIP, on a utilisé une simulation sur Virtual box et je fais aussi VMware.

Pour le système d’exploitation de notre serveur est linux sous la distribution de famille Redhat Centos 7, puis

On va faire la configuration de base pour fixe l’adresse ip de notre serveur et le nom de notre serveur.

Puis nous configurons un dhcp pour attribue les adresses ip au machine clients automatique, pour faire ce démarche on doit avoir les carte de réseaux des au Réseaux interne.

Une fois la configuration de base fonctionne, on passe la configuration dynamique de notre solution facilement à explique.

Première étape on va test si la connexion ou dns de google fonction sur notre serveur juste pour voire on va utiliser la commande ping qui nous permet de vérifier si la connexion fonctionne exactement.

Ensuit on va à jour pour le système exploitation et l’installation des package requis or asterisk est exigence sur cette point et aussi pas mal d’exigence à installer pour bien fonctionner de notre cas de serveur.

Lorsque l’installation de notre application asterisk est installer, pour vérifier si ce bien installer ou pas on redémarre le serveur pour que il prend en compte les modifications qui été effectué pendant l’installation des requis.

Les systèmes d’exploitation de notre client on va utiliser windows 7 et windows xp pour leur avantage qu’ils sont léger et que on peut utiliser trois machine client et un serveur en même temps.

Pour test des appelés et Voice mail on va utiliser les téléphones X-lite et Zoiper.

Les tests vont ses faires la manière suivant genre on lance un appel X-lite à partir de Zoiper et le durée que il va sonner est déterminer notre serveur.

Pour Voice mail si on ne prend pas appel on va passer directement en mode message vocal pour laisse des messages pour destinateur.

## **V.3.1 IPPHONE**

L’IP-Phone est un terminal téléphonique fonctionnant sur le réseau LAN IP à 10/100 avec une norme soit propriétaire, soit SIP, soit H.323. Il peut y avoir plusieurs codecs pour l’audio, et il peut disposer d’un écran monochrome ou couleur, et d’une ou plusieurs touches soit programmables, soit préprogrammées. Il est en général doté d’un hub passif à un seul port pour pouvoir alimenter le PC de l’utilisateur (l’IP-Phone se raccorde sur la seule prise Ethernet mural et le PC se raccorde derrière l’IP-Phone).



Figure  : L’IP-Phone

## **V.3.2 Les Soft Phone, Zoiper et 3CX téléphonie SIP/VOIP-téléphonie SIP sur logiciel :**

Le soft phone est un programme qui emprunte les haut-parleurs et les microphones des ordinateurs, ou un casque qui se branche au PC pour permettre de passer et de recevoir des appels. C’est en complément de ce type de téléphone que sera utilisée notre application puisqu’elle nécessite d’être exécuté sur un PC capable de lancer un programme Java. Les autres types de téléphones sont donnés à titre d’information.



Figure  : Soft Phone

****

Figure  : Zoiper

## **V.3.3 Téléphones VOIP USB**

Un téléphone USB se connecte au port USB d’un ordinateur et avec un logiciel soft phone SIP/VoIP il fonctionnera comme un téléphone normal. En essence, il s’agit d’un microphone et d’un haut-parleur. Toutefois, leur apparence identique à celle d’un téléphone normal fait que l’utilisateur saura s’en servir plus facilement.



Figure  : Les serveurs IP PBX ATCOM

Les serveurs IP PBX ATCOM de la série IP embarquent un système Asterisk sur une plateforme Linux et un puissant processeur Blackfin. Ils permettent une solution très rentable avec une gamme de produits variée du tout analogique (1 à 8 ports), au tout numérique (BRI et PRI).

Figure  : SWITCH

Un commutateur réseau (ou Switch, de l'anglais) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines). Il a donc la même apparence qu'un concentrateur (hub).

Contrairement à un concentrateur, un commutateur ne reproduit pas sur tous les ports chaque trame qu'il reçoit : il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs.

Contrairement à un routeur, un commutateur de niveau 2 ne s'occupe pas du protocole IP. Il utilise les adresses MAC et non les adresses IP pour diriger les données. Les commutateurs de niveau 2 forment des réseaux de niveau 2 (Ethernet). Ces réseaux sont reliés entre eux par des routeurs (ou des commutateurs de niveau 3) pour former des réseaux de niveau 3 (IP).

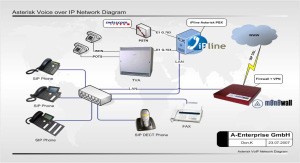


Figure  : Exemple d’une architecture Interne et Externe d’une plateforme ASTERISK

Pour conclure, Depuis le moment ou la VoIP est devenue une technologie relativement nouvelle, le système téléphonique de nombreux fabricants ont dû mettre au point du matériel supplémentaire pour permettre aux systèmes téléphoniques analogiques de gérer les appels VoIP. Cela garantit que les entreprises ne sont pas tenues de remplacer leurs infrastructures téléphoniques et pourront ajouter des fonctionnalités VoIP à leur système de téléphone pour des coûts relativement faibles.

# Chapitre VI : Mise en place de la Solution et Test des Fonctionnements

## **VI.1 Introduction**

Asterisk est une plate-forme ouverte et Open Source de téléphonie et voix sur IP. Elle permet de concevoir des solutions complète de téléphonie et voix intégrant aussi bien la téléphonie traditionnelle en analogique ou numérique que la téléphonie sur IP avec les protocoles MGCP, SIP et un protocole inter-PABX propriétaire : IAX.

On trouve de nombreux document sur Internet concernant Asterisk et comment le configurer, mais nous avons décidé de vous proposer une mise en œuvre simplifié et prenant les concepts à la base afin de faciliter la compréhension de la plate-forme. Nous commençons par ce billet sur la configuration de base autorisant l‘appel entre plusieurs postes localisés sur le même PABX.

## **VI.2 Installation d’asterisk et configuration**

D**’**abord on va installation les prérequis nécessaire pour notre serveur Voip, pour installer les prérequis on doit faire la correction de notre système c’est-à-dire mettre le système d’exploitation à jour.

Nous allons faire la mise à jour de système dans cet un premier temps.

Pour faire la mise à jour il faut avoir la connexion haut-bit et la carte réseaux en NAT comme on va utiliser des serveurs Virtual et il faut se connecte en tant que administrateur de votre serveur.

Le choix de système d’exploitation de notre serveur est Centos 7.

Maintenant nous allons la mise à jour de système :

Commande :

Yum update –y, exécute

Yum upgarde –y, exécute

En mode exécution



Figure  :la mise à jour du système

Une fois la mise à et terminer on va passer à installer aussi les prérequis :

« yum install -y epel-release dmidecode gcc-c++ ncurses-devel libxml2-devel make wget openssl-devel newt-devel k ernel-devel sqlite-devel libuuid-devel gtk2-devel jansson-devel binutils-devel libedit libedit-devel »

En mode exécution

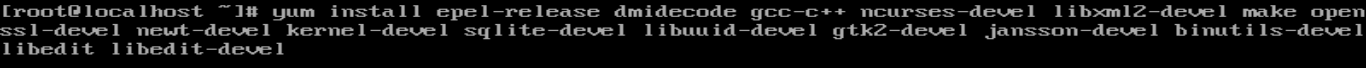


Figure  : les Prérequis

Lorsque l’installation de prérequis et terminer.

Ensuite, installez PJSIP, Une bibliothèque de communication multimédia open source gratuite qui implémente des protocoles standards tels que SIP, SDP, RTP, STUN, TURN et ICE. C'est le pilote de canal SIP Asterisk qui devrait améliorer la clarté des appels.

Pour obtenir la dernière version, créons d’abord un répertoire temporaire dans lequel nous allons construire le paquet à partir de la source.

Le nom de répertoire est build après on se déplace dans le répertoire build alors nous reste de installer PJSIP qui est vraiment important.

Mkdir ~ / build && cd ~ / build.

Nous allons installer PJSIP directement à l’internet.

Wget https://www.pjsip.org/release/2.9/pjproject-2.9.tar.bz2

En mode d’exécution

Figure  : L’installation PJSIP

Ensuit on va décompresse le répertoire pjproject-2.9.tar.bz2

En mode d’exécution



Figure  : Décompresse de pjprojetc-2.9.tar.bz2

Alors une fois que on a décompresse puis on va se déplace dans le répertoire pjproject-2.9.tar.bz2

En mode d’exécution



Figure  : Déplace dans le répertoire pjprojetc-2.9.tar.bz2

Dans l’étape suivant consiste à préparer le package à compiler.

Nous pouvons utiliser la commande suivante : 

Figure  : Préparations de Package

Vous ne devriez voir aucune erreur ni aucun avertissement. Assurez-vous que toutes les dépendances sont remplies:



Figure  : Les Dépendances sont remplies

Et maintenant, nous pouvons compléter les bibliothèques d'installation et de liaison avec:



Figure  : Installation de bibliothèques

Enfin, assurez-vous que toutes les bibliothèques sont installées et présentes:



Figure  : Vérification bibliothèques

Nous sommes maintenant prêts à lancer l'installation d'Asterisk. Revenez dans notre répertoire ~ / build :



Figure  : Déplacement de build

Accédez à la [page de téléchargement d'Asterisk](https://www.asterisk.org/downloads) et récupérez la dernière version. Vous pouvez également utiliser la [commande wget](https://www.tecmint.com/wget-download-file-to-specific-directory/) suivante pour télécharger le fichier dans le terminal.



Figure  : Téléchargement d’asterisk

Lors de la réalisation de notre serveur, la dernière version d'Asterisk est la 16.6.0. Assurez-vous de télécharger la dernière version d'Asterisk lorsque vous suivez les étapes.

Maintenant, extrayez l'archive et accédez au répertoire nouvellement créé:



Figure  : Décompression le répertoire asterisk

Une fois la décompression est terminer, on se déplace dans le répertoire asterisk-16.6.0/.

Figure  : déplacement dans le répertoire

C’est le moment de mentionner que si vous souhaitez activer la prise en charge du format MP3 pour lire de la musique alors que le client est en attente, vous devez installer quelques dépendances supplémentaires. Ces étapes sont facultatives:



Figure  : L’installation de la prise en charge du format MP3

Une fois l’installation est terminer, nous allons exécuterons le script suivant :



Figure  :Exécute du script

Commencez par exécuter le script configure pour préparer le paquet à la compilation:





Figure  : Les paquets à la compilation

Lorsque l’installation est terminer est fini lance simplement scripts suivant pour faire le tour de installations.



Figure  : l’installation des package manquant

Une fois l’installation et la vérification est complète voilà le résultat des installations asterisk :

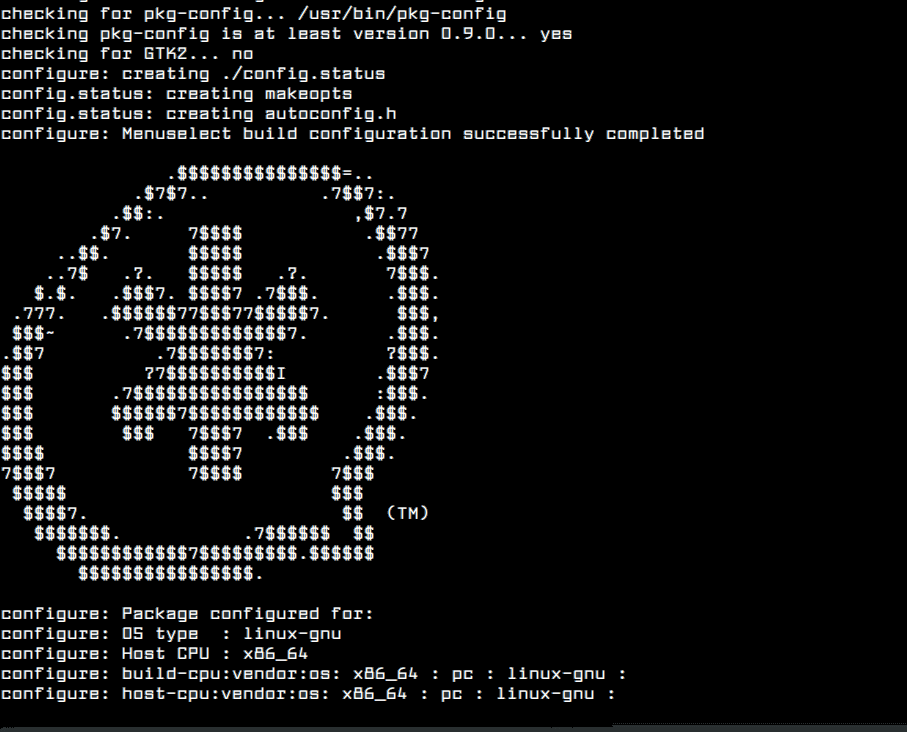


Figure  : l’installation asterisk terminer

Maintenant, commençons le processus de construction:



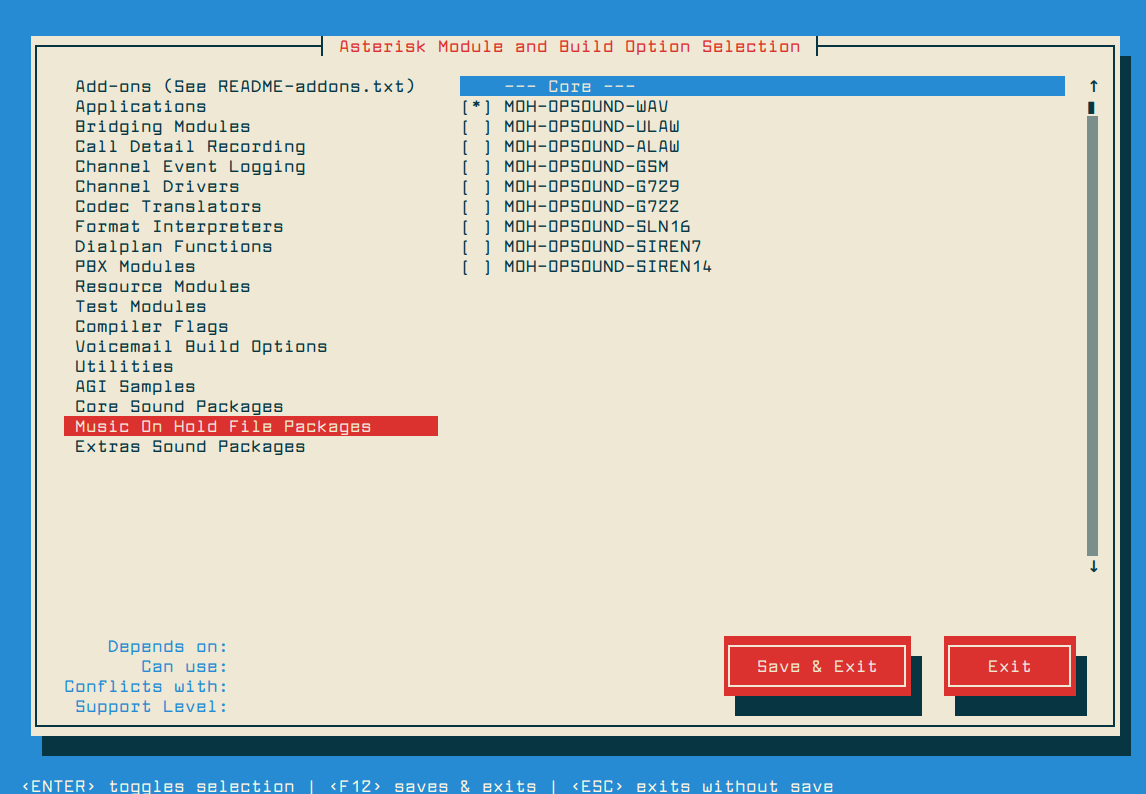


Figure  : Active de la fonction de format\_MP3

Si vous essayez d'utiliser la fonction de musique en attente, vous devrez activer la fonction « **format\_mp3** » à partir de la section « **Modules complémentaires** ». Enregistrez votre liste et exécutez la commande suivante:



Figure  : Module complémentaires pour la fonction format\_mp3

Pour installer les exemples de fichiers de configuration, utilisez la commande ci-dessous:



Figure  : les exemples de fichier de configuration

Pour démarrer Asterisk au démarrage, utilisez:



Figure  :Démarrage de asterisk

Mettez à jour la propriété des répertoires et fichiers suivants:



Figure  : Le droit de propriété des répertoires

Enfin, testons notre installation avec:

Pour teste l’installation il faut redémarre le serveur pour qu’il prend en compte les modifications des serveurs :



Figure  : redémarrage de serveur et lancement de serveur asterisk

Vous devriez voir une sortie similaire à celle-ci:



Figure  : Fin d’installation d’asterisk dans notre serveur centos7

## **VI.3 Configurations des utilisateurs**

Asterisk doit aussi reconnaître vos softphone pour cela les fichiers sip.conf et extensions.conf doivent être configuré

## **VI.3.1 Configurations de fichier sip.conf**

Nous allons créerons les utilisateurs dans le fichier sip.conf pour mettre les utilisateurs simplement :

Pour les utilisateurs on va aller directement dans le fichier /etc/ asterisk/sip.conf



Figure  : Fichier de configuration

Dans fichier quand on va créer nos utilisateurs :

Par exemple je créer trois utilisateur pour test mais on peut créer leur utilisateur avec une syntaxe simple et factorise

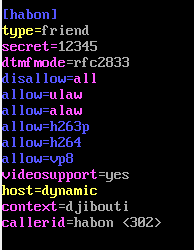


Figure  : Création d’un utilisateur

[Le nom d’un utilisateur]

Type = friend, peut émettre et recevoir des appels

Host = dynamic, type d’adressage IP

Callerid = le nom utilisateur et son le numéro de téléphone

Secret = 12345 = mot de passe

Defaultip = l’adresse ip de serveur asterisk

Context = nom\_context numéro d’appel

## **VI.3.2 Configurations de fichier extension.conf**

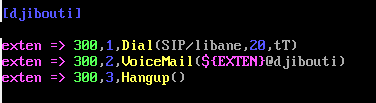


Figure  : Configuration d’extension utilisateur

Exten = le nom telephone de utilisateur, action 1, Dail (SIP/le nom de utilisation, durée de sonnerie, tranfer d’appel)

Exten = le nom telephone de utilisateur, action 2, VoiceMail (${EXTEN}@le nom de context)

Exten = le nom telephone de utilisateur, action 3, Hangup () decroche l’appel.

**VI.3.3 Configurations de Voice mail**

Pour configure le voice mail on va edite le fichier suivant :



Figure  : Fichier de configuration de Voice mail

Une fois le fichier ouvrier on va configure la manière suivant :

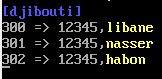


Figure  : Configuration de boite vocale

[Le nom de context]

Le numéro de téléphone = le mot de passe, le nom de utilisateur.

Puis nous allons configure les appels simultanée et pour configure on va éditer le fichier extension.conf



Figure  : Configuration des appels simultanée

Après une fois la configuration de boite vocale est configure, maintenant nous allons ferons la configuration des transferts d’appel, genre transfert aveugle A appelle B alors B le met en attend et transfert à c.

Quand on va éditer le fichier features.conf, on va trouver ligne 41 avec numéro # 1 et 44 \* numéro 2 qui est comment mais nous on va décommet et enlever les numéros seulement.

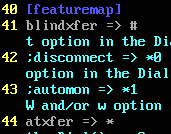


Figure  : Activation des touche de transfère

Et maintenant pour active du transfert pour les utilisateurs nous allons encore éditer le fichier suivant extension.conf juste on va ajouter tT après le durée sonner de téléphone lors d’appel

t : appelant (celui qui émet l’appel)

T : l’appel (celui qui reçoit l’appel)



Figure  : Activation du transfert pour les utilisateurs

Puis nous allons mettre un parking d’appels pour les appelants, pour configure on va éditer le fichier suivant res\_parking.conf

On va juste modifier les lignes 49, 60, 70 pour la ligne 70 on va décommet la durée de parking

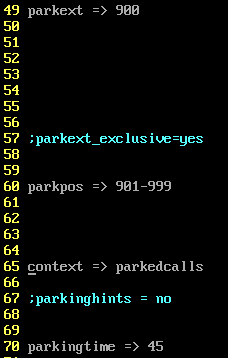


Figure  : Parking d’appels

Une fois que ce fichier est configure alors on va aller passer dans le fichier extension pour inclure la parkedcalls simplement.



Figure  : inclure parkedcalls

Pour configure les conférences vidéo on va aller dans le fichier /etc/asterisk/confbridge.conf :

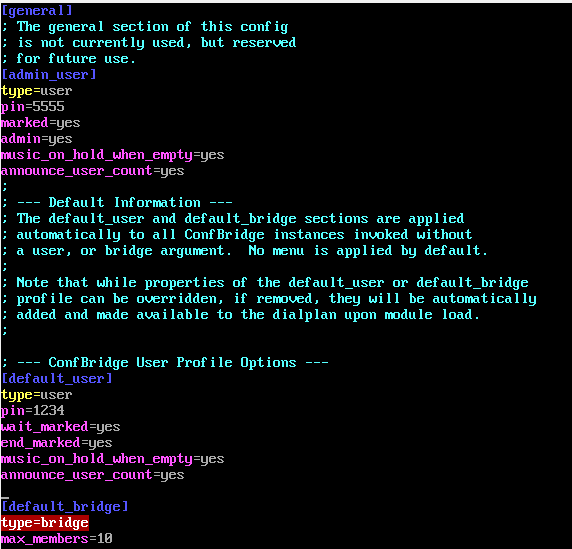
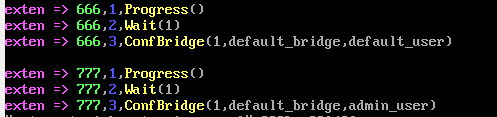


Figure : vidéo conférences

Pour mettre la vidéo en place on va configuration le fichier /etc/asterisk/extension.conf :



**Figure 60: configuration mise en place les conférences**

Le résultat de la configuration pour la vidéo de conférences :

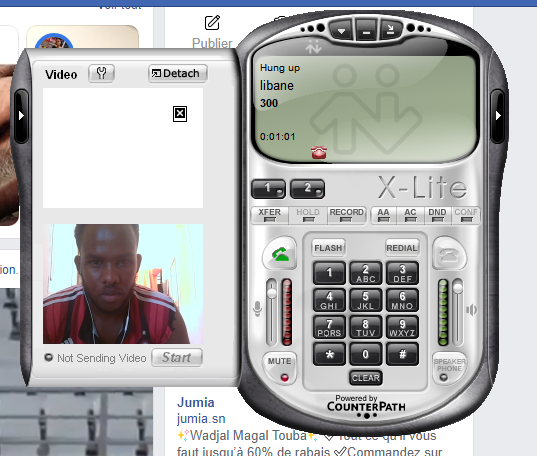
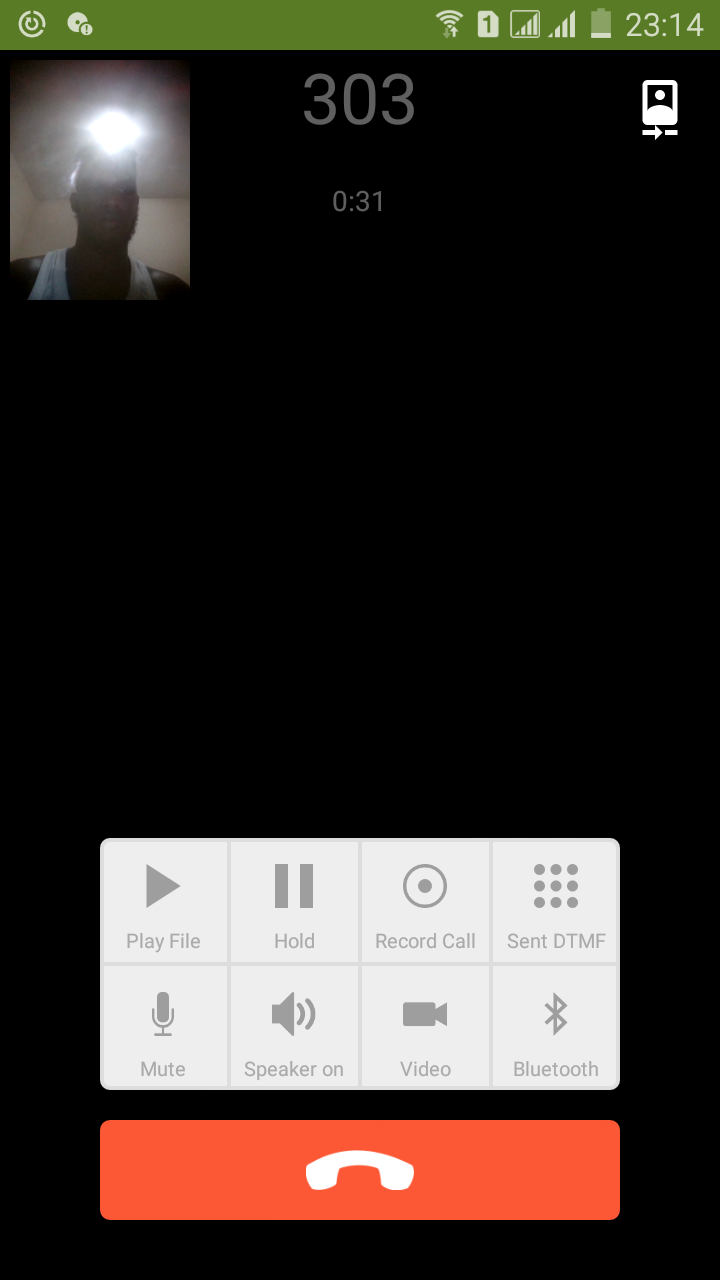
 

Figure  : les conférences avec xlite

Pour conclure l’installation et la configuration de notre serveur asterisk qui est ouvert à tous, gratuit et simple d’utilisation. Asterisk a de quoi s’imposer. Ces vrais concurrents sont plutôt les PBX Hardware. Qui sont chers mais performant et fiable. Les solutions libres peuvent fournir les outils les plus performants et les mieux documentés sans procurer un même service relationnel.

## **VI.3.2 Sécurisations de la solution mise en place**

Après avoir étudié les protocoles de la Voip, identifié les attaques qui menacent les systèmes de Voip et les bonnes solutions afin de sécuriser le serveur Asterisk. Nous allons nous intéresser dans ce chapitre 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 utiliserons un logiciel d’attaques, Wireshark et nous expliquerons comment il fonctionne. Nous présenterons des scénarios d’attaques réalisés par ces logiciels. Dans la deuxième partie, nous montrerons les solutions implémentées pour sécuriser la solution déployée.

## **VI.3.1 Localisation des serveurs Voip**

Toute bonne attaque VoIP commence par une étape qui établit le profil de la cible connu sous le nom profiling ou encore foot printing. Une empreinte englobe les informations sur la cible qui déploie le serveur VoIP et ces paramètres de sécurité. Il existe plusieurs méthodes pour la collecte des informations en voici quelques-unes des plus utilisées :

* **Utilisation des Serveurs whois**

Les whois sont des services proposés gratuitement en ligne permettant d’obtenir des informations sur un domaine particulier, sur une adresse de messagerie. Grâce à ses bases de données comme : Whois.ripe.net : s’occupe d’attribuer des adresses IP pour l’Europe. Whois.apnic.net : attribue les adresses IP pour l’Asie.

* **Utilisation des aspirateurs de sites**

Un des grands avantages des moteurs de recherches Internet est leurs énormes potentiels pour découvrir les plus obscurs des détails sur l'Internet. L'un des plus grands risques pour la sécurité est aujourd'hui l’énorme potentiel des moteurs de recherche pour découvrir les détails sur l'Internet. Il existe une variété de façons qu’un hacker peut exploiter en utilisant simplement les fonctionnalités avancées d'un service tel que Google. Le ciblage des catégories suivantes des résultats de recherche peuvent souvent fournir de riches détails sur la solution VoIP déployée par un organisme:

• Vendeur de produit VoIP, les communiqués de presse et des études de cas

• CV de l’administrateur ou liste de références des vendeurs

• Les forums

* **Balayage (Scan) des réseaux VoIP**

Pour pouvoir identifier chaque composante du réseau, il faut déchiffrer et comprendre un bon nombre de paquets afin de reconnaitre par exemple leur adresse IP et son ID. D’autant plus qu’un réseau VoIP ne se limite pas à quelques clients et un serveur Asterisk. Les serveurs TFTP par exemple sont d’une nécessité pour un attaquant afin de retrouver les fichiers de configurations des téléphones IP pour leur usurper leurs identités par exemple. Afin de scanner un réseau, l’outil nécessaire pour cela est un scanner de réseau (sniffer en anglais). C’est un logiciel permettant de découvrir les équipements présents sur un réseau et les services qu’il offre. Le scanner est souvent utilisé par les administrateurs réseau au cours de test de sécurité. Son principe de fonctionnement est de tester chaque adresse IP et chaque port TCP ou UDP afin de vérifier la présence d'un serveur ou d'un quelconque équipement fonctionnant en TCP/IP. Dans le cadre de notre projet on va se limiter seulement au sniffing des paquets au niveau du serveur et des clients VoIP. Pour cela on aura besoin des outils adéquats pour effectuer cette opération. Parmi les logiciels les plus connues en matière de sniffing dans un réseau basé sur la VoIP sont Wireshark.

## **VI.3.2 Les logiciels d’attaques**

## **VI.3.2.1 Wireshark**

Wireshark est un logiciel libre d'analyse de protocole, utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétroingénierie, mais aussi le piratage. C’est l'analyseur réseau le plus populaire du monde. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau. 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).

* **Captures de trames**

Nous avons placé Wireshark dans une 3éme machine Virtual qui va jouer le rôle de l’attaquant car on va utiliser la machine physique et un téléphone portable Android. Elle va sniffer tous le trafic circulant dans notre réseau local. Nous avons lancé au début la capture des trames ensuite on a initialisé une connexion entre deux clients, « 300 » ayant comme adresse IP 192.168.1.12 et « 302 » ayant comme adresse IP 192.168.1.35. Voilà le résultat de la capture :

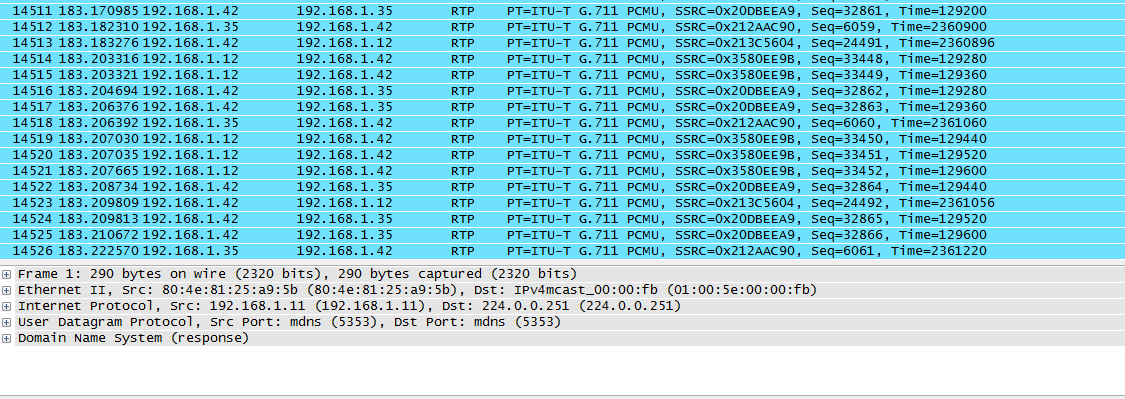


Figure  : capture avec Wireshark sans la sécurité

Comme nous pouvons le voir dans la figure 61, 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 celle la plus intéressante, nous pouvons lire le contenue des paquets et donc collecter des informations très indispensables pour effectuer une bonne attaque.



Figure  : : les paquets qui contient une requête INVITE

Voilà en plus grand, dans la figure 13, le paquet que nous avons choisi pour examiner. Celui-ci est un paquet utilisant le protocole SIP 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.

* **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 client nommé libane ayant comme adresse IP 192.168.1.12 va appeler le client nommé habon ayant comme adresse 192.168.1.35. Il faut savoir que ces deux clients 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 autorisé 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 14 :

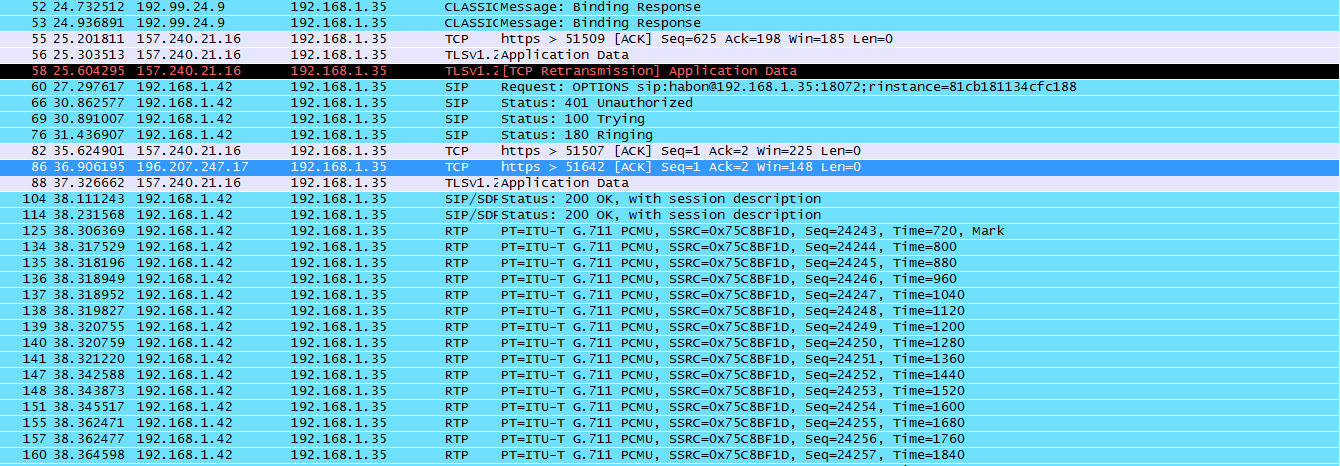


Figure  : Capture d’une communication téléphonique

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 65 :

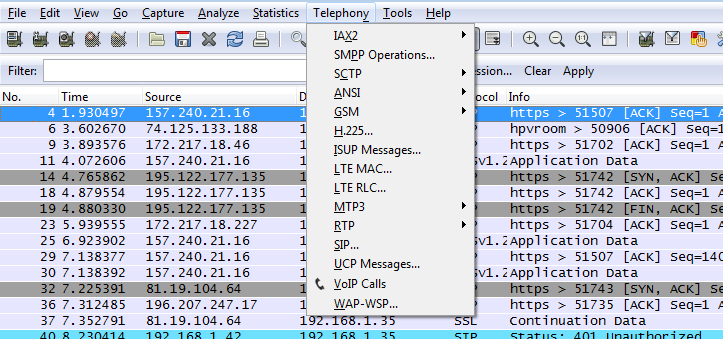


Figure  : Décodage: Bouton VoIP Calls

Une deuxième fenêtre s’ouvre (voir figure 65) contenant les communications dans les deux sens, du client 192.168.1.12 vers 192.168.1.35, et inversement.

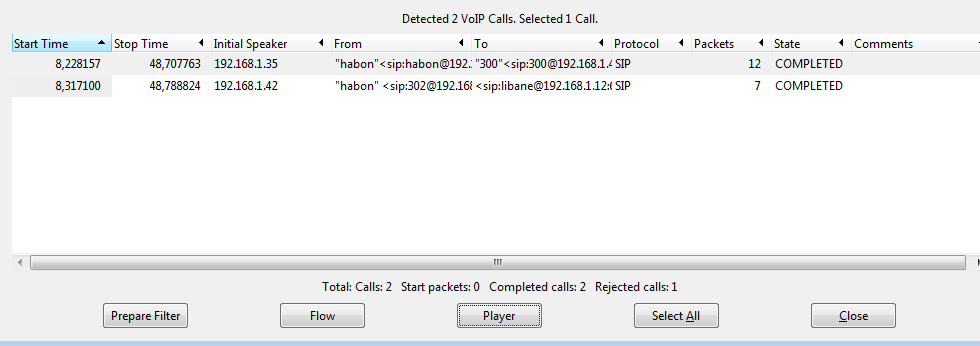
****

Figure  : Communication téléphonique détectés

Maintenant que le décodage a abouti nous pouvons aussi voir sur la figure 66 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. Nous avons choisi ici d’écouter la communication qui se dirige de l’adresse IP192.168.1.12 vers l’adresse IP 192.168.1.35. La communication est de durée 17,26 s.

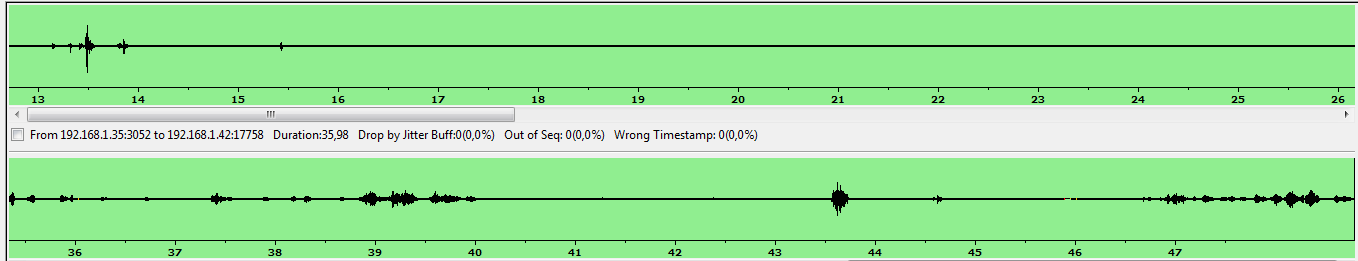


Figure  : Communication téléphonique décodé

## **VI.3.3 Choix et implémentation des bonnes pratiques**

Pour se protéger contre les attaques réalisées et même d’autres attaques similaires comme les attaques DOS, nous avons choisi un ensemble de solutions qui peuvent aider à minimiser les menaces, nous ne pouvons pas dire que les solutions proposés et implémentés sont efficaces. Parce qu’il existe toujours des problèmes de sécurités.

## **VI.3.4 Bonne pratique contre l’écoute clandestine**

Parmi les solutions les plus performantes et les plus faciles à mettre en œuvre, pour contourner l’attaque de l’Eavesdropping ou l’écoute clandestine, est l’implémentation d’openvpn sur notre serveur Asterisk. En effet, openvpn est un logiciel libre permettant de créer un réseau privé virtuel. De cette façon une personne malveillante essayant de décoder les paquets, ne pourra plus user de cette attaque. Ce logiciel qui crée un réseau prive et chaque aura une adresse prive qui est configure par l’administrateur mais pour applique la utilisation de openvpn dans tout les réseaux de l’entreprise on doit faire des routages entre le serveur et les clients.

## **VI.3.4.1 Installation et Configuration d’openvpn**

D’abord on va installer openvpn et son dépendance sur notre serveur asterisk



Figure  : installation des dépendances



Figure  : l’installation d’openvpn

On se déplace le répertoire dans /usr/share/easy-rsa/3 :



Figure  : Déplacement dans le répertoire 3

Initialisation de pki dans le répertoire 3 :

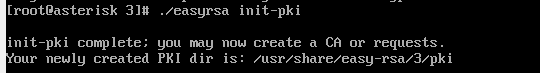


Figure  : Initialisation de pki

Générations de clé build-ca



Figure  : build-ca

Générations de clé pour le serveur



Figure  :build-serveur

Générations de clé pour les clients



Figure  : build-client

Générations de gen-dh



Figure  : Gen-dh

Générations de genkey pour le secret



Figure  : GenKey Secret

On va copier dans le répertoire server les clés :

Cp -pR /usr/share/easye-rsa/3/pki/{issued,private,ca.crt,dh.pem,ta.key} /etc/openvpn/server

****

Figure  : se déplace dans le serveur

Activation des routages, Pour faire on va editer le vim 10-ipv4\_forward.conf





Figure  : Activation de routage

Encore on va se copier dans le répertoire serveur encore pour configure le fichier serveur.conf de openvpn les paramètres à spécifie, alors on va éditer le fichier serveur.conf

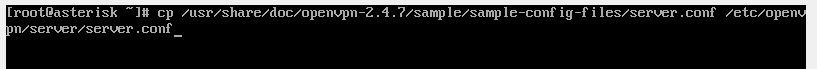
















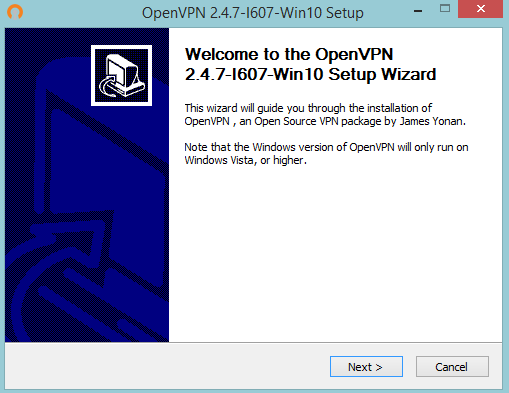


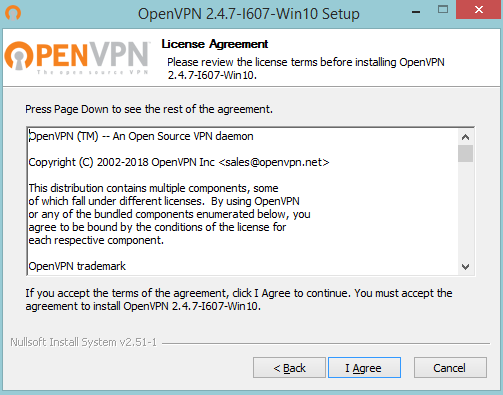
Figure   : Configuration d’openvpn cote serveur

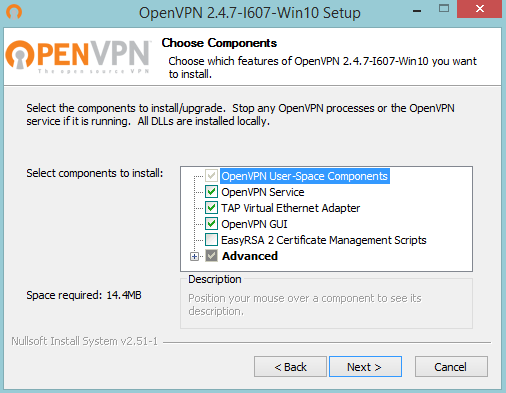
Maintenant une fois quand on a terminé la configuration de openvpn sur notre serveur asterisk alors on va passer l’installation et la configuration de openvpn de cote client.

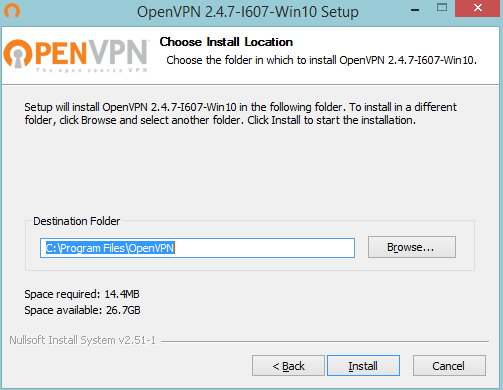
La configuration du client est simple. Il faut tout d’abord installer le client OpenVPN sur la machine.

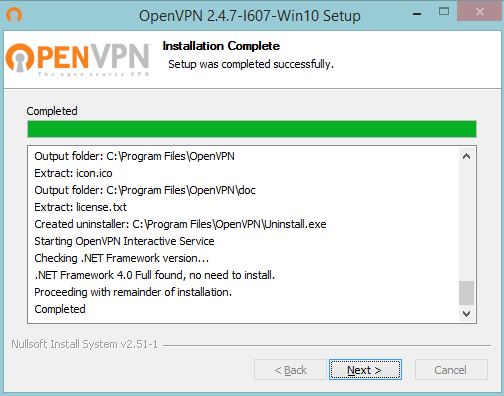












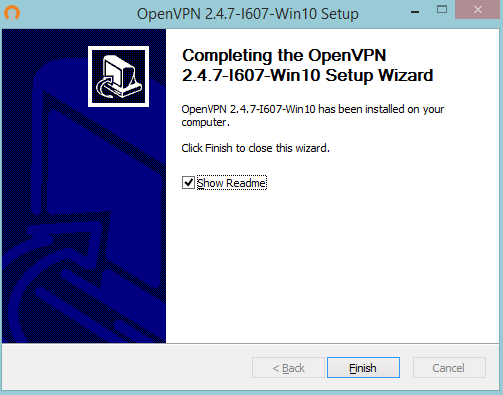
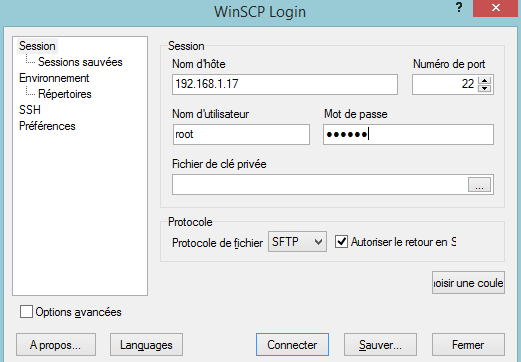


Figure  : L’installation d’openvpn sur le client

Ensuite il faut copier les fichiers suivant (Ca.crt, Client.crt, ta.key et Client.key) qui se trouvent sous le répertoire /etc/openvpn du coté serveur, pour faire ce travailler on va utiliser application winscp pour se connecte notre serveur asterisk.



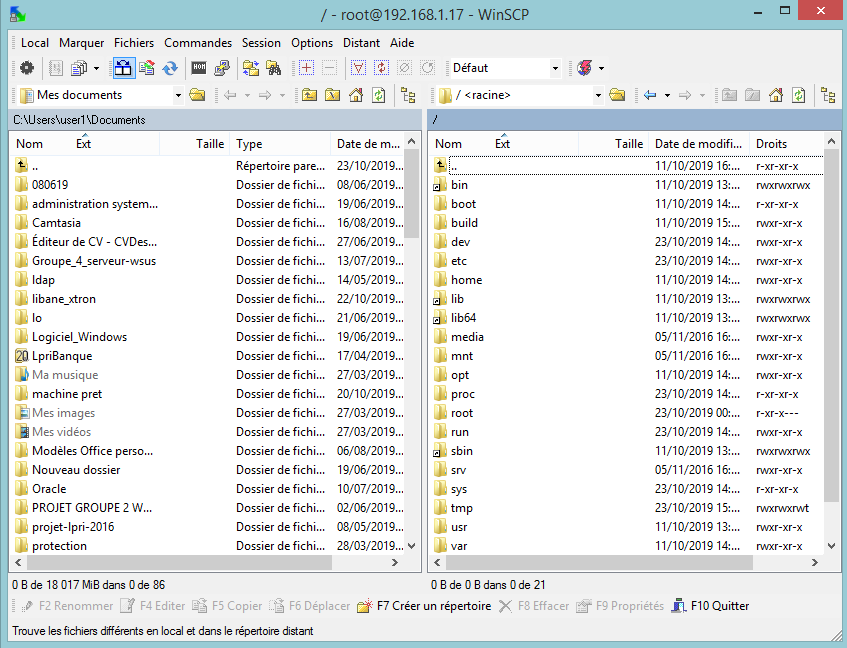


Figure  : Connexion de client vers le serveur

Maintenant pour copier les fichiers des certificats pour se déplacé dans le répertoire etc/openvpn/



Figure  : Copier les clés et certificat dans les clients

Ensuite noter fichier client.conf quand dois configure il se trouve le répertoire sample-config mais il faut copier dans le répertoire config et configurer le fichier client.conf afin qu’il puisse reconnaître le serveur grâce à l’ajout de la ligne suivante dans le fichier :

Pour configuration il faut juste éditer le fichier de configuration client.conf après il faut modifier la ligne 42 pour configure l’adresse remote voilà :



Figure  : l’adresse de vpn de notre serveur

Il faut décommet la ligne 121 pour comp-izo :



Figure  : compresse

Maintenant que on a terminé la configuration de fichier client.conf alors on copier les quatre fichiers des clés et le certificat dans répertoires config.

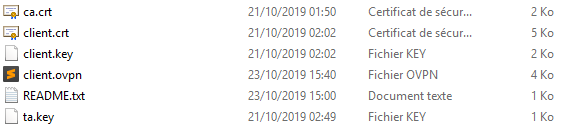


Figure  : copier de fichier dans le répertoire

Alors on a fin de cote client maintenant on va connecte notre client vpn voila :



Figure  : connexion au vpn au client

Tout au long de ce chapitre, nous avons pu voir les différentes attaques effectués au sein du réseau VoIP et les mesures de sécurités à prendre, afin de les éviter. Mais il faut savoir qu’il est impossible d’avoir une sécurité parfaite au niveau du réseau VoIP et généralement sur tous les réseaux.

# CONCLUSION GENERALE

L’objectif de ce projet, après avoir établi des études sur voix sur IP et des études de la sécurité, est de sécuriser un réseau VoIP mis en place. L’étude consiste à effectuer des scénarios d’attaques sur le réseau et voir quelles sont les vulnérabilités existantes afin de sécuriser le réseau VoIP. Dans une première étape, nous nous sommes intéressés à l’étude de cette technologie avec ses différents protocoles et standards. Dans une deuxième étape, nous avons étudié les problèmes de sécurité de la voix sur IP, les attaques, les vulnérabilités sur différents niveaux et les bonnes pratiques possibles pour les attaques cités. Comme troisième étapes, nous avons installé et configuré une solution de VoIP utilisant le serveur Asterisk et de deux clients x-lite. En dernière étape, nous sommes testés des attaques de sécurité contre la solution installée, et nous avons proposé et implémenté des mécanismes et des protocoles pour la sécuriser. Ce projet a été une expérience fructueuse qui nous a permis de mieux s’approcher du milieu professionnel. Cette expérience nous a permis de savoir comment gérer et optimiser le temps dans le but d’en profiter au maximum.

# Webographie

[http://fr.abcarticulos.info/article/l-histoire-de-la-technologie-voip](http://fr.abcarticulos.info/article/l-histoire-de-la-technologie-voip  29/08/2019)

[29/08/2019](http://fr.abcarticulos.info/article/l-histoire-de-la-technologie-voip  29/08/2019) à 12h56

<https://wikimemoires.net/2011/03/protocole-de-transport-de-voip-codecs>

31/08/2019 à 14H22

[http://www.radioactif.com/blog/communication-par-voix-sur-ip-voip-comprendre-son-fonctionnement-805078.html 12h44](http://www.radioactif.com/blog/communication-par-voix-sur-ip-voip-comprendre-son-fonctionnement-805078.html%2012h44)

<http://pf-mh.uvt.rnu.tn/620/1/%C3%89tude_et_Mise_en_place_d%27une_Solution_VOIP_S%C3%A9curis%C3%A9e.pdf>

15/09/2019 à 22h20

<https://www.youtube.com/watch?v=UQ14hhTvMu4&t=2405s>

25/09/2019 à 12h30

# Bibliographie

[1] Éric Cole, "Hackers : Attention danger ! "

2001, Campus Press. [2] Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky, "WiFoo"

2005, Campus Press. [3].

Cour de Mr Racine en TOIP l’Anne académiques 2018/2019.

**Table des matières**

[SOMMAIRE i](#_Toc23151830)

[DEDICACES ii](#_Toc23151831)

[REMERCIEMENTS iii](#_Toc23151832)

[AVANT-PROPOS iv](#_Toc23151833)

[LISTE DE FIGURES v](#_Toc23151834)

[LISTE DE TABLEAUX viii](#_Toc23151835)

[LISTE DES SIGLES ET ABREVIATIONS ix](#_Toc23151836)

[INTRODUCTION GENERALE 1](#_Toc23151837)

[Chapitre I : Cadre théorique 4](#_Toc23151838)

[I.1 : Problématique 4](#_Toc23151839)

[I.2 : Objectifs 5](#_Toc23151840)

[I.2.1 : objectifs générale 5](#_Toc23151841)

[I .2.2 : Objectifs spécifiques 5](#_Toc23151842)

[I.3 Pertinence de Sujet 5](#_Toc23151843)

[Chapitre II : Cadre Méthodologique 7](#_Toc23151844)

[II.1 Délimitation de sujet 7](#_Toc23151845)

[II.2 hypothèses 7](#_Toc23151846)

[II.2.1 hypothèse 1 7](#_Toc23151847)

[II.2.2 hypothèse 2 7](#_Toc23151848)

[II.3 LES DIFFICULTES 7](#_Toc23151849)

[DEUXIEME PARTIE 8](#_Toc23151850)

[Chapitre III : ETUDES DETAILLES 9](#_Toc23151851)

[Dans ce chapitre nous traiterons du cadre Etudes détaillés, c’est à dire nous parlerons des rappels réseau informatique et la technologie sur la voix sur IP et puis de les rappels sur la sécurité. 9](#_Toc23151852)

[III.1 Rappel sur les réseaux informatiques 9](#_Toc23151853)

[Global Area Network (GAN) 23](#_Toc23151854)

[III.2 Technologie sur Voip 28](#_Toc23151855)

[Dans cette partie nous traiterons du cadre Etudes comparatives, c’est à dire nous parlerons des rappels réseau informatique et la technologie sur la voix sur IP. 28](#_Toc23151856)

[III .2 .1 Historie du téléphone 28](#_Toc23151857)

[III.2 .2 Mode fonctionnement et protocole associe Voip 30](#_Toc23151858)

[III.2.2.1 PROTOCOLE TCP /IP 30](#_Toc23151859)

[III.2.2.2 PROTOCOLE UDP 30](#_Toc23151860)

[III.2.2.3 PROTOCOLE RTP 30](#_Toc23151861)

[III.2.2.4 PROTOCOLE RTP 31](#_Toc23151862)

[III.3 RAPPELLE SUR LA SECURITE 35](#_Toc23151863)

[III.3 .1 Introduction 35](#_Toc23151864)

[I.3.2 Cryptologie 38](#_Toc23151865)

[III.3.2.1 Cryptographie 39](#_Toc23151866)

[A Cryptographie symétrique 40](#_Toc23151867)

[A.1 les avantages et inconvénients Cryptographie symétrique 41](#_Toc23151868)

[A.1.1 Chiffrement de Vernam 41](#_Toc23151869)

[A.2 Méthodes de Chiffrement 43](#_Toc23151870)

[A.2 .1 Chiffrement par flux 43](#_Toc23151871)

[A.2 .2 Chiffrement par blocs 44](#_Toc23151872)

[A.3 Algorithmes 44](#_Toc23151873)

[A.3.1 ROT13 44](#_Toc23151874)

[B Cryptographie Asymétrique 45](#_Toc23151875)

[C Cryptographie Hybride 46](#_Toc23151876)

[III.3.2.2 Cryptanalyse 47](#_Toc23151877)

[III.3.2 Gestion des certificats et système authentification 50](#_Toc23151878)

[III.3.2.1 Gestion des Certificats 50](#_Toc23151879)

[III.3.2.2 Système Authentification 53](#_Toc23151880)

[Chapitre IV : Etudes Comparatives et le choix de les solutions 61](#_Toc23151881)

[Introduction : 61](#_Toc23151882)

[IV.1 Etudes comparatives 61](#_Toc23151883)

[IV.1.1 Logiciels Propriétaires de la VoIP 61](#_Toc23151884)

[IV.1.2 Logiciels libres de la VoIP 62](#_Toc23151885)

[IV.2 Choix de la solution 64](#_Toc23151886)

[IV.2.1 Choix d’Asterisk 64](#_Toc23151887)

[IV.2.2 Présentation d’Asterisk 64](#_Toc23151888)

[IV.2.3 Fonctionnalités 64](#_Toc23151889)

[Chapitre V : Architecteur et Représentation de la solution 67](#_Toc23151890)

[V.1 Introduction 67](#_Toc23151891)

[V.2 Architecteur du réseau Voip 67](#_Toc23151892)

[V.2.1 Architecteur complet 68](#_Toc23151893)

[V.3 Représentation de la Solution 68](#_Toc23151894)

[V.3.1 IPPHONE 69](#_Toc23151895)

[V.3.2 Les Soft Phone, Zoiper et 3CX téléphonie SIP/VOIP-téléphonie SIP sur logiciel : 69](#_Toc23151896)

[V.3.3 Téléphones VOIP USB 70](#_Toc23151897)

[Chapitre VI : Mise en place de la Solution et Test des Fonctionnements 73](#_Toc23151898)

[VI.1 Introduction 73](#_Toc23151899)

[VI.2 Installation d’asterisk et configuration 73](#_Toc23151900)

[VI.3 Configurations des utilisateurs 79](#_Toc23151901)

[VI.3.1 Configurations de fichier sip.conf 79](#_Toc23151902)

[VI.3.2 Configurations de fichier extension.conf 80](#_Toc23151903)

[VI.3.2 Sécurisations de la solution mise en place 85](#_Toc23151904)

[VI.3.1 Localisation des serveurs Voip 85](#_Toc23151905)

[VI.3.2 Les logiciels d’attaques 86](#_Toc23151906)

[VI.3.2.1 Wireshark 86](#_Toc23151907)

[VI.3.3 Choix et implémentation des bonnes pratiques 90](#_Toc23151908)

[VI.3.4 Bonne pratique contre l’écoute clandestine 90](#_Toc23151909)

[VI.3.4.1 Installation et Configuration d’openvpn 91](#_Toc23151910)

[CONCLUSION GENERALE 100](#_Toc23151911)

[Webographie 101](#_Toc23151912)

[Bibliographie 102](#_Toc23151913)