**REPUBLIQUE DU SENEGAL**

Un peuple - Un but - Une foi

**MINISTERE DE LôENSEIGNEMENT SUPERIEUR ET**

**DE LA RECHERCHE**

Université Dakar-Bourguiba

# Mémoire de Fin de Cycle

Pour lôobtention du Diplôme de Master en Informatique

Option : **Systèmes - Réseaux - Télécoms**

# ETUDE ET MISE EN PLACE DôUNE SOLUTION DE VOIX SUR IP

# DANS UN ENVIRONNEMENT MULTI-SITE :

# CAS DU MINISTERE GUINEEN DE LA DEFENSE NATIONALE


Réalisé et soutenu par :

M. Bakaramoko Kaba

Année Universitaire 2016/2017

Encadré par :

M. Massamba LO

Professeur en Administration Systèmes/Réseaux


Année de Soutenance 2017

DEDICACE

**A mon Père Elhadj Abdourahamane Kaba**

**Aucune dédicace ne saurait exprimer l'amour,**

**L'estime, le dévouement et le respect que j'ai toujours eu pour Toi.**

**Rien au monde ne vaut les efforts fournis jour et nuit pour mon éducation et mon bien être.**

**Ce travail est le fruit de tes sacrifices que tu as consentis pour mon éducation et ma formation.**

**Puisse Allah le Tout Puissant me donne les moyens pour te rendre heureux et fiers.**

## REMERCIEMENTS

Je tiens à remercier mon Créateur Dieu le Tout Puissant Allah pour la santé, le courage qu'il m'a accordé pour faire ce travail.

**A ma très chère mère Hadja Aissatou Souaré** Affable, honorable, aimable : Tu représentes pour moi le symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi. Ta prière et ta bénédiction m'ont été d'un grand secours pour mener à bien mes études. Aucun remerciement ne saurait être assez éloquente pour exprimer ce que tu mérites pour tous les sacrifices que tu n'as cessé de me donner depuis ma naissance, durant mon enfance et même à l'âge adulte. Tu as fait plus qu'une mère puisse faire pour que ses enfants suivent le bon chemin dans leur vie et leurs études.

Mes remerciements à mes frères, sœurs (**N'Famory**,**Fanta, Zenab, Mohamed Nourdine, Moustapha, Ibrahima, Hassan, Tiguidanké, Fatoumata**) qui n'ont cessé de m'encourager durant mon Circus scolaire.

Mes remerciements au **Haut Commandant de la Gendarmerie et Directeur de la justice militaire guinéenne le Général de Corps d'armée Ibrahima Baldé** pour m'avoir facilité la tâche dans la rédaction de mon mémoire.

Mes remerciements à nos professeurs, et à l'administration de **l'UDB (Université Dakar Bourguiba)**, pour les efforts qu'ils ont consenti dans le but de nous donner une formation de qualité

Mes profonds remerciements vont à mon encadreur **Mr MASSAMBA LÔ**, plus qu'un professeur il est devenu un mentor pour moi, merci d'avoir accepté d'encadrer mes travaux.

Merci à vous **Dr Youssef Khlil**(mon professeur de sécurité informatique),**Ibrahima Touré** ,Grace à vous je suis certifié Cisco CCNA R&S ,au **Professeur Sakhir Thiam** Président de l'UDB. Mes remerciements vont à mes camarades de classe.

## GLOSSAIRE

ACL : Access Control List/liste de contrôle d'accès - système permettant de faire une gestion plus fine des droits d'accès aux fichiers.

ADSL : Asymetrical Data Subscriber Line/Ligne d'abonné numérique asymétrique - technologie d'accès à Internet sur ligne téléphonique.

ARPANET : Advanced Research Project Agency NETwork - premier réseau à transfert de paquets développé aux États-Unis.

ATM : Asynchronous Transfer Mode - technologie réseau, apparue au début des années 1990, gérant le transport de la voix, de la vidéo aussi que celle des données en garantissant une qualité de service.

CAA : Commutateur à Autonomie d'Acheminement

CL : Commutateur Local

CTP : Commutateur de Transit Principal

CTS : Commutateur de Transit Secondaire

DHCP : Dynamic Host Configuration Protocol - protocole chargé de la configuration automatique des adresses IP d'un réseau informatique.

DiffServ : Differentiated Services - architecture de réseau qui spécifie un mécanisme pour classer et contrôler le trafic tout en fournissant de la qualité de service, en différenciant les services des données.

DNS : Domain Name System - service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresse IP de la machine portant ce nom.

Dos : Denial of Service/Déni de Service

DSP : Digital Signal Processor - microprocesseur optimisé pour exécuter des applications de traitement numérique du signal le plus rapidement possible, utilisé dans la plupart des applications du traitement numérique du signal en temps réel.

FTP : File Transfer Protocol - Protocole de transfert de Fichier.

FXO/FXS : Foreign eXchange Office/ Foreign eXchange Subscriber - ports utilisés par des lignes téléphoniques analogiques. L'interface FXS ste le port qui raccorde la ligne analogique de l'abonné.

GPL : General Public License - Accord qui réglemente la distribution des logiciels libres afin que les programmes ainsi que tous les travaux dérivés soient distribués avec le code source.

GSM : General System for Mobile communications - norme numérique de seconde génération pour la téléphonie mobile.

Hard phone : Téléphone matériel

HTTP : HyperText Transfer Protocol - Ce protocole définie la communication entre un client et un serveur sur le World Wide Web (WWW).

HCGN : Haut commandement de la gendarmerie Nationale

IAP : Internet Access Provider - Fournisseur d'Accèsà Internet (FAI).

IETF : Internet Engineering Task Force - Groupe spécial d'ingénierie d'Internet : grande communauté internationale ouverte de concepteurs de réseaux, d'opérateurs, de vendeurs et de chercheurs intéressés par l'évolution de l'architecture et le fonctionnement sans heurt d'Internet.

IP : Internet Protocol - un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des paquets de données, sans toutefois en assurer la « livraison ».

IP-phone : Téléphone IP

IP sec : Internet Protocol security - ensemble de protocoles (couche 3 modèle OSI) utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.

ISO : International Organization for Standardization - organisation internationale de normalisation

ITSP : Internet Telephony Service Provider - prestataire de services de téléphonie Internet

LAN : Local Area Network

LTE : Long Term Evolution - technologies de téléphonie mobile de quatrième génération (4G)

MAN : Metropolitan Area Network

MGCP : Media Gateway Control Protocol - protocole permettant de contrôler les passerelles multimédia qui assurent la conversion de la voix etde la vidéo entre les réseaux IP et le Réseau Téléphonique Commuté.

MPLS : Multi-Protocol Label Switching - technique réseau dont le rôle principal est de combiner les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2 telles que implémentées dans ATM ou FrameRelay.

OSI : Open System Interconnection - modèle de communication entre ordinateurs proposé par l'ISO qui décrit les fonctionnalités nécessaires laà communication et l'organisation de ces fonctions.

PABX : Private Automatic Branch eXchange/PBX

PABX-IP : Private Automatic Branch eXchange-Internet Protocol/IPBX

PAN : Personal Area Network

PME : Petite et Moyenne Entreprise

PSTN: Public Switched Telephone Network/RTPC

QoS : Quality of Service/Qualité de Service

QSIG : Protocole de signalisation standard basé sur RNIS utilisé afin d'interconnecter des PABX de constructeurs différents

RAS : Registration Admission and Status

RNIS : Réseau Numérique à Intégration de Service réseau- de télécommunications qui se distingue du réseau téléphonique. Entièrement numérisé, il permet une liaison plus rapide et de meilleure qualité.

RSVP : Resource ReSerVation Protocol - protocole de la couche transport du modèle OSI, permettant de réserver des ressources dans un réseau informatique.

RTCP : Real Time Control Protocol - protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service.

RTP : Real Time Protocol - protocole de communication permettant le transport de données soumises à des contraintes de temps réel, tels que des flux média audio ou vidéo.

RTPC : Réseau Téléphonique Public Commuté/RTC

RTSP : Real Time Streaming Protocol - protocole de communication de niveau applicatif destiné aux systèmes de streaming média.

SIP : Session Initiation Protocol - protocole utilisé pour la connexion, la modification et la fin des appels téléphoniques VoIP.

SMTP : Simple Mail Transfer Protocol - protocole de communication utilisé lors de l'adressage des courriers électroniques sortants.

SNMP : Simple Network Management Protocol - protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau.

Soft phone : Téléphone logiciel

SRTP : Secure Real Time Protocol - profil de RTP qui a pour but d'apporter le chiffrement, l'authentification et l'intégrité des messages.

SSI : Sécurité des Systèmes d'Information.

TCP : Transmission Control Protocol - Protocole de transport, prenant à sa charge l'ouverture et le contrôle de la liaison entre deux ordinateurs.

Telnet : Terminal network - protocole utilisé sur tout réseau TCP/IP, permettant de communiquer avec un serveur distant.

TFTP : Trivial File Transfer Protocol - protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP.

TLS : Transport Layer Security et son prédécesseur SSL (Secure Sockets Layer) - protocoles de sécurisation des échanges sur Internet.

TTS : Text To Speech - consiste à transformer un tex te en suite de sons se rapprochant autant que possible de la parole humaine.

UDP : User Datagram Protocol - un des principaux protocoles de télécommunication tilisésu par Internet. Il fait partie de la couche transport du modèle OSI.

UIT-T : Union Internationale des Télécommunications- agence des Nations unies pour le développement spécialisé dans les technologies d'information et de la communication.

UMTS : Universal Mobile Télécommunications System - technologies de téléphonie mobile de troisième génération (3G)

VoIP : Voice over Internet Protocol

VoIPsec : VoIP utilisant IPsec

VPN : Virtual Private Network/Réseau Privé Virtuel

WAN : Wide Area Network

ZAA : Zone à Autonomie d'Acheminement

ZRTP : Zimmermann Real-Time Transport Protocol - protocole de chiffrement pour les appels téléphoniques passé en VoIP utilisant la méthode Hellman pour l'échange de clé et le protocole SRTP pour le chiffrement.

ZTP : Zone de Transit Principal

ZTS : Zone de Transit Secondaire

# LISTES DES FIGURES

Figure 4.2 : Maquette de test

# LISTE DES TABLES

# SOMMAIRE

# Introduction

Lorsque, le 2 juin 1875, le Canadien Alexandre Graham Bell tente de transformer des ondes sonores en impulsions électromagnétiques, nul n'imaginait que ce professeur de physiologie vocale, spécialisé dans l'enseignement du langage pour sourds et muets, allait inventer le téléphone. Accompagné de son assistant Thomas Watson, Bell expérimente le premier modèle de téléphone à distance limitée et à correspondance réduite : placés dans deux pièces distinctes, les deux physiciens disposent entre eux un fil conducteur dont une extrémité est munie d'une lamelle reliée à un électro-aimant. L'expérience consiste à écarter cette lamelle de l'électroaimant puis à la relâcher. Le résultat est prodigieux : un son se propage sur le fil conducteur jusqu'à parvenir à l'autre extrémité du fil. II faudra moins d'un an au scientifique Bell, tout juste âgé de 28 ans, pour perfectionner son prototype et rendre les transmissions d'un bout à l'autre d'un fil conducteur parfaitement intelligibles pour l'oreille humaine.

En 1964, en pleine guerre froide, le projet de Paul Baran sur un réseau informatique totalement distribué et dédié aux communications militaires est refusé par les autorités. Presque en parallèle, les travaux du français Louis Pouzin, mettant au point le tout premier réseau à commutation de paquets, émule la communauté scientifique. Au début des années 70, un réseau imaginé par des laboratoires de recherche académiques voit le jour. Constitué de quatre ordinateurs répartis dans le monde, il est réalisé par l'ARPA *(Advanced Research Projects Agency)* et prend le nom d'ARPAnet. Au même moment, en France, le projet Cyclades relie plusieurs ordinateurs par une technologie de datagramme.

Pendant plusieurs décennies, la transmission analogique de la voix fut la seule technologie maîtrisée et utilisée. Mais au milieu du vingtième siècle, grâce aux techniques d'échantillonnage, de quantification et de codage, la

transmission numérique de la voix fut rendue possible. Aussi bien la transmission de gros volumes de données requise par l'industrie informatique que l'écoulement d'un grand trafic vocal trouvent leur application à travers les réseaux numériques notamment le RNIS, l'INTERNET.

Pour tirer profit du développement d'Internet pour le grand public, des sociétés ont développé des logiciels de *téléphonie. Il* est alors possible de transporter de la voix entre deux ordinateurs et ainsi de communiquer.

Les réseaux de données et de voix étaient clairement distincts, avec des câblages différents, des protocoles différents et des fonctionnalités différentes. Aujourd'hui la tendance a nettement changé. Les réseaux IP se sont démocratisés : on assiste à une convergence des données, de la voix et même de la vidéo, à tel point que les principaux moteurs de développement des réseaux sont la voix et la vidéo. La voix sur IP devient aujourd'hui une solution incontournable pour les entreprises qui voudrait soit remplacer l'ancien système PBX en faveur d'une plate-forme VoIP ou en créer un pour la réalisation efficiente et efficace d'un système de communication basé sur IP.

L'existence du réseau téléphonique et Internet a amené un certain nombre de personnes à penser à un double usage pour unifier tous ces réseaux, en opérant une convergence voix, données et vidéo, autrement appelé « triple play ». Les opérateurs, les entreprises ou les organisations et les fournisseurs devaient, pour bénéficier de l'avantage du transport unique IP, introduire de nouveaux services voix et vidéo. Ainsi, l'une des solutions qui marquent le « boom » de la voix sur IP au sein des entreprises est la solution PABX-IP (Private Automatic Branch eXchange IP).

C'est dans cette optique que nous travaillons sur : **« Etude et mise en place d'une solution de voix sur IP (VOIP) dans un environnement Multi site. Cas du ministère de la défense nationale guinéenne ».**

**La première partie** est la présentation du cadre de référence ou nous allons présenter le ministère de la défense, l'étude et la critique de l'existant,

l'énoncer de la problématique du projet, ensuite nous allons envisager un ensemble de solutions.

**La deuxième partie** fera l'objet de l'étude de conception technique des solutions et choisir la solution adéquate.

Enfin, **la troisième et dernière partie** est la phase de planification du déploiement ensuite de la mise en œuvre du nouveau système. Et enfin l'évaluation financière.

# PREMIERE PARTIE : Cadres Général et Méthodologique

## CHAPITRE PREMIER : Cadre Général

### Section 1 : Problématique

Le ministère délégué à la présidence chargé de la défense nationale guinéenne est l'un des ministères les plus importants du gouvernement. Il a sous son tutelle l'État-major général des armées, haut commandement de la gendarmerie nationale, les états-majors de terre, mer et de l'air.

Vu l'importance d'un tel ministère, il serait judicieux que l'armée dispose d'un service de téléphonie privé pour assurer la confidentialité de leurs communications internes.

De nos jours il existe deux moyens de communication au sein des forces armées guinéennes qui sont :

La téléphonie GSM contrôlée par les opérateurs téléphoniques du pays et la communication radio.

Face à cette nécessité et par souci d'apporter une contribution dans la reforme et la modernisation des forces armées guinéennes, l'implémentation de la VoIP sera une des solutions appréciables de tous.

Dans cet ordre d'idées, il convient de se poser quelques questions, telles que : Est-il possible d'améliorer les moyens de communication au sein des forces armées guinéennes ?

Est-il possible d'implémenter la solution VoIP dans le réseau informatique du ministère de la défense nationale ?

Comment sécuriser la solution VoIP qui sera implémentée ?

Telles sont les questions auxquelles nous allons tenter de répondre dans la suite de notre travail.

## Section 2 : Objectif de la recherche

Après avoir posé la problématique, il nous incombe de citer les objectifs de notre étude

### Objectif général

L'objectif général de notre étude est la mise en place d'un réseau de téléphonie sur IP, et sécurisé par la technologie VoIP avec des routeurs CISCO et un service d'appel sous le système d'exploitation (Linux). Pour arriver à un tel objectif, nous allons nous atteler à montrer l'importance de la VoIP et leur mise en œuvre.

### Objectifs spécifiques

La VoIP, qui signifie "Voice over IP", permet de transmettre la voix par le réseau IP. La **VoIP** peut notamment être prise en charge par des logiciels d'appels téléphoniques et de visioconférences via internet. Au sein des entreprises, des solutions de téléphonie VoIP sont proposées afin de communiquer via le réseau internet, cela prend alors le nom de ToIP ou "Telephony over Internet".

L'objectif général ainsi présenté, suppose pour être atteint que nous prenions en compte au moins trois paramètres essentiels. Il s'agit de :

· mettre en lumière les outils permettant de réduire les coûts d'installation, extension et exploitation de la VoIP ;

· accroître la capacité d'exploitation de la téléphonie ;

· identifier les actions à mener pour maintenir un bon niveau de sécurité des échanges sur la VoIP.

### Démarche utilisée

Afin de parvenir à la réalisation effective de ce projet nous devons passer par plusieurs étapes :

- Premièrement nous procéderons à une étude suivie d'une analyse de l'existant afin de prendre connaissance des forces et ses faiblesses de l'infrastructure réseau ;
- Deuxièmement, nous examinerons des propositions de solutions, puis nous entretiendrons une ;
- Troisièmement nous passerons à la simulation de configuration des équipements.

A la fin de cette étude, nous aurons comme résultat une infrastructure réseau capable de répondre aux exigences en termes de téléphonie sur IP et de sécurité.

## Section 3 : Hypothèses de recherche

Après avoir formulé et décomposé la problématique en objectifs, nous avons jugé nécessaire de bâtir des hypothèses de travail qui constitueront des éléments de réponses aux interrogations cités plus haut. Ainsi, conformément aux objectifs ci-dessus, les hypothèses suivantes sont formulées pour servir de repères dans les investigations à mener.

### Hypothèse 1

Le choix des entreprises ou des structures gouvernementales sur la téléphonie sur IP serait motivé par le besoin de communiquer en toute sécurité à un coût très faible.

### Hypothèse 2

Notre projet tentera de trouver les limites du réseau actuel en termes de communication et contribuera de manière significative son efficacité.

### Hypothèse 3

Une mise en place de solution de VoIP sécurisé sera très bénéfique au ministère de la défense nationale et l'aidera à avoir son propre réseau téléphonique privé.

## Section 4 : Pertinence du sujet

La téléphonie IP (Internet Protocol, ou protocole Internet) ou VoIP (Voice over Internet Protocol, ou voix par IP) est un mode de téléphonie utilisant le protocole de télécommunications créé pour Internet. La voix est numérisée, puis acheminée sous forme de paquets comme toutes les autres données.

L'augmentation des débits Internet et les économies réalisées sur la facture mensuelle de télécommunications suscitent l'engouement des entreprises et des structures gouvernementales. Sécurité, infrastructure et coût réel sont des paramètres dont nous devons tenir compte lorsque nous remettons en question le système téléphonique actuel.

**Voici 6 avantages pour les organisations d'opter pour la téléphonie IP ou de migrer vers elle :**

**1. Facture réduite**

Grâce au coût avantageux de la VoIP, la téléphonie IP offre de réelles économies pour les entreprises.

**2. Investissement pour demain**

Le marché de la téléphonie d'entreprise IP-PBX a déjà dépassé celui du PBX (autocommutateurs traditionnels). Le passage vers un central téléphonique fonctionnant sur un réseau IP est donc un choix stratégique d'avenir.

**3. Gains en mobilité**

Avec des postes qui ne sont plus physiquement reliés à des lignes, la téléphonie IP permet à l'utilisateur de conserver son numéro dans ses déplacements. Vous pouvez même travailler de la maison en affichant le numéro du bureau ! Terminés les appels de client sur votre cellulaire personnel, en dehors des heures du bureau, lorsque les clients sont pris de panique !

**4. Souplesse accrue**

La téléphonie IP rassemble tous les appareils de l'entreprise (téléphones, visioconférence, télécopieur, ordinateurs, etc.) sur un même réseau et donc sur un même protocole.

**5. Même câblage réseau**

Parfois les coûts de câblage peuvent être un poids dans la balance. La majorité des téléphones offrent à l'arrière un 2e port réseau qui permet d'utiliser un 2e câble pour alimenter votre ordinateur sur le même réseau. Donc, en gros, vous utilisez votre fil réseau d'ordinateur dans votre téléphone et un autre fil du téléphone qui entre dans votre ordinateur.

**6. Les fonctions les plus appréciées**

La téléphonie IP offre une panoplie de fonctions intéressantes et pratiques : enregistrement des appels, renvoi d'appels via le téléphone, envoi par courriel des messages laissés dans la boîte vocale, possibilité de ponts entre 2 succursales ou plus, visualisation des statistiques d'appels entrants et sortants, intégration du télécopieur avec la réception par courriel, renvoi vers cellulaire avec ou sans horaire et bien plus encore !

# CHAPITRE DEUXIEME : Cadre Méthodologique

## Section 1 : Cadre de l'étude

L'étude a été effectuée au siège du **haut commandement de la gendarmerie nationale et direction de la justice militaire guinéenne situé dans le quartier Boulbinet commune de Kaloum région administrative de Conakry.**

Le sujet porte sur la mise en place d'une solution VOIP au sein du haut commandement de la gendarmerie guinéenne. Et nous avons axé nos recherches sur l'utilisation des VOIP comme moyen de communication efficace, sécurisé. Pour atteindre nos objectifs de recherche fixée, nous avons compté sur le soutien et la coopération des différents officiers du haut commandement de la gendarmerie guinéenne.

## Section 2 : Délimitation du champ de l'étude

Nous avons focalisé notre étude sur l'influence d'une solution VOIP au sein des services du HCGN, l'utilité de cette nouvelle technologie dans son fonctionnement.

## Section 3 : Les techniques de la recherche

Dans le but de rassembler des informations pertinentes, importantes et nécessaires à la résolution de notre problématique et afin d'établir des conclusions, nous avons fait recours à deux types d'informations :

- Des informations primaires, recueillies par interrogation ; par le biais d'entretiens individuels avec des responsables du HCGN.

Pour les interviews destinées aux utilisateurs du réseau nous avons tenté de saisir l'intérêt qu'ils accordent à la sécurité et la

gratuité des appels téléphoniques, l'idée que ces mêmes utilisateurs se font des VOIP.

Concernant les interviews réalisées avec les responsables du HCGN, nous avons essayé de connaitre les raisons qui poussent les entreprises et structure de l'administration à mettre en place des solutions de téléphonie sur VOIP et une idée de l'estimation du retour sur investissement.

- Des informations secondaires ont été recueillies grâce à une étude documentaire ; nous avons notamment consulté Internet, des ouvrages.

Ainsi, nous avons eu recours à l'usage des études aussi bien qualitatives que quantitatives pour atteindre les objectifs de recherche qui ont été fixés.

En plus des éléments de recherches cités plus hauts, nous avons recours à l'internet qui est aujourd'hui, une source d'informations on ne peut plus indispensable. Cette forme de recherche s'est avérée très utile. Car elle nous a aidé à consulter des sites web spécialisés qui nous nous ont fourni des informations nous aidant ainsi à mieux cerner les concepts réseau et mieux comprendre VOIP.

## Section 4 : Observations

Une longue période d'observation des procédures techniques et administratives nous a permis d'avoir une description quasi générale de l'ensemble des entités qui composent le HCGN. C'est sur cette base que nous avons pu faire une critique de l'existant, en termes de communication.

## Section 5 : Difficultés rencontrées

Durant la période de rédaction du mémoire ainsi que celle de la réalisation de notre solution VOIP multi site, nous avions eu

quelques difficultés dont la principale était le manque de détail au niveau de l'information donnée par les officiers supérieurs de la HCGN. L'autre difficulté était le manque d'outils réels pour le test de cette solution.

# DEUXIEME PARTIE CADRES ORGANISATIONNEL ET CONCEPTUEL

# DEUXIEME PARTIE : Cadres Organisationnel et Conceptuel

## CHAPITRE TROIS : Cadre Organisationnel

### Section 1 : Présentation du Haut Commandement de la Gendarmerie :

La **Gendarmerie nationale guinéenne** est une force armée chargée des missions de police et placée sous la tutelle du ministère à la présidence chargée de la défense nationale. Contrairement aux policiers, ses membres sont des militaires. La Gendarmerie est l'une des plus anciennes institutions Guinéennes.

### Activité de la Gendarmerie :

La Gendarmerie est habituellement chargée de la sécurité dans les zones rurales et dans les zones périurbaines, alors que la Police nationale est chargée de cette mission dans les zones urbaines. Les deux forces ont ainsi chacune une zone de responsabilité propre, dites ZGN pour la Gendarmerie nationale, ou ZPN pour la Police nationale. La ZGN représente environ 75 % de la population guinéenne et 95 % du territoire national.

La Gendarmerie assure trois types de missions :

- Missions de police judiciaire ;
- Missions de police administrative ;
- Missions militaires de police et de défense.

## Implantation géographique

Le Haut commandement de la gendarmerie guinéenne direction de la justice militaire est situé dans le quartier boulbinet dans la commune de Kaloum.

ORGANIGRAMME

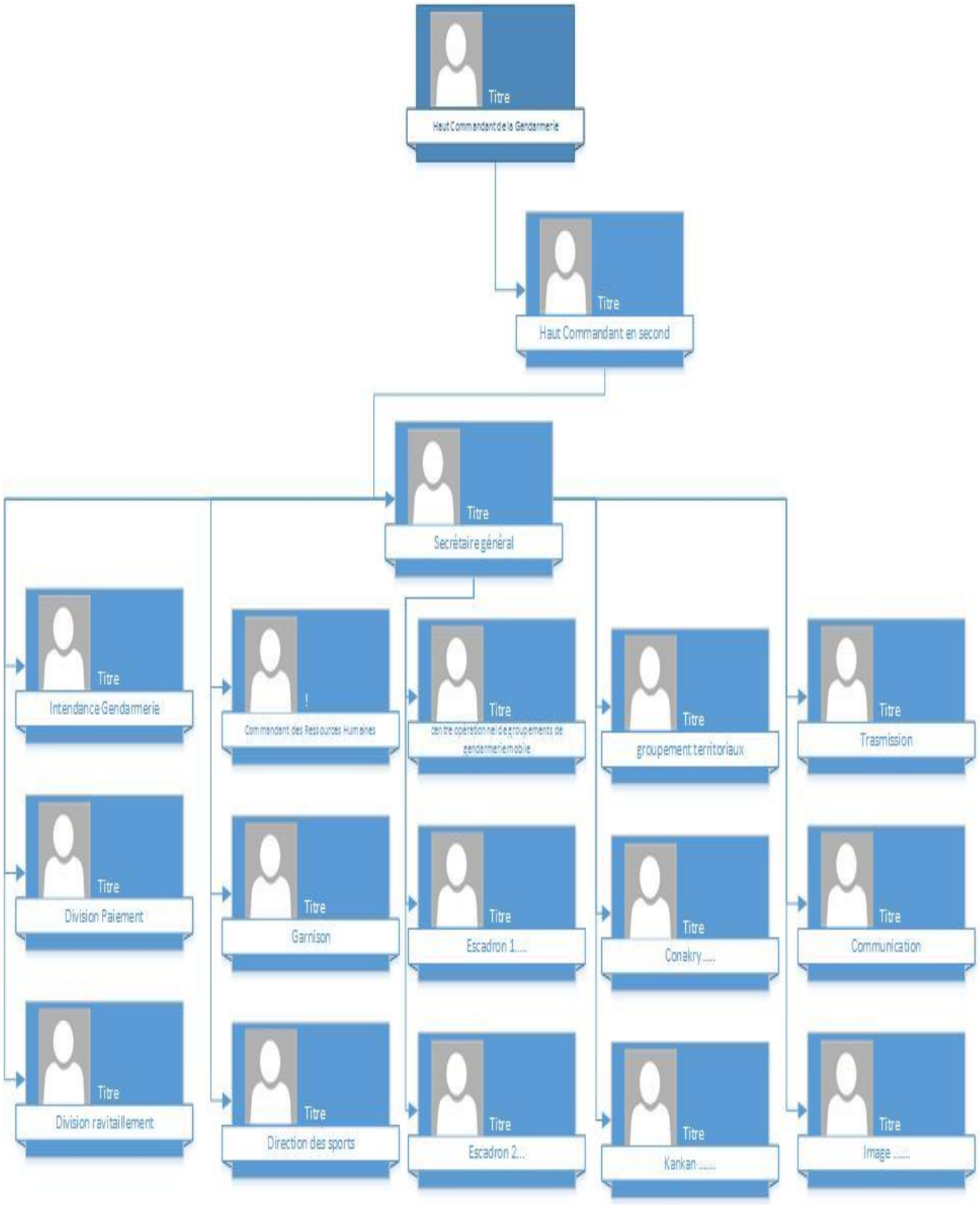


Figure 1 : Organigramme du Haut Commandement de la Gendarmerie Nationale

## Section 2 : Présentation de la Direction de la transmission

Une spécialité méconnue de la gendarmerie

Ce sont les gendarmes des sections des systèmes d'information et de communication qui assurent au quotidien la maintenance des installations de la gendarmerie.

La chaine des systèmes de communication est une composante intégrée et indissociable de l'action opérationnelle permanente de la gendarmerie. Les personnels qui la composent doivent répondre aux attentes quotidiennes en matière d'emploi des technologies de l'information dans l'engagement opérationnel (Police judiciaire, sécurité publique, sécurité des systèmes d'information, etc. …).

Ainsi, les gendarmes de cette spécialité reçoivent une formation interne de haut niveau, durant deux années, sanctionnée par un diplôme homologué de niveau III de l'enseignement technologique.

Ces militaires sont habilités au travail en hauteur, ils sont également appelés régulièrement à intervenir sur les mâts de radiocommunication installés sur les bâtiments (casernes et relais radio) de la gendarmerie.

La gendarmerie dispose donc de ses propres spécialistes SIC capables d'appuyer en permanence la manœuvre opérationnelle des unités sur n'importe quel théâtre d'opération (dans toutes les régions du pays ).

Les militaires de la Gendarmerie Nationale des Sections « SIC « (Systèmes d'Information et de Communication) sont d'abord des officiers et des sous-officiers de gendarmerie spécialistes qui appuient en tout temps et en tout lieu, l'action des unités opérationnelles, escadron de Gendarmerie mobile, les Compagnies de Gendarmerie départementale, des Transports aériens, bref toutes les unités PGHM, Brigades Territoriales (BT), etc… dans l'installation, la mise en œuvre et le dépannage des moyens de radio-télécommunication, des matériels et appareillages informatiques ainsi que de leurs différents

logiciels.

Le C.N.F.S.I.C.G. c'est le Centre National de Formation aux Systèmes d'Information et de Communication de la Gendarmerie.
On y forme des personnels de la gendarmerie pour tout ce qui touche au domaine des télécommunications & de l'informatique. Ce sont des spécialistes formés aux systèmes d'information et de communication.

Les spécialistes en question reviennent assez régulièrement au sein de cette structure dans le cadre de la formation continue, dans le cadre d'utilisation de nouvelles applications, de nouvelles technologies.

Il n'y a pas beaucoup de communication sur cette spécialité, c'est bien dommage…car c'est passionnant de travailler dans un tel domaine, pour qui aime les math l'électricité et l'électronique, s'intéresse aux technologies modernes en terme d'information et de communication ; en terme d'image, c'est probablement moins porteur que d'autres spécialités ou spécificités qui font partie de la gendarmerie

La chaine SIC est une composante intégrée et indissociable de l'action opérationnelle permanente de la gendarmerie.
Les SIC ont dans leurs attributions :
- l'informatique : installation et maintenance de réseaux, assistance aux utilisateurs, déploiement de matériels ou de logiciels, développement de logiciels pratiques, …
- la téléphonie : installation et gestion d'autocommutateurs de petite et grande capacité, dépannage…
- la radio : équipement complet des véhicules opérationnels, maintenance de sites relais, supervision du réseau départemental,
-l'appui N'TECH (Nouvelles technologies)

# Section 3 : Etude et critique du réseau existant

## I - Etude de l'existant

### I. 1 Présentation du réseau du Haut commandement de la gendarmerie guinéenne

Le réseau du Haut commandement de la gendarmerie, est un réseau hybride composé d'un réseau Ethernet commuté à 100 Mb/s et d'une station radio, il est basé sur la topologie étoile.
Le réseau ne contient aucun sous réseau, ce qui réduit ses performances compte tenu du nombre important du trafic qui en découle. Il a été bâti au fil des dernières années dans un contexte d'évolutions stratégiques importantes au sein de celle-ci et sans le support de document formalisé (de **type schéma directeur, Plan informatique,)** permettant de déterminer et de cadrer les axes de construction de ce SI.
De ce fait, le système d'information du **HCGN** se caractérise par un ensemble relativement hétérogène d'outils informatiques plus ou moins disparates et nécessitant d'importants moyens humains pour être alimentés.

### I .2 Architecture du réseau existant

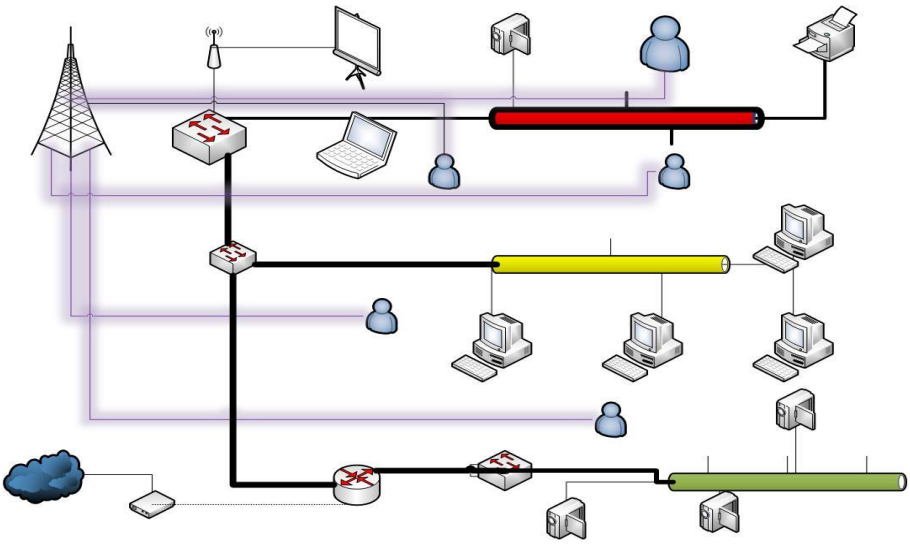


**Figure 2 : Architecture du réseau existant**

## I. 3 Explication Technique du réseau

L'architecture du SI du **HCGN** est caractérisé par :

Une station radio reliant le personnel du haut commandement aux autres sites du **HCGN** et du ministère de la défense nationale.

Un réseau local **(LAN)** Ethernet couvrant principalement le bâtiment administratif et disposant d'une connexion internet le reliant aux escadrons et autres divisions.

Un niveau de sécurisation de l'ensemble de la plateforme technologique quelque peu minimaliste et largement perfectible.

Un parc de postes de travail d'environ 100 PC (connectés au réseau du HCGN) relativement hétérogène aussi bien en termes de matériel que de logiciels installés.

Des caméras de surveillance sont relié aux réseaux.

Des talkiewalkies utilisés par les officiers et sous-officiers sont directement reliés à la station radio.

## I. 4 Inventaire du matériel et des logiciels existants

Le réseau du **HCGN** se compose d'environ :

- 3 commutateurs d'accès Cisco Catalyst 2960-X Series Switches
- 1 routeur de marque Cisco 800 Series Routers;
- Environs 100 talkiewalkies ;
- Plus de 100 PC utilisateurs

  Certains de ces équipements seront proposés dans la mise en œuvre de notre projet tandis que d'autres seront remplacés.

### I .4.2 Conception de Développement, Atelier de Génie Logiciel

Base de Données : SAARI ERP

### I .4.3 Les Serveurs

La base de données SAARI : c'est l'application destinée à la gestion et la comptabilité de la HCGN.

## II Critique de l'existant

L'analyse du réseau du HCGN, des équipements trouvés, ainsi que la politique d'organisation et de gestion, nous a permis de relever des avantages, mais aussi des inconvénients.

### II .1 Les avantages de l'architecture réseau

L'architecture du réseau est élaborée de manière à ce que son organisation repose sur une épine dorsale. Chaque niveau du bâtiment principal constitue un nœud auquel sont raccordées les salles s'y rattachant. Ces nœuds principaux sont à leur tour reliés au routeur et ce dernier relier à l'internet.

### II .1.1 les équipements d'interconnexion

Les équipements d'interconnexion (Switch, routeurs ...) sont nouveaux ils ont été mis en place en 2015 et permettent la réalisation de l'organisation logique à laquelle nous aspirons à savoir la téléphonie sur IP. En majorité de marque Cisco (switch Cisco Catalyst 2960-X Series Switches, switch TP- Link), ces équipements sont fournis avec leurs lOS et sont couverts par une garantie. Le Routeur est de marque Cisco 800 Series Routers.

De plus ces équipements connaissent une sécurité tant au niveau physique qu'électrique. Ils sont installés dans des armoires sécurisées et protégés par des onduleurs.

### II .1.2 le câblage

Les liaisons sont réalisées à l'aide de deux types de câble. La fibre optique (multimode et monomode) permet d'interconnecter les différents le bâtiment et les commandements dans les environs de HCGN avec tous les avantages qu'elle offre en matière de bande passante ou de sécurité. Quant à la paire torsadée, elle correspond aux meilleures spécifications (catégorie 5, EIA/TIA 568-A-5) et est utilisée pour les LANs du bâtiment.

## II.2 Les inconvénients

Les points faibles de l'architecture existante sont :

- ✓ Architecture vétuste
- ✓ Réseau non segmenté
- ✓ Importance des collisions dans le réseau
- ✓ Volume accru du trafic généré par chaque utilisateur
- ✓ Echange volumineux de fichiers non nécessaire entre utilisateurs
- ✓ Applications toujours plus complexes et fichiers plus volumineux
- ✓ Nécessité d'adaptateur de conversion du signal RJ45, FO.

- ✓ Aucune possibilité d'une administration et supervision centralisées au vu de l'éloignement physique des différentes entités
- ✓ Absence de politique de sécurité.
- ✓ Manque de documentation complète relative aux interventions et modifications effectuées sur le réseau.
- ✓ Accroissement rapide des utilisateurs

- ✓ Dysfonctionnement de certains équipements causé par les coupures de courant, entrainant une instabilité momentanée du réseau.
- ✓ L'absence de tâches de maintenance préventive de la poussière s'encrasse sur les équipements, faute d'un plan de maintenance préventive (nettoyage) bien établi. Ces dépôts de poussière peuvent être à la base de pannes qui affecteraient le réseau et entraîneraient des coûts de dépannage plus élevés.

# CHAPITRE QUATRIEME : Cadre Conceptuel

## Section 1 : Notions de base

### Notions de base sur les réseaux

Le réseau informatique est un ensemble d'équipements informatiques ou systèmes digitaux interconnecté entre eux via un milieu de transmission de données en vue partage de ressources informatiques et de la communication.

### I.CLASSIFICATION DES RÉSEAUX INFORMATIQUE

La classification se fait par rapport à un critère donné, ainsi nous pouvons classifier les réseaux informatiques de la manière suivante :

Classification selon leur étendue géographique ;

Classification selon les fonctions assumées par les ordinateurs ;

Classification selon la topologie.

### I.1 CLASSIFICATION SELON LEUR ETENDUE GEOGRAPHIQUE

Selon la taille géographique qu'occupe un réseau, on peut les classer en grandes catégories suivantes :

LAN (Local Area Network);

MAN (Metropolitan Area Network); WAN (Wide Area Network);

#### a) Le réseau LAN (local area network)

Les réseaux locaux connectent plusieurs ordinateurs situés sur une zone géographique relativement restreinte, tels qu'un domicile, un bureau, un bâtiment, un campus universitaire.

Ils permettent aussi aux entreprises de partager localement des fichiers et des imprimantes de manière efficace et rendent possibles les communications internes.

### b) Le réseau MAN (Métropolitain area network)

Tout réseau métropolitain est essentiellement un LAN, du point de vue de la technologie utilisée. Il peut couvrir un grand campus ou une ville.

### c) Le réseau WAN (Wide area network)

Pour des raisons économiques et techniques, les réseaux locaux (LAN) ne sont pas adaptés aux communications couvrant de longues distances.

C'est pour toutes ces raisons que les technologies des réseaux étendus (WAN) diffèrent de celles des réseaux locaux. Un WAN est un réseau à longue distance qui couvre une zone géographique importante (un pays, voir même un continent).

## I.1.2 CLASSIFICATION SELON LES FONCTIONS ASSUMEES PAR LES ORDINATEURS

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 ses 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.

### a) 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. Ce réseau est illustré par la Figure I.1

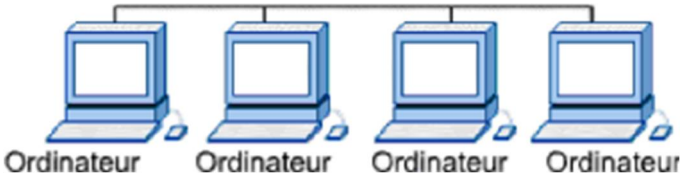



Figure I.1 : Schéma d'un réseau poste à poste

1. Avantages

Implémentation moins coûteuse ;

Ne requiert pas un système d'exploitation de réseau ; Ne requiert pas un administrateur de réseau dédié.

2. Inconvénients

Moins sécurisé

Chaque utilisateur doit être formé aux tâches d'administration

Rend donc vite l'administration très complexe.

### b) 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 importante assurent la fonction de serveurs. Les serveurs sont conçus pour gérer simultanément les requêtes de nombreux clients.

La figure I.2 illustré ce réseau

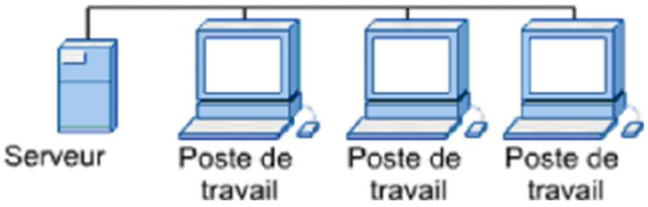



Figure I.2 : Schéma d'un réseau client serveur

Figure I.3 : Schéma réseau d'une topologie en bus

1. Avantages

Garantit une meilleure sécurité ;

Plus facile à administrer lorsque le réseau est étendu car l'administration est centralisée ;

Possibilité de sauvegarder toutes les données dans un emplacement central.

2. Inconvénients

Requiert l'utilisation d'un système d'exploitation de réseau, tel que NT, novelle Netware, Windows server 2003 etc. ...

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.

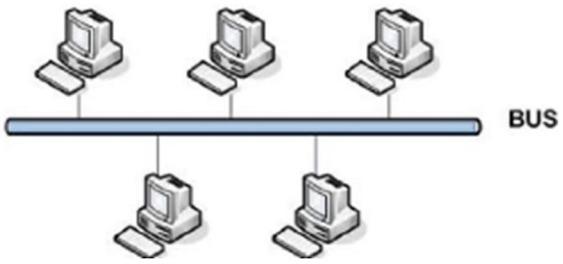
### 1.1.3 CLASSIFICATION SELON LA TOPOLOGIE RESEAU

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.

#### 1.1.3.1 TOPOLOGIE PHYSIQUE

La topologie physique du réseau se rapporte à la disposition des équipements et des supports. Ainsi, nous avons :

**a) Topologie 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.

Figure I.5 : Schéma réseau d'une topologie en anneau

### b) **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.

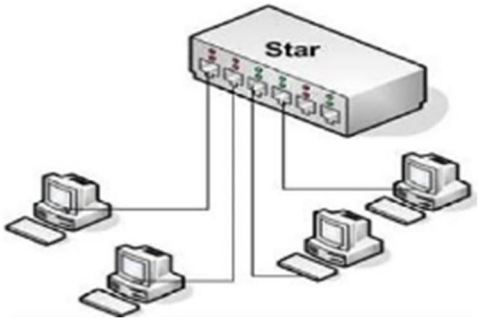
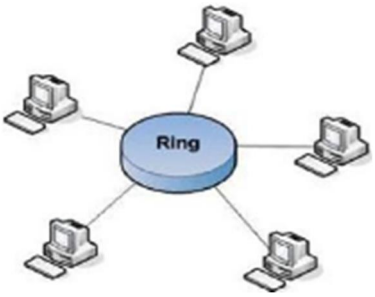



Figure I.4 : Schéma réseau d'une topologie en étoile

### c) **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 nœud 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.




### d) Topologie maillée

La topologie maillée permet de connecter tous les équipements, ou nœuds, 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.

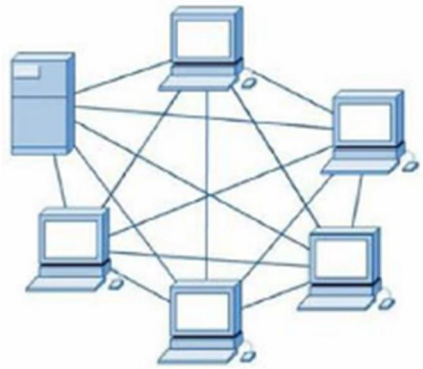


Figure I.6 : Schéma réseau d'une topologie maillée

## 1.1.3.2 TOPOLOGIE LOGIQUE

La topologie logique représente des voies par lesquelles sont transmis les signaux sur le réseau (mode d'accès des données aux supports et de transmission des paquets de données).

## 1.2 RAPPEL SUR LE RESEAU TELECOM

Les télécommunications sont définies comme la transmission à distance d'informations avec des moyens à base d'électronique et d'informatique. Ce terme a un sens plus large que son acception équivalente officielle « communication électronique ». Elles se distinguent ainsi de la poste qui transmet des informations ou des objets sous forme physique.

Dans les débuts des télécommunications modernes, des inventeurs comme Antonio Meucci, Alexander Graham Bell ou Guglielmo Marconi ont mis au point des dispositifs de communication comme le télégraphe, le téléphone ou la radio. Ceux-ci ont révolutionné les moyens traditionnels tels que les pavillons ou le télégraphe optique Chappe.

Actuellement, les télécommunications concernent généralement l'utilisation d'équipements électroniques associés à des réseaux analogiques ou numériques comme le téléphone fixe ou mobile, la radio, la télévision ou l'ordinateur. Celles-ci sont également une partie importante de l'économie et font l'objet de régulations au niveau mondial.

## 1.3 RAPPEL SUR LE PROTOCOLE IP

IP signifie « Internet Protocol », protocole Internet. Il représente le protocole réseau le plus répandu. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée. Ce protocole utilise ainsi une technique dite de commutation de paquets. Il apporte, en comparaison à Ipx/Spx et Netbeui, l'adressage en couche 3 qui permet, par exemple, la fonction principale de routage.

Il est souvent associé à un protocole de contrôle de la transmission des données appelé TCP, on parle ainsi du protocole TCP/IP. Cependant, TCP/IP est un ensemble de protocole dont voici les plus connu.

IP – Internet Protocol – Couche 3 – IP natif.

ARP – Address Resolution Protocol – Couche 3 – Résolution d'adresse IP en adresse MAC.

RARP – Reverse Address Resolution Protocol – Couche 3 – Résolution d'adresse MAC en adresse IP.

ICMP – Internet Control Message Protocol – Couche 3 – Gestion des messages du protocole IP.

IGMP – Internet Group Management Protocol – Couche 3 – Protocole de gestion de groupe.

TCP – Transmission Control Protocol – Couche 4 – Transport en mode connecté.

UDP – User Datagram Protocol – Couche 4 – Transport en mode non connecté.

## 1.4 SECURITE INFORMATIQUE

La sécurité des systèmes d'information (SSI) ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

### LA SÉCURITÉ INFORMATIQUE VISE GÉNÉRALEMENT CINQ 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.
- La **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.

# Section 2 : Considérations générales sur la VOIP

## II.1 INTRODUCTION

Dans ce chapitre, nous allons décrire le fonctionnement de la VoIP, ses protocoles, mais aussi les matériels adaptés à son implémentation.

Nous ferons également allusion aux avantages que cette nouvelle technologie occasionne lors qu'elle est mise en œuvre.

## II.2 PRESENTATION DE LA STRUCTURE VOIX SUR IP

### II.2.1 DEFINITION

La VoIP signifie Voice over Internet Protocol ou Voix sur IP (IP = Protocole Internet). Comme son nom l'indique, **la voix sur IP (VoIP)** désigne la technique d'acheminement des appels téléphoniques sur un réseau de données IP, qu'il s'agisse d'Internet ou du réseau IP interne propre à une entreprise.

On parle de la téléphonie sur IP **(Telephony Over IP ou ToIP)** quand, en plus de transmettre de la voix, on associe les services de téléphonie, tels l'utilisation de combinés téléphoniques, les fonctions de centraux téléphoniques (transfert d'appel, messagerie…), et bien entendu la liaison au réseau **RTC.**

### II.2.2 ARCHITECTURE DE LA VoIP

La VoIP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les trois principaux protocoles

utilisés sont H.323, SIP et MGCP/MEGACO. Il existe plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP. Certains placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence répartie à chaque périphérie. Chacune ayant ses avantages et ses inconvénients.

La figure II.1 décrit, de façon générale, la topologie d'un réseau de téléphonie IP.

Elle comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/ contrôleur de commutation, appelées Gatekeeper.

Dans une architecture VoIP, on trouve les éléments communs suivants :

Le routeur : permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs permettent de simuler un Gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP.

- ✓ La passerelle : permet d'interfacer le réseau commuté et le réseau IP.
- ✓ Le PABX : est le commutateur du réseau téléphonique classique. Il permet d'établir le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté (RTC). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.
- ✓ Les Terminaux : sont généralement de type logiciel (software phone) ou matériel (hard phone). Le softphone est installé dans le PC de l'utilisateur, l'interface audio peut être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé. Pour une meilleure clarté, un téléphone USB ou Bluetooth peut aussi être utilisé.
- ✓ Le hardphone est un téléphone IP qui utilise la technologie Voix sur IP pour permettre des appels téléphoniques sur un réseau IP, tel que l'Internet au lieu de l'ordinaire système PSTN. Les appels peuvent

parcourir par le réseau internet comme par un réseau privé. Un terminal utilise des protocoles comme le SIP (Session Initiation Protocol) ou l'un des protocoles propriétaires tel que celui utilisé par Skype. Cette Figure II.1 représente l'architecture d'un réseau VoIP.

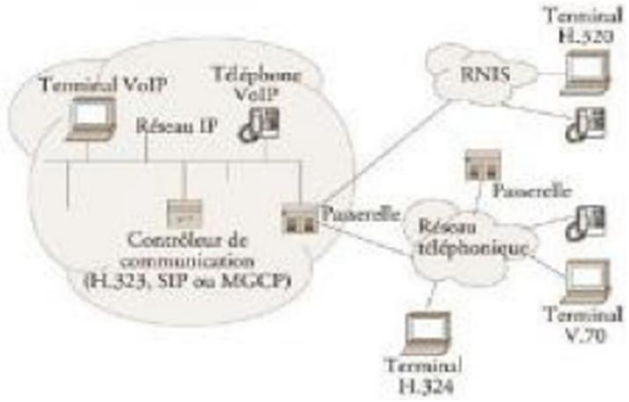



Figure II.1 : Architecture d'un réseau VoIP

## II.2.3 PRINCIPE DE FONCTIONNEMENT

Le principe de la voix sur IP est basé sur la numérisation de la voix, c'est-à-dire le passage d'un signal analogique à un signal numérique. Celui-ci est compressé en fonction des codecs choisis, cette compression a comme but de réduire la quantité d'information qui est transmise sur le réseau (comme par exemple la suppression des silences). Le signal obtenu est découpé en paquets, à chaque paquet on ajoute les entêtes propres au réseau (IP, UDP, RTP….) et pour finir, il est envoyé sur le réseau. Ce principe est illustré dans la figure II.2.

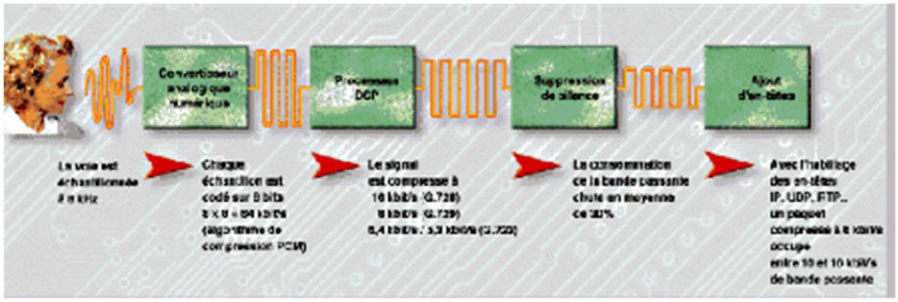


Figure II.2 : Passage du signal analogique au signal numérique

A l'arrivée, les paquets transmis sont réassemblés en supprimant d'abord les entêtes. Le signal de données ainsi obtenu est décompressé puis converti en signal analogique afin que l'utilisateur puisse écouter le message d'origine.

### II.2.4 LES CONTRAINTES DE LA VOIX SUR IP

La qualité du transport de la voix est affectée par les paramètres suivants :

- ✓ La qualité du codage ;
- ✓ Le délai d'acheminement (delay) ;
- ✓ La gigue (jitter) ;
- ✓ La perte de paquets (packetloss) ;
- ✓ L'écho.

Toutes ces contraintes déterminent la QoS (Quality of Service ou Qualité de service en français). Le transport de la voix sur IP implique l'utilisation de nombreux protocoles, tels : RTP, RTCP, H245, H225....

Des normes ont vu le jour afin que les équipements de différentes entreprises puissent Communiquer entre eux, la première fut H.323, puis arriva la norme SIP en second lieu.

#### II.2.4.1 QUALITE DU CODAGE

Généralement, plus le taux de compression est élevé par rapport à la référence de 64Kb/s (G711), moins la qualité de la voix est bonne. Toutefois, les algorithmes de compression récents permettent d'obtenir des taux de compression élevés, tout en maintenant une qualité de la voix acceptable. L'acceptabilité par l'oreille humaine des différents algorithmes est définie selon le critère MOS (Mean Operationnal Score), défini par l'organisme de normalisation internationale ITU (International Télécommunication Union / Union internationale des Télécommunications). Dans la pratique, les deux algorithmes les plus utilisés sont le G.729 et le G.723.1. Le tableau II.1 ci-après montre une liste de codecs avec leur débit correspondant :

**Tableau II.1:** Liste des codecs avec leur débit correspondant

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

### II.2.4.2 DELAI D'ACHEMINEMENT :

LATENCE (Delay) Selon la norme ITU G114, le délai d'acheminement permet :

- ✓ Entre 0 et 150 ms, une conversation normale ;
- ✓ Entre 150 et 300 ms, une conversation de qualité acceptable ;
- ✓ Entre 300 et 700 ms, uniquement une diffusion de voix en half duplex (mode talkie-walkie) Au-delà, la communication n'est plus possible.

Précisons que le budget temps (latence) est une combinaison du délai dû au réseau et du délai lié au traitement de la voix par le codec (algorithmes de compression/décompression de la voix). Dans la pratique, si l'on enlève le temps dû aux algorithmes de compression, il est impératif que le réseau achemine la voix dans un délai de 100 à 200 ms. Or, la durée de traversée d'un réseau IP est dépendante du nombre de routeurs traversés ; le temps de traversée d'un routeur étant lui-même fonction de la charge de ce dernier qui fonctionne par file d'attente.

### II.2.4.3 GIGUE (JITTER)

La gigue (variation des délais d'acheminement des paquets voix) est générée par la variation de charge du réseau (variation de l'encombrement des lignes ou des équipements réseau) et donc à la variation de routes dans le réseau. Chaque paquet est en effet susceptible de transiter par des combinaisons différentes de routeurs entre la source et la destination. Pour compenser la gigue, on peut utiliser des buffers (mémoire tampon) côté récepteur, afin de reconstituer un train continu et régulier de paquets voix. Toutefois, cette technique a l'inconvénient de rallonger le délai d'acheminement des paquets. Il est donc préférable de disposer d'un réseau à gigue limitée.

### II.2.4.4 PERTE DES PAQUETS

Lorsque les routeurs IP sont congestionnés, ils libèrent automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrants en fonction de seuils prédéfinis.

La perte de paquets est préjudiciable, car il est impossible de réémettre un paquet voix perdu, compte tenu du temps dont on dispose. Le moyen le plus efficace de lutter contre la perte d'informations consiste à transmettre des informations redondantes (code correcteur d'erreurs), qui vont permettre de reconstituer l'information perdue. Des codes correcteurs d'erreurs, comme le Reed Solomon, permettent de fonctionner sur des lignes présentant un taux d'erreur de l'ordre de 15 ou 20 %. Une fois de plus, ces codes correcteurs d'erreurs présentent l'inconvénient d'introduire une latence supplémentaire. Certains, très sophistiqués, ont une latence très faible.

### II.2.4.5 ECHO

L'écho est un phénomène lié principalement à des ruptures d'impédance lors du passage de 2 fils à 4 fils. Le phénomène d'écho est particulièrement sensible à un délai d'acheminement supérieur à 50 ms. Il est donc nécessaire d'incorporer un équipement ou un logiciel qui permet d'annuler l'écho.

## II.3 LES PROTOCOLES DE SIGNALISATION

Un protocole est un ensemble de spécifications décrivant les conventions et les règles à suivre dans un échange de données. Jusqu'à présent, il existe trois standard ou protocoles qui permettent la mise en place d'un service VoIP. Le plus connu est le standard H.323, ensuite, plus ancien le MGCP (Media Gateway Control Protocol) et le plus récent SIP. Notre étude sera basée sur les protocoles les plus utilisés : H323 et SIP que nous allons développer dans cette section.

## II.3.1 LE PROTOCOLE H.3236

### II.3.1.1 DESCRIPTION GENERALE DU PROTOCOLE H.323

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

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

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

-Les messages de signalisation sont ceux envoyés pour demander la mise en relation de deux clients, qui indique que la ligne est occupée ou que le téléphone sonne, etc.

En H.323, la signalisation s'appuie sur le protocole RAS pour l'enregistrement et l'authentification, le protocole Q.931 pour l'initialisation et le contrôle d'appel.

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

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

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

### II.3.1.2 ROLE DE COMPOSANTS

L'infrastructure H.323 repose sur quatre composants principaux : les terminaux, les Gateways, les Gatekeepers, et les MCU (Multipoint Control Unit). La figure II.3 représente les composants de l'architecture H.323.

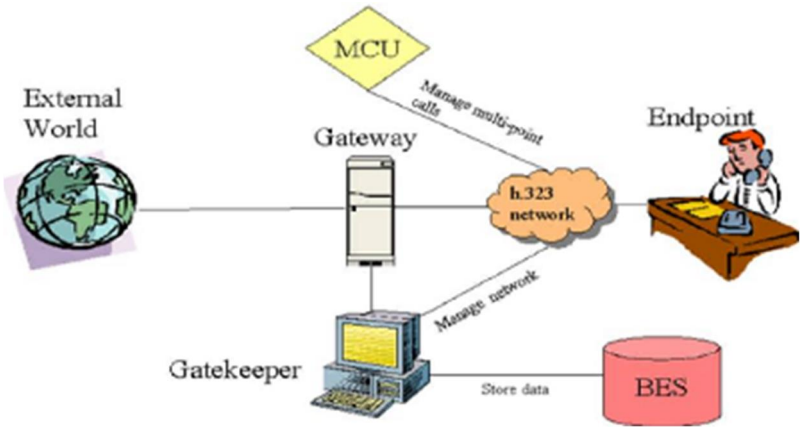



Figure II.3 : Les composants de l'architecture H.323

## A. LES TERMINAUX H.323

Le terminal peut être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet. Le minimum imposé par H.323 est qu'il mette en œuvre la norme de compression de la parole G.711, qu'il utilise le protocole H.245 pour la négociation de l'ouverture d'un canal et l'établissement des paramètres de la communication, ainsi que le protocole de signalisation Q.931 pour l'établissement et l'arrêt des communications.

Le terminal possède également des fonctions optionnelles, notamment, pour le travail en groupe et le partage des documents. Il existe deux types de terminaux H.323, l'un de haute qualité (pour une utilisation sur LAN), l'autre optimisé pour de petites largeurs de bandes (28,8/33,6 kbit/s - G.723.1 et H.263).

## B. GATEWAY OU PASSERELLE

Les passerelles H.323 assurent l'interconnexion avec les autres réseaux, ex:(H.320/RNIS), les modems H.324, les téléphones classiques, etc. Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodage audio).

## C. GATEKEEPER OU PORTIERS

Dans la norme H323, Le Gatekeeper est le point d'entrée au réseau pour un client H.323.

Il définit une zone sur le réseau, appelée zone H.323 (voir figure II.4 ci-dessous), regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dès l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe obtenu auprès de son Gatekeeper de rattachement.

Le Gatekeeper a pour fonctions :

- la translation des alias H.323 vers des adresses IP, selon les spécifications RAS (Registration/Admission/Status) ;

- le contrôle d'accès, en interdisant les utilisateurs et les sessions non Autorisés ;

- et la gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées.

Concrètement, une fraction de la bande passante est allouée à la visioconférence pour ne pas gêner les applications critiques sur le LAN et le support des conférences multipoint ad hoc.

Les composants du protocole H.323 sont représentés dans la figure II.4, qui constitue une zone H.323 :

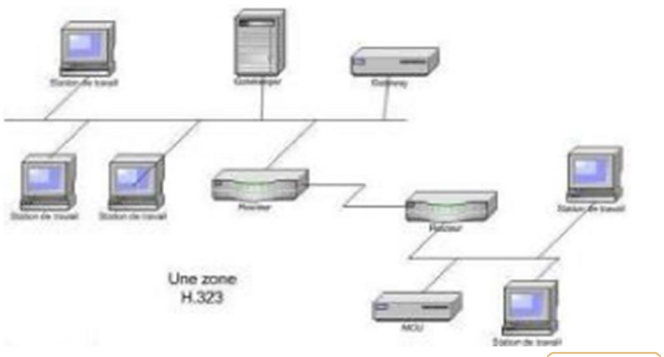


Figure II.4 : Zone H.323

### D. LES MCU

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

## II.3.1.3 LES AVANTAGES ET INCOVENIENTS DU PROTOCOLE H.3237 A. AVANTAGES

Les réseaux IP sont à commutation de paquets, les flux de données transitent en commun sur une même liaison. Les débits des réseaux IP doivent donc être adaptés en fonction du trafic afin d'éviter tout risque de coupure du son (et de la vidéo).

Tous les sites n'ont pas le même débit. Plus le débit sera élevé et plus le risque de coupure sera faible. Par ailleurs, tant que la qualité de service n'existera pas dans les réseaux IP, la fiabilité des visioconférences sur les lignes à faible débit sera basse.

Voici les principaux bénéfices qu'apporte la norme H.323 :

- ✓ **Codecs standards** : H.323 établit des standards pour la compression et la décompression des flux audio et vidéo. Ceci assure que des équipements provenant de fabricants différents ont une base commune de dialogue.

- ✓ **Interopérabilité** : Les utilisateurs peuvent dialoguer sans avoir à se soucier de la compatibilité du terminal destinataire. En plus d'assurer que le destinataire est en mesure de décompresser l'information, H.323 établit des méthodes communes d'établissement et de contrôle d'appel.
- ✓ **Indépendance vis à vis du réseau** : H.323 est conçu pour fonctionner sur tout type d'architecture réseau. Comme les technologies évoluent et les techniques de gestion de la bande passante s'améliorent, les solutions basées sur H.323 seront capables de bénéficier de ces améliorations futures.
- ✓ **Indépendance vis à vis des plates-formes et des applications** : H.323 n'est lié à aucun équipement ou système d'exploitation.
- ✓ **Support multipoint** : H.323 supporte des conférences entre trois terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.
- ✓ **Gestion de la bande passante** : Le trafic audio et vidéo est un grand consommateur de ressources réseau. Afin d'éviter que ces flux ne congestionnent le réseau, H.323 permet une gestion de la bande passante à disposition. En particulier, le gestionnaire du réseau peut limiter le nombre simultané de connexions H.323 sur son réseau ou limiter la largeur de bande à disposition de chaque connexion. De telles limites permettent de garantir que le trafic important ne soit pas interrompu.
- ✓ **Support multicast** : H.323 supporte le multicast dans les conférences multipoint. Multicast, c'est le fait d'envoyer un paquet vers un sous ensemble de destinataires sans réplication, permet une utilisation optimale du réseau.
- ✓ Indispensable pour permettre un minimum d'interopérabilité entre équipements de fournisseurs différents, ce standard présente toutefois les inconvénients suivants.

### B. INCOVENIENTS

H.323 est un protocole complexe, créé initialement pour les conférences multimédia et qui incorpore des mécanismes superflus dans un contexte purement téléphonique. Ceci a notamment des incidences au niveau des terminaux H.323 (téléphones IP, par exemple) qui nécessitent de ce fait une capacité mémoire et de traitement non sans incidence au niveau de leur coût.

Il comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité ou de plus petit dénominateur commun (dans le choix du codec, par exemple) ; D'autre part, comme le seul codec obligatoire est le codec G.711 (64 Kbps) et que le support des autres codecs plus efficaces est optionnel, l'interopérabilité entre produits provenant de constructeurs différents ne signifie pas qu'ils feront un usage optimal de la bande passante. En effet, dans le cas où les codecs à bas débits sont différents, le transport de la voix se fera à 64 Kbps, ce qui, en termes de bande passante, ne présente guère d'avantages par rapport à un système téléphonique classique.

Le protocole H.323 est une des normes envisageables pour la voix sur IP à cause de son développement inspiré de la téléphonie. Cependant, il est pour l'instant employé par des programmes propriétaires (Microsoft, etc.). La documentation est difficile d'accès car l'ITU fait payer les droits d'accès aux derniers développements de cette technologie, en dehors des efforts faits par le projet Open H.323 pour rendre cette technologie accessible à tous. Ainsi son adaptation au réseau IP est assez lourde. C'est pourquoi au fil des recherches est né le protocole SIP.

## II.3.2 LE PROTOCOLE SIP

### II.3.2.2 HISTORIQUE

SIP (Session Initiation Protocol) a été normalisé par le groupe de travail WG MMUSIC (Work Group Multiparty Multimedia Session Control) de l'IETF. La version 1 est sortie en 1997, et une seconde version majeure a été proposée en mars 1999 (RFC 2543). Cette dernière a elle-même été largement revue, complétée et corrigée en juin 2002 (RFC 3261). Des compléments au protocole ont été définis dans les RFC 3262 à 3265.

SIP est au sens propre un protocole de signalisation hors bande pour l'établissement, le maintien, la modification, la gestion et la fermeture de sessions interactives entre utilisateurs pour la téléphonie et la vidéoconférence, et plus généralement pour toutes les communications multimédias.

Le protocole n'assure pas le transport des données utiles, mais a pour fonction d'établir la liaison entre les interlocuteurs. Autrement dit, il ne véhicule pas la voix, ni la vidéo, mais assure simplement la signalisation. Il se situe au niveau de la couche applicative du modèle de référence OSI et fonctionne selon une architecture client-serveur, le client émettant des requêtes et le serveur exécutant en réponse les actions sollicitées par le client.

SIP fournit des fonctions annexes évoluées, comme la redirection d'appel, la modification des paramètres associés à la session en cours ou l'invocation de services. En fait, SIP ne fournit pas l'implémentation des services, mais propose des primitives génériques permettant de les utiliser. De cette manière, l'implémentation des services est laissée libre, et seul le moyen d'accéder aux services est fourni.

### II.4.1.1 ARCHITECTURE DE SIP

Contrairement à H.323, largement fondé sur une architecture physique, le protocole SIP s'appuie sur une architecture purement logicielle.

L'architecture de SIP s'articule principalement autour des cinq entités suivantes :

- ✓ Terminal utilisateur ;
- ✓ Serveur d'enregistrement ;
- ✓ Serveur de localisation ;
- ✓ Serveur de redirection ;
- ✓ Serveur proxy.

La figure II.5 illustre de façon générique les communications entre ces éléments. Un seul terminal étant présent sur cette figure, aucune communication n'est possible. Nous nous intéressons en fait ici aux seuls échanges entre le terminal et les services que ce dernier est susceptible d'utiliser lors de ses communications.

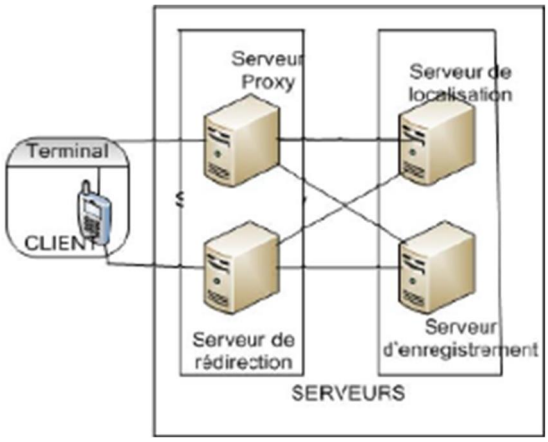



Figure II.5 : Architecture du protocole SIP

On peut schématiquement observer qu'il existe deux catégories de services :

L'un fourni au niveau de l'utilisateur (par le terminal), l'autre fourni au niveau des serveurs du réseau. Ces derniers sont répartis en deux classes : les serveurs de redirection et proxy, qui facilitent le routage des messages de signalisation et jouent le rôle d'intermédiaires, et les serveurs de localisation et d'enregistrement, qui ont pour fonction d'enregistrer ou de déterminer la localisation des abonnés du réseau.

### a) Terminal

Le terminal est l'élément dont dispose l'utilisateur pour appeler et être appelé. Il doit donc permettre de composer des numéros de téléphone. Il peut se présenter sous la forme d'un composant matériel (un téléphone) ou d'un composant logiciel (un programme lancé à partir d'un ordinateur).

Le terminal est appelé UA (User Agent), est constitué de deux sous-entités, comme illustré à la figure II.6 :


Figure II.6 : Communication entre UAC et UAS

- la partie cliente, appelée UAC (User Agent Client), chargée d'émettre les requêtes, initie un appel ;

- la partie serveur, appelée UAS (User Agent Server), est en écoute, reçoit et traite les requêtes, répond à un appel.

L'association des requêtes et des réponses entre deux entités de type UA constitue un dialogue.

Par analogie, on peut remarquer que la même chose se produit avec le protocole HTTP dans une application Web : un utilisateur exploite son navigateur comme client pour envoyer des requêtes et contacter une machine serveur, laquelle répond aux requêtes du client. La différence essentielle par rapport aux applications standards utilisant HTTP est qu'en téléphonie un terminal doit être à la fois utilisé pour joindre un interlocuteur et pour appeler. Chaque terminal possède donc la double fonctionnalité de client et de serveur.

Lors de l'initialisation d'un appel, l'appelant exploite la fonctionnalité client de son terminal (UAC), tandis que celui qui reçoit la communication exploite sa fonctionnalité de serveur (UAS).

La communication peut être clôturée indifféremment par l'User Agent Client ou l'User Agent Server.

De nombreuses implémentations de clients SIP sont disponibles sur les plates-formes les plus courantes, Windows, Linux ou Mac. Elles sont le plus souvent gratuites, sous licence GPL.

Parmi les clients SIP les plus réputés, citons notamment les suivants :

- ✓ X-Lite Free;
- ✓ 3CX Phone Free;
- ✓ Phone Gaim;
- ✓ Wengo.

Ces clients SIP disposent de diverses fonctionnalités améliorées. En choisir un est souvent affaire de goût, selon l'ergonomie du logiciel et les caractéristiques souhaitées (support d'un codec particulier, support de la messagerie instantanée, etc.).

### b) **Serveur d'enregistrement**

Deux terminaux peuvent communiquer entre eux sans passer par un serveur d'enregistrement, à condition que l'appelant connaisse l'adresse IP de l'appelé. Cette contrainte est fastidieuse, car un utilisateur peut être mobile et donc ne pas avoir d'adresse IP fixe, par exemple s'il se déplace avec son terminal ou s'il se connecte avec la même identité à son lieu de travail et à son domicile. En outre, l'adresse IP peut être fournie de manière dynamique par un serveur DHCP.

Le serveur d'enregistrement (Register Server) offre un moyen de localiser un correspondant avec souplesse, tout en gérant la mobilité de l'utilisateur. Il peut en outre supporter l'authentification des abonnés.

Dans la pratique, lors de l'activation d'un terminal dans un réseau, la première action initiée par celui-ci consiste à transmettre une requête d'enregistrement auprès du serveur d'enregistrement afin de lui indiquer sa

présence et sa position de localisation courante dans le réseau. C'est la requête REGISTER, que nous détaillons plus loin, que l'utilisateur envoie à destination du serveur d'enregistrement. Celui-ci sauvegarde cette position en l'enregistrant auprès du serveur de localisation.

L'enregistrement d'un utilisateur est constitué par l'association de son identifiant et de son adresse IP. Un utilisateur peut s'enregistrer sur plusieurs serveurs d'enregistrement en même temps. Dans ce cas, il est joignable simultanément sur l'ensemble des positions qu'il a renseignées.

### c) Serveur de localisation

Le serveur de localisation (Location Server) joue un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation de l'abonné.

Ce serveur contient la base de données de l'ensemble des abonnés qu'il gère. Cette base est renseignée par le serveur d'enregistrement. Chaque fois qu'un utilisateur s'enregistre auprès du serveur d'enregistrement, ce dernier en informe le serveur de localisation.

Presque toujours, le serveur de localisation et le serveur d'enregistrement sont implémentés au sein d'une même entité. On parle alors souvent non pas de serveur de localisation, mais de service de localisation d'un serveur d'enregistrement, tant que ces fonctionnalités sont proches et dépendantes.

Les serveurs de localisation peuvent être collaboratifs. Le fonctionnement d'un serveur d'enregistrement est analogue à celui d'un serveur DNS dans le monde Internet : pour joindre un site Internet dont on ne connaît que le nom, il faut utiliser un serveur DNS, qui effectue la conversion (on parle de résolution) du nom en adresse IP. Ce serveur a connaissance d'une multitude d'adresses, qu'il peut résoudre parce qu'elles appartiennent à son domaine ou qu'il a la capacité d'apprendre dynamiquement en fonction des échanges qu'il voit passer. Dès qu'un nom lui est inconnu, il fait appel à un autre DNS, plus important ou dont le domaine est plus adéquat. De la même

manière, les serveurs de localisation prennent en charge un ou plusieurs domaines et se complètent les uns les autres.

### d) Serveur de redirection

Le serveur de redirection (Redirect Server) agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur.

L'appelant envoie une requête de localisation d'un correspondant (il s'agit en réalité d'un message d'invitation, qui est interprété comme une requête de localisation) au serveur de redirection. Celui-ci joint le serveur de localisation afin d'effectuer la requête de localisation du correspondant à joindre. Le serveur de localisation répond au serveur de redirection, lequel informe l'appelant en lui fournissant la localisation trouvée. Ainsi, l'utilisateur n'a pas besoin de connaître l'adresse du serveur de localisation.

### e) Serveur proxy

Le serveur proxy (parfois appelé serveur mandataire) permet d'initier une communication à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux des interlocuteurs et agit pour le compte de ces derniers.

Le serveur proxy remplit les différentes fonctions suivantes :

- ✓ Localiser un correspondant ;
- ✓ Réaliser éventuellement certains traitements sur les requêtes ;
- ✓ Initier, maintenir et terminer une session vers un correspondant.

Lorsqu'un utilisateur demande à un serveur proxy de localiser un correspondant, ce dernier effectue la recherche, mais au lieu de retourner le résultat au demandeur (comme le ferait un serveur de redirection), il utilise cette réponse pour effectuer lui-même l'initialisation de la communication en invitant le correspondant à ouvrir une session.

Bien que fournissant le même type de service de localisation qu'un serveur de redirection, un serveur proxy va donc plus loin que la simple localisation, en initiant la mise en relation des correspondants de façon transparente pour le client. Il peut acheminer tous les messages de signalisation des terminaux, de l'initialisation de la communication à sa terminaison, en passant par sa modification. En contrepartie, le serveur proxy est une entité beaucoup plus sollicitée que le serveur de redirection, et donc plus lourde.

Chaque terminal peut et devrait en principe disposer d'un tel serveur sur lequel se reposer pour interpréter, adapter et relayer les requêtes. En effet, le serveur proxy peut reformuler une requête du terminal UAC afin de la rendre compréhensible par le serveur auquel s'adresse l'UAC. Cela accroît la souplesse d'utilisation du terminal et simplifie son usage. Les serveurs proxy jouent aussi un rôle collaboratif, puisque les requêtes qu'ils véhiculent peuvent transiter d'un serveur proxy à un autre, jusqu'à atteindre le destinataire. Notons que le serveur proxy ne fait jamais transiter de données multimédias et qu'il ne traite que les messages SIP.

Le proxy est une entité très souvent utilisée dans la pratique.

Par analogie avec l'architecture illustrée à la figure II.7, symbolisant l'organisation des communications, on parle souvent du trapèze SIP pour désigner l'ensemble formé par ces quatre entités.

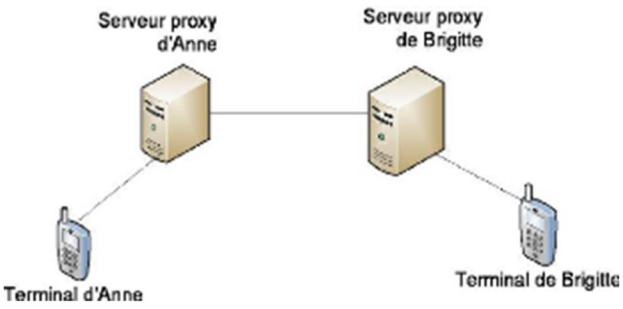



Figure II.7 : Trapèze SIP

On distingue deux types de serveurs proxy, à savoir :

- Proxy statefull, qui maintient pendant toute la durée des sessions l'état des connexions.

- Proxy stateless, qui achemine les messages indépendamment les uns des autres, sans sauvegarder l'état des connexions.

Les proxys stateless sont plus rapides et plus légers que les proxys statefull, mais ils ne disposent pas des mêmes capacités de traitement sur les sessions.

### II.4.1.2 L'ADRESSAGE SIP

L'objectif de l'adressage est de localiser les utilisateurs dans un réseau. C'est une des étapes indispensables pour permettre à un utilisateur d'en joindre un autre.

Pour localiser les utilisateurs, il faut pouvoir les identifier de manière univoque. SIP propose des moyens très performants pour nommer les utilisateurs, grâce au concept d'URI, classique sur Internet, que nous allons détailler avant de voir son utilisation par SIP.

Un URI est formé d'une chaîne de caractères. Sa syntaxe a été définie au CERN (Centre Européen pour la Recherche Nucléaire) de Genève, par Tim Berners-Lee dès 1989, dans le cadre du système d'hyperliens (liens hypertextes) qu'il proposait la même année. Cette syntaxe a été normalisée par l'IETF en août 1998 dans la RFC 2396 puis révisée de nombreuses fois, notamment dans la RFC 2396bis, et reprise en janvier 2005 dans la RFC 3986.

À la différence d'un URI, une URL se contente d'apporter une localisation et non une définition de la ressource. Ainsi, un même document peut se trouver à deux emplacements différents, donc à deux URL différentes dans le réseau Internet, alors qu'il fait référence à une même ressource.

### II.4.1.3 FORMAT DES ADRESSES SIP

Tout utilisateur SIP dispose d'un identifiant unique. Cet identifiant constitue l'adresse de l'utilisateur permettant de le localiser.

Le format d'une adresse SIP (ou URL SIP) respecte la RFC 3986 (nommée Uniform Resource Identifier : Generic Syntax) et se présente sous la forme illustrée à la figure II.8

sip: identifiant[:mot_de_passe]@serveur[paramètres]

Figure II.8 : Syntaxe d'une adresse SIP

On distingue dans cette adresse plusieurs parties, telle que :

- le mot-clé sip qui spécifie le protocole à utiliser pour la communication. Par analogie avec le Web (où une page est référencée par une adresse de type *http://monsite*), l8e mot-clé *sip* précise que ce qui va suivre est l'adresse d'un utilisateur ;

- la partie *identifiant* qui définit le nom ou le numéro de l'utilisateur. Cet identifiant est nécessairement unique pour désigner l'utilisateur de manière non ambiguë ;

- La partie *mot_ de_passe* qui est facultative. Le mot de passe peut être utile pour s'authentifier auprès du serveur, notamment à des fins de facturation. C'est aussi un moyen pour joindre un utilisateur qui a souhaité s'enregistrer sur l'équivalent d'une liste rouge : sans la connaissance de ce mot de passe, le correspondant n'est pas joignable.

De manière générale, cette possibilité offre le moyen de restreindre l'utilisation de certains services.

- la partie *serveur* qui spécifie le serveur chargé du compte SIP dont l'identifiant précède l'arobase. Le serveur est indiqué par son adresse IP ou par un nom qui sera résolu par DNS. Des paramètres URI peuvent être associés à ce nom. C'est ce serveur qui sera contacté pour joindre l'abonné correspondant. Un port peut être spécifié à la suite du serveur ;

- la partie *paramètres* est facultative. Les paramètres permettent soit de modifier le comportement par défaut (par exemple, en modifiant les protocoles de transport ou les ports, ou encore le TTL par défaut), soit de spécifier des informations complémentaires (par exemple, l'objet d'un appel qui sera envoyé à l'appelé en même temps que l'indication d'appel, à la manière d'un e-mail précisant l'objet du message).

**Tableau II.3** : Exemples d'adresses SIP commentées.

| **Adresse SIP** | **Commentaire** |
|---|---|
| <*sip:guy.laurent@123.123.123.123*> | C'est le format le plus commun. L'identifiant de l'utilisateur est spécifié par un nom ou un pseudonyme, *bakaramoko*. Après l'arobase est spécifiée l'adresse IP du serveur en charge de la gestion du compte de *bakaramoko*. Cette adresse IP étant fixe, il n'est pas nécessaire de la résoudre par un DNS, et il est possible de contacter directement ce serveur. L'IP fixe n'est généralement pas pratique, car une adresse fixe oblige le fournisseur d'accès à conserver ses mécanismes d'adressage ou à avertir ses utilisateurs de toute modification. |
| <*sip:+22145555555:mon_pass123* | Le premier nombre (*+22145555555*) est le numéro |
| *@ma_passerelle_rtc*> | de téléphone du correspondant. On peut supposer qu'il s'agit d'un numéro géographique et que le correspondant est actif dans le réseau RTC. Pour |

| | |
|---|---|
| | joindre ce réseau, il faut passer par une passerelle, donnée juste après l'arobase, dont le nom est *ma_passerelle_rtc*. L'utilisation d'un mot de passe |
| | (*mon_pass123*) permet à l'appelant de s'authentifier auprès du serveur *ma_passerelle_rtc*pour avoir le droit d'émettre l'appel (notamment pour la facturation). |

On retiendra deux avantages de l'adressage SIP :

- l'adressage est indépendant de la localisation géographique des abonnés. SIP est conçu pour assurer la mobilité de ses utilisateurs, et donc permettre de joindre quelqu'un avec une adresse SIP unique, quels que soient sa localisation et son terminal. Le réseau peut toutefois adopter un plan de numérotation selon n'importe quel critère, comme la localisation géographique, sans que cela soit gênant ;

- Un utilisateur peut avoir plusieurs adresses SIP aboutissant toutes au même terminal.

Par exemple, si quelqu'un souhaite différencier son adresse SIP professionnelle de son adresse SIP personnelle, il peut utiliser un même terminal référencé sur deux adresses distinctes. Il lui est alors possible d'activer la messagerie de son compte personnel pendant son travail et, le week-end, de rediriger les appels sur son adresse professionnelle vers un centre de permanence. Le tout en utilisant un terminal unique.

Ce mécanisme d'adressage particulièrement souple permet de supporter la mobilité des utilisateurs et le monde Internet.

### II.4.1.4 LES MESSAGES SIP

Les messages SIP sont décrits dans la RFC 822, qui définit la syntaxe à la fois des requêtes et des réponses. On y trouve une très forte influence des autres protocoles de l'IETF, principalement HTTP et SMTP. Le format des requêtes et réponses est en effet similaire à celui utilisé dans le protocole HTTP, et les en-têtes s'apparentent à celles utilisées dans le protocole SMTP. On y retrouve par ailleurs le concept d'URL.

### II.4.1.5 LES REQUETTES SIP

La version actuelle de SIP prévoit 6 requêtes distinctes, permettant l'établissement d'un appel, la négociation des capacités (types de média, paramètres de la session, éléments de sécurité) ou la fermeture d'une session. Ces requêtes sont détaillées dans le tableau II.4.

**Tableau II.4** : Les requêtes SIP

| **Requête** | **Définition** |
|---|---|
| INVITE | Requête d'établissement d'une session, invitant un usager (humain ou non) à participer à une communication téléphonique ou multimédia ; l'émetteur de cette requête y indique les types de média qu'il souhaite et peut recevoir, en général au travers d'une description de session SDP (Session Description Protocol). |
| ACK | Requête d'acquittement, émise pour confirmer que le client émetteur d'un INVITE précédent a reçu une réponse finale ; cette requête peut véhiculer une description de session qui clôt la négociation. |
| BYE | Requête de clôture d'un appel. |
| CANCEL | Requête d'annulation, signifiant au serveur de détruire le contexte d'un appel en cours d'établissement (cette requête n'a pas d'effet sur un appel en cours). |

| | |
|---|---|
| OPTIONS | Cette requête permet à un client d'obtenir de l'information sur les capacités d'un usager, sans pour autant provoquer l'établissement d'une session. |
| REGISTER | Requête à destination d'un serveur SIP et permettant de lui faire parvenir de l'information de localisation (machine sur laquelle se trouve l'utilisateur). |

### II.4.1.6 LES REPONSES SIP

Après réception et traitement d'une requête, un agent ou un serveur SIP génère un message de réponse (succès ou échec du traitement). Ces réponses sont codées par une séquence de trois chiffres, où le premier est un code de classe. Le tableau II.5 donne quelques réponses SIP possibles.

**Tableau II.5** : Les réponses SIP

| **Code** | **Définition de la famille de réponse** | **Principales réponses** |
|---|---|---|
| 1XX | Réponse intermédiaire d'information (traitement en cours) | 100 Trying 180 Ringing |
| 2XX | Succès | 200 OK |
| 3XX | Redirection | 301 Moved permanently<br>302 Moved temporarily |
| 4XX | Erreur client | 400 Bad Request<br>401 Unauthorized |
| 5XX | Erreur serveur | 500 Server Internal Error<br>501 Not Implemented |
| 6XX | Echec global du traitement | 600 Buzy Everywhere 603 Decline |

## II.4.1.7 SCENERIOS DE COMMUNICATION

Nous allons illustrer la succession chronologique des messages de requêtes et de réponses dans les six scénarios classiques suivants :

1. Initialisation d'une communication directe ;

2. Enregistrement d'un terminal ;

3. Initialisation d'une communication avec un serveur proxy ;

4. Localisation par un serveur de redirection et initialisation d'appel directe ;

5. Modification dynamique d'une communication SIP ;

6. Terminaison d'une communication.

### 1. Initialisation d'une communication directe

Une communication peut s'effectuer directement entre deux correspondants, sans faire intervenir d'autres entités.

Dans ce cas, l'appelant doit connaître la localisation (sous forme d'adresse IP) de la personne qu'il souhaite contacter. La figure II.9 illustre ce scénario.

Terminal SIP

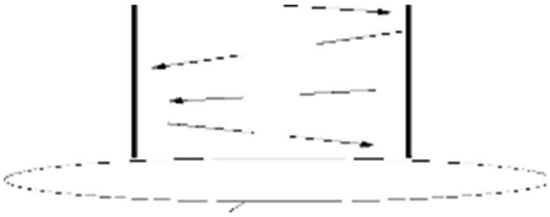
Appelant

(UAC)

Terminal SIP

Appelé

(UAS)




*Initiation d'une communication directe*

Figure II.9 : Initiation d'une communication directe

Cette communication reflète la simplicité d'utilisation du protocole SIP. Quatre étapes seulement suffisent pour mettre en relation les deux utilisateurs :

1. l'appelant (UAC) envoie un message (requête INVITE) proposant à son correspondant (UAS) d'initier une communication. Ce message contient les paramètres désirés pour établir la communication ;

2. dès que l'UAS reçoit le message, il en informe l'utilisateur appelant (le téléphone sonne, avec indication de l'appelant et du motif de son appel s'il a renseigné ce champ, ainsi que des services disponibles). Dans le même temps, il indique à l'appelant (par une réponse provisoire *180* RINGING) que l'appelé est en train d'être averti de l'appel ;

3. dès que l'appelé accepte l'appel (en décrochant), l'UAS informe l'appelant (par une réponse définitive *200* OK) que l'appel peut débuter. Ce message contient les paramètres que l'UAS supporte pour la session ;

4. l'UAC retourne à l'UAS un message d'acquittement (requête ACK) lui indiquant qu'il a pris note que l'appel peut débuter. Ce message comporte les paramètres fixés pour la session, qui tiennent compte de ces possibilités et de celles de l'UAS. Les intervenants sont ensuite mis en relation et peuvent communiquer.

## 2. Enregistrement d'un terminal

Lorsqu'un terminal est activé dans un réseau, sa première action consiste à se déclarer auprès d'un serveur d'enregistrement, de manière à être disponible si un appelant souhaite le joindre. Ce scénario est illustré à la figure II.10.

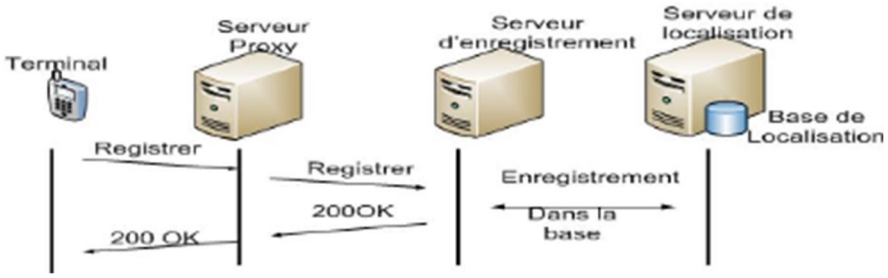



Figure II.10 : Enregistrement d'un terminal SIP

Le serveur de localisation maintient dans sa base de données une entrée associant l'identifiant d'un utilisateur avec sa position dans le réseau (adresse IP du terminal de l'utilisateur, port utilisé par l'application SIP et identifiant de l'utilisateur sur ce poste).

## 3. Initialisation d'une communication SIP avec un serveur proxy

Les étapes et messages envoyés pour initier une session entre deux correspondants dans le cas où un proxy est utilisé sont illustrés à la figure II.11. Dans cet exemple, Anne souhaite ouvrir une session avec Brigitte. Comme elle ne connaît pas la localisation de cette dernière, elle sollicite son proxy afin de la déterminer.

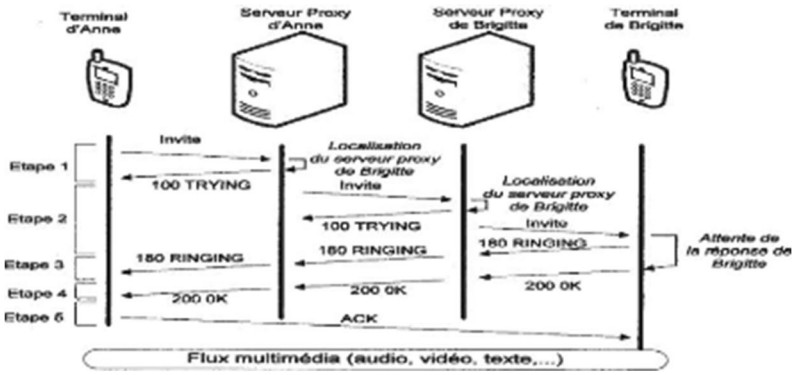



Figure II.11 : Initialisation d'un appel avec un proxy

Les étapes suivantes sont nécessaires :

1. Anne compose sur son terminal l'adresse SIP de Brigitte. Cette dernière n'est pas nécessairement une adresse IP, mais peut être un identifiant qu'il faut résoudre. Un message d'invitation (requête INVITE) est envoyé de l'UAC d'Anne vers son serveur proxy SIP. L'adresse du proxy d'Anne peut être configurée sur son terminal ou être automatiquement distribuée, par DHCP par exemple. À la réception de ce message, le serveur proxy d'Anne utilise la partie domaine de l'adresse SIP de Brigitte pour déterminer le serveur en charge de la gestion du compte de Brigitte (c'est-à-dire en charge du domaine de Brigitte). À cette fin, un serveur DNS peut être sollicité pour localiser le serveur proxy de Brigitte. En parallèle, le serveur proxy informe Anne qu'il prend en charge la requête et tente de la mettre en relation. La réponse temporaire *100* TRYING indique à cette dernière que le message a été reçu et qu'il est en cours de traitement ;

2. Routage du message d'invitation. Le serveur proxy d'Anne transmet l'invitation au serveur proxy de Brigitte après l'avoir localisé. C'est le message d'invitation original qui est intégralement relayé du proxy d'Anne vers celui de Brigitte. La seule modification apportée au message par le premier serveur proxy concerne le champ VIA, qui liste l'ensemble des machines parcourues lors de l'acheminement du paquet, et auquel il ajoute sa propre adresse réseau (en plus de celle d'Anne, qui y figure initialement) ;

Le serveur proxy de Brigitte informe le serveur proxy d'Anne (par un message de réponse temporaire *100* TRYING) de la réception de la requête et de la tentative d'initialisation. Parallèlement, il recherche la localisation du terminal de Brigitte en utilisant le service de localisation. Une fois la position du terminal dans le réseau trouvé, il lui transmet l'invitation d'Anne. À nouveau, ce message est conforme à l'original, et seul le champ VIA a été enrichi de l'adresse du serveur proxy de Brigitte ;

3. Le terminal de Brigitte sonne, (éventuellement un softphone) et reçoit l'invitation et la fait connaître à l'utilisateur Brigitte, le plus souvent par une sonnerie. En parallèle, il indique à son proxy (par un message *180* RINGING) que l'appel est en train d'être notifié à Brigitte et que la communication est en attente de son acceptation. Ce message informatif est relayé jusqu'à l'émettrice Anne, qui reçoit généralement un retour audio ou visuel (une tonalité de sonnerie particulière le plus souvent). L'utilisation du champ d'en-tête VIA permet de remonter de proche en proche jusqu'à Anne selon le même chemin ;

4. Brigitte répond au téléphone. On suppose le cas où Brigitte a choisi de répondre à l'appel. À l'instant où elle décroche, l'UAS retourne à l'UAC un message *200* OK pour l'informer que l'appel est accepté. Ce message est relayé par les différents proxys. À ce stade, la communication n'a pas encore débuté, et aucun son n'est transmis ;

5. Le terminal d'Anne confirme les paramètres d'appel. En tenant compte des capacités prises en charge par les correspondants, le terminal d'Anne envoie un message d'acquittement ACK qui spécifie les paramètres définitifs à utiliser lors de cette session. Notons que le message d'acquittement peut passer directement d'un interlocuteur à l'autre, sans transiter par les serveurs proxy. À ce stade, chacun des utilisateurs a pu apprendre la localisation exacte de son interlocuteur, et il n'est donc plus nécessaire de recourir aux serveurs proxy. Toutes les transactions qui suivent sont effectuées directement, de poste utilisateur à poste utilisateur.

Ainsi, les serveurs proxy sont sollicités au minimum. De la même manière, pour ne pas saturer les serveurs proxy inutilement, les flux de données multimédias ne transitent jamais par eux.

À la réception de ce message, la communication entre les interlocuteurs peut débuter. Tous ces échanges n'ont réclamé que quelques millisecondes, imperceptibles pour les intervenants.

Globalement, on retrouve dans cet appel, les trois phases fondamentales de l'appel direct entre les correspondants :

1. Requête INVITE : invitation de l'appelant ;

2. Réponse *200* OK : acceptation par l'appelé ;

3. Acquittement ACK : confirmation par l'appelant.

Il s'agit des trois messages nécessaires à la modification dynamique d'une communication SIP. Les autres messages concernent essentiellement la localisation ou sont à titre informatif.

## 4. Localisation par un serveur de redirection et initialisation d'appel direct

La figure II.12 illustre le scénario où un serveur de redirection est utilisé par le terminal appelant afin de localiser son correspondant et pour l'échange qui s'ensuit. L'objectif est toujours de mettre en relation le terminal d'Anne avec celui de Brigitte, mais par un autre moyen.

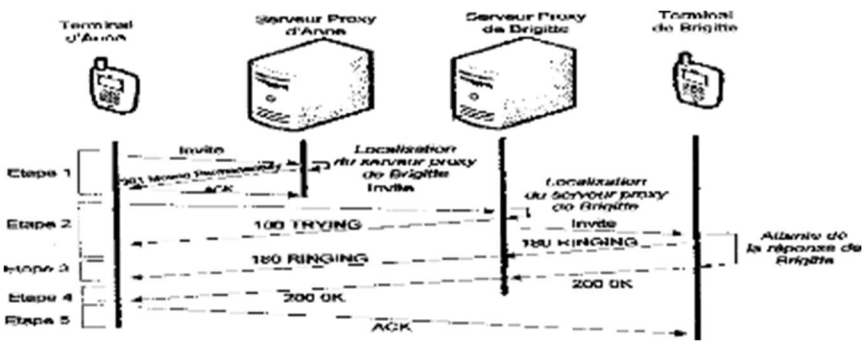


Figure II.12 : Localisation avec un serveur de redirection et initialisation d'appel direct

Dans la première étape, le terminal d'Anne sollicite le serveur de redirection pour déterminer sa localisation. Une fois cette recherche effectuée, la réponse est envoyée directement au terminal d'Anne, lequel initie l'appel lui-même, en contactant le serveur proxy de Brigitte.

Les étapes qui suivent sont identiques à celles du scénario précédent avec l'initialisation d'appel par un serveur proxy, si ce n'est que ce dernier n'intervient pas dans les échanges intermédiaires.

## 5. Modification d'une communication SIP

Lorsqu'un utilisateur est en communication, il peut arriver qu'il souhaite modifier les paramètres de cette communication tout en la conservant active. Par exemple, s'il commence un téléchargement et que son débit risque de diminuer en conséquence, il peut souhaiter utiliser un codec moins gourmand. Dans un autre cas, l'utilisateur peut vouloir enrichir la communication audio avec une diffusion vidéo. Ou encore, il peut souhaiter inviter à une conférence un nouveau correspondant, qui ne supporte pas le codec utilisé par les autres conférenciers.

Ces cas sont parfaitement envisageables avec le protocole SIP, qui offre, rappelons-le, une très grande souplesse. À tout moment, l'appelant ou l'appelé peut envoyer un nouveau message d'invitation, avec la requête INVITE, afin de renégocier les paramètres de la communication. Bien sûr, dans ce contexte, le message n'a pas pour objectif d'inviter à une nouvelle session, mais d'utiliser de nouveaux paramètres.

C'est pour cette raison qu'on nomme **RE**-INVITE ce type de requête d'invitation. Du reste, la communication en cours n'est pas interrompue par la réception de cette requête. S'il accepte les modifications sollicitées dans la requête d'invitation, le récepteur confirme son accord par l'envoi d'une réponse *200* OK, qui sera ensuite acquittée par le demandeur, comme pour

l'initiation d'une communication (voir figure II.13*)*. Dans ce contexte, cette requête ne fait pas sonner le poste de l'interlocuteur puisque la communication est déjà en cours.

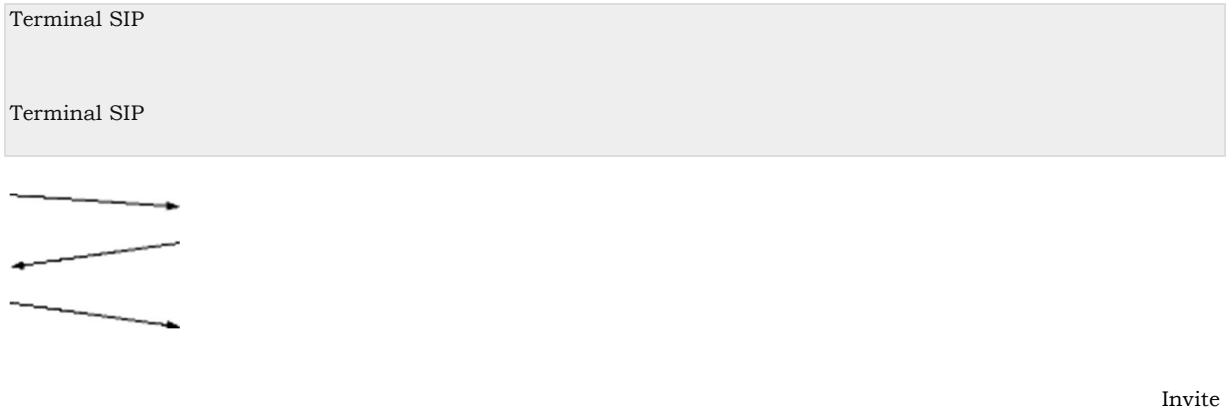



Figure II.13 : Requête RE-INVITE acceptée

Le demandeur qui en prend connaissance ne peut effectuer la modification désirée et doit soit se contenter des paramètres de la session actuelle, soit faire une nouvelle offre, en suggérant l'utilisation d'autres paramètres.

Dans le cas contraire, où le récepteur ne supporte pas ou ne souhaite pas accepter la modification de la session en cours, il reste libre de le faire, sans pour autant mettre fin à la communication, en envoyant un message de réponse *488 NOT ACCEPTABLE HERE,* comme l'illustre la figure II.14.

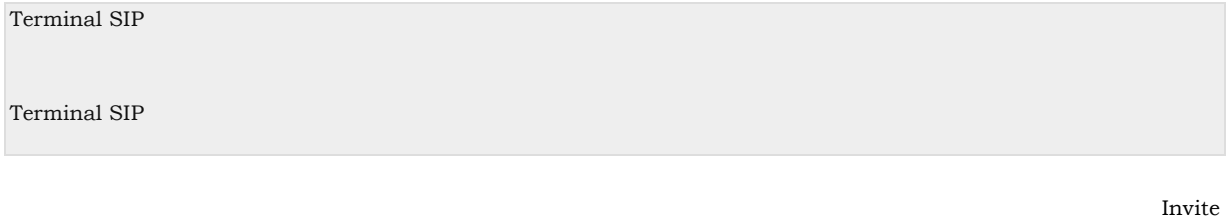



Figure II.14 : Requête de RE-INVITE refusée

## 6. Terminaison d'une communication SIP

La figure II.15 illustre la terminaison d'une session à l'initiative de n'importe quelle entité souhaitant mettre fin à l'appel.

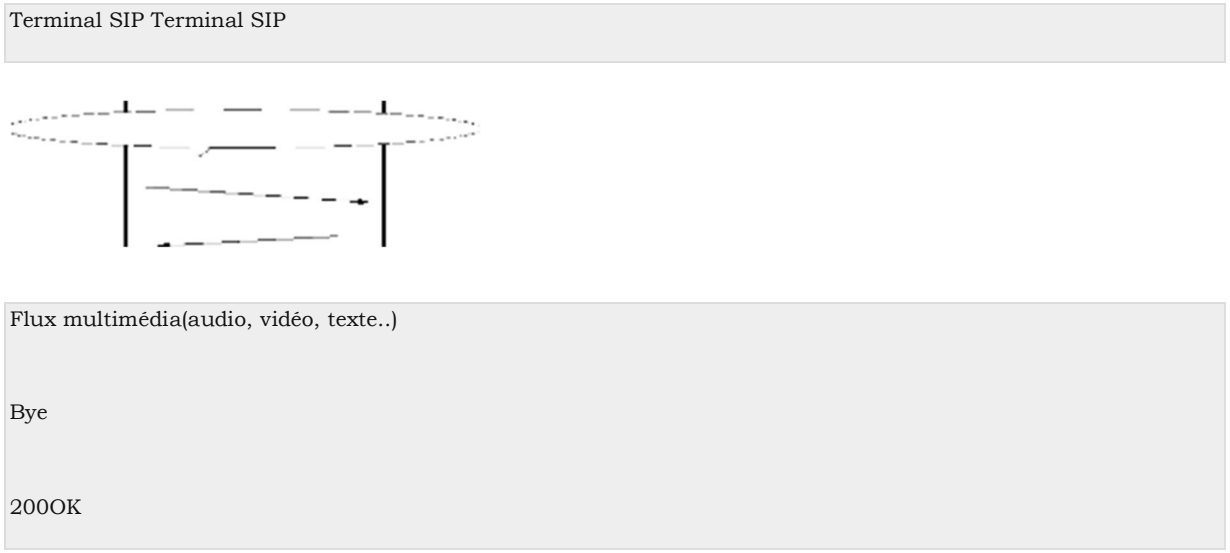



Figure II.15 : Terminaison d'une Communication

Cette opération ne comporte que les deux étapes très simples suivantes :

1. Un message (requête BYE) est envoyé pour indiquer au correspondant que la session va être clôturée ;

2. Le correspondant répond à cette requête en validant la prise en compte de cette demande par une réponse *200* OK. La communication entre les intervenants est alors rompue.

## II.5 AVANTAGES ET INCONVENIENTS DU PROTOCOLE SIP

### II.5.1 AVANTAGES

L'implémentation de la VoIP avec le protocole de signalisation SIP (Session Initiation Protocol) fournit un service efficace, rapide et simple d'utilisation. SIP est un protocole rapide et léger. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau.

Les utilisateurs s'adressent à ces serveurs Proxy pour s'enregistrer ou demander l'établissement de communications. Toute la puissance et la simplicité du système viennent de là. On peut s'enregistrer sur le Proxy de son choix indépendamment de sa situation géographique. L'utilisateur n'est plus "attaché" à son autocommutateur.

Une entreprise avec plusieurs centaines d'implantations physique différente n'a besoin que d'un serveur Proxy quelque part sur l'Internet pour établir "son" réseau de téléphonique "gratuit" sur l'Internet un peu à la manière de l'émail. Les dizaines de milliers d'autocommutateurs peuvent être remplacés par quelques serveurs proxy.

On imagine bien la révolution. Mais comme d'habitude rien n'empêchera de remplacer un autocommutateur par un serveur Proxy réduisant ainsi l'intérêt du système. SIP est un protocole indépendant de la couche transport. Il peut aussi bien s'utiliser avec TCP que le protocole UDP.

### II.5.2 INCONVENIENTS

L'une des conséquences de cette convergence est que le trafic de voix et ses systèmes associés sont devenus aussi vulnérables aux menaces de sécurité que n'importe quelle autre donnée véhiculée par le réseau.

En effet, SIP est un protocole d'échange de messages basé sur HTTP. C'est pourquoi, il est très vulnérable face à des attaques de types DoS (Dénis de Service), détournement d'appel, trafic de taxation, etc. De plus, le protocole de transport audio associé RTP (Real Time Protocol) est lui aussi très peu sécurisé face à l'écoute indiscrète ou des DoS.

Le SIP est une norme pour la communication multimédia, il devient de plus en plus utilisé pour la mise en place de la téléphonie sur IP, la compréhension de ce protocole aidera le professionnel à l'épreuve de la sécurité sur le réseau. Ce protocole est un concurrent direct à H.323.

## II.6 COMPARAISON ENTRE LE PROTOCOLE SIP ET H.323

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

Tous les deux utilisent le protocole RTP comme protocole de transfert des données multimédia.

Au départ, H323 fut conçu pour la téléphonie sur les réseaux sans QoS, mais on l'adopta pour qu'il prenne en considération l'évolution complexe de la téléphonie sur internet.

Pour donner une idée de la complexité du protocole H323 par rapport à SIP, H323 est défini en un peu plus de 700 pages et SIP quant à lui en moins de 200 pages. La complexité de H323 provient encore du fait de la nécessité de faire appel à plusieurs protocoles simultanément pour établir un service, par contre SIP n'a pas ce problème.

SIP ne requiert pas de comptabilité descendante, c'est un protocole horizontal qui est le contraire de H323 : Les nouvelles versions de H323 doivent tenir compte des anciennes versions pour continuer à fonctionner. Ceci entraîne pour H323 de traîner un peu plus de codes pour chaque version.

H323 ne reconnaît que les Codecs standardisés pour la transmission des données multimédias proprement dit alors que SIP, au contraire, peut très bien en reconnaître d'autres. Ainsi, on peut dire que SIP est plus évolutif que H323. Le tableau II.6 nous donne l'approche comparative du protocole SIP et du protocole H.323.

**Tableau II.6** : Tableau de comparaison entre le protocole SIP et H.323

| | **SIP** | **H.323** |
|---|---|---|
| Nombre d'échanges pour établir la connexion | 1,5 aller-retour | 6 à 7 allers retours |
| Maintenance du code Protocolaire | Simple par sa nature textuelle à l'exemple de http | Complexe et nécessitant un compilateur |
| Evolution du protocole | Protocole ouvert à de nouvelles fonctions | Ajout d'extensions propriétaires<br><br>sans concertation entre vendeurs |
| Fonction de conférence | Distribuée | Centralisée par l'unité MCU |
| Fonction de télé services | Oui, par défaut | H.323 v2 + H.450 |
| Détection d'un appel en Boucle | Oui | Inexistante sur la version 1, un appel routé sur l'appelant provoque une infinité de requêtes |
| Signalisation multicast | Oui, par défaut | Non |

En résumé, La simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, du protocole SIP sont autant d'arguments qui pourraient lui permettre de convaincre les investisseurs. De plus, ses avancées en matière de sécurisation des messages sont un atout important par rapport à ses concurrents.

## II. 6' LE PROTOCOLE IAX

Le protocole d'Echange Inter-Asterisk (Inter-Asterisk eXchange, IAX) version 2 (IAX2) propose une alternative aux protocoles de signalisation tels que SIP. IAX2 a été créé dans le cadre du projet de PBX Open source Asterisk. Contrairement à SIP qui utilise 2 paires de flux (l'une pour la signalisation, l'autre pour la voix), IAX utilise une seule paire de flux pour communiquer entre les extrémités de la ligne (téléphone ou central téléphonique). La signalisation comme les données (la conversation vocale) sont transmises sur le même canal, par opposition à SIP qui utilise un second canal (« out-of-band ») pour les flux de données (RTP) transportant la voix. De plus, IAX2 permet à plusieurs appels d'être rassemblés dans un seul ensemble de paquets IP, puisque qu'un seul paquet peut transporter des informations concernant plusieurs appels en cours.

Ce mécanisme se nomme « trunking ». Avec IAX2, le « trunking » permet des économies de bande passante. Le concept de « trunking » nous l'expliquons comme ceci : imaginez que vous ayez à envoyer cinq lettres à des destinataires vivant dans un autre pays. Vous pouvez utiliser une enveloppe par lettre, ou inclure les cinq lettres dans une seule enveloppe et inclure le nom du destinataire final en première ligne de chacune des lettres. Le « trunking » opère de façon similaire et permet d'envoyer plusieurs lettres (appels) dans une seule enveloppe (paquet IP). En résumé, IAX2 présente les caractéristiques suivantes :

Minimise la bande passante par appel

Réduit la consommation de bande passante pour un ensemble d'appels (par l'utilisation du « trunking »).

En bref, la simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, du protocole SIP sont autant d'arguments qui pourraient nous permettre d'opter pour son choix. De plus, ses avancées en matière de sécurité des messages sont un atout important par rapport à ses concurrents.

## II. 6'' PROTOCOLES SCCP

La différence fondamentale entre les produits CISCO et les autres produits en termes de VOIP se situe au niveau du protocole de signalisation car CISCO est propriétaire du protocole SCCP (Skinny Client Control Protocol) depuis 1998 lors du rachat de Selsius Corporation.

Le SCCP est un protocole le plus léger et plus souple qui permet aux clients Skinny de communiquer avec Call Manager. Il utilise le port TCP 2000 pour la signalisation et RTP over UDP pour le trafic temps-réel (flux audio) avec les autres clients Skinny.

SCCP a été prévu pour des périphériques hardware et autres systèmes embarqués possédant un CPU relativement important et des contraintes au niveau de la mémoire.

Le H.323 étant trop rigoureux pour certaines utilités de la téléphonie IP (comme le renvoi d'appel, le transfert d'appel, la mise en attente), Cisco a mis en place ce protocole beaucoup plus léger qu'est le SCCP (comme nous l'avons dit ci-haut, il utilise le port 2000). L'avantage de Skinny est qu'il utilise des messages prenant très peu de bande passante c'est pourquoi il est utilisé pour les communications entre les téléphones IP et le Call Manager ainsi que pour contrôler une conférence.

Le SCCP est un protocole propriétaire originellement développé par Selsius Corporation, et qui appartient aujourd'hui à Cisco Systems. Le protocole SCCP utilise TCP qui est un moyen de communication fiable alors que SIP n'impose pas de protocole de transport, cela pouvant être aussi bien de l'UDP ou du TCP en fonction de la taille du message. Par contre, le transport de la voix est réalisé en UDP afin de privilégier la rapidité de transmission. De plus, on ne se soucie pas de la perte de paquets.

## II. 7 PROTOCOLES DE TRANSPORT

Nous décrivons deux autres protocoles de transport utilisés pour la voix sur IP, à savoir : le RTP et le RTCP.

## II.7.1 LE PROTOCOLE RTP

### II.7.1.1 DESCRIPTION GENERALE DU PROTOCOLE RTP

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

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

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

### II.7.1.2 LES FONCTIONS DU PROTOCOLE RTP

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie.

Ceci, de façon à reformer les flux avec ses caractéristiques de départ. C'est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de

l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. C'est aussi un protocole adapté aux applications présentant des propriétés temps réel.

Il permet ainsi de :

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

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

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

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

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

### II.7.1.3 AVANTAGES ET INCONVENIENTS DU PROTOCOLE RTP

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

### II.7.2 LE PROTOCOLE RTCP

### II.7.2.1 DESCRIPTION GENERALE DU PROTOCOLE RTCP

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

Le protocole RTP utilise le protocole RTCP, Real-time Transport Control Protocol, qui transporte les informations supplémentaires pour la gestion de la session.

Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS.

Ces rapports comprennent le nombre de paquets perdus, le paramètre indiquant la variance d'une distribution (plus communément appelé la gigue :

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

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

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

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

- le contrôle de la session : en effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet

Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. La périodicité est calculée en fonction du nombre de participants de l'application. On peut dire que les paquets RTP ne transportent que les données des utilisateurs, tandis que les paquets RTCP ne transportent en temps réel, que les signaux de supervision.

On peut détailler les paquets de supervision en 5 types :

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

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

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

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

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

### II.7.2.2 POINTS FORTS ET LIMITES DU PROTOCOLE RTCP

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

## II.8 AVANTAGES ET INCONVENIENTS DE LA TELEPHONIE SUR IP

### II.8.1 AVANTAGES

#### II.8.1.1 REDUCTION DES COUTS

Il y a une convergence vers un réseau unique : des flux de voix, de vidéo, de textes et d'applicatifs transitent sur le même réseau. Par exemple les utilisateurs peuvent travailler sur des applications client-serveur, naviguer sur internet et téléphoner tout en même temps et ceci en utilisant le même réseau.

La téléphonie IP permet de relier et/ou de configuration des téléphones au analogiques au IPBX sans passer par un PABX traditionnel et ainsi conserver les anciens téléphones (analogiques) ou le câblage.

De plus, cette technologie permet à un utilisateur nomade d'utiliser les services téléphoniques partout où il se connecte, ainsi cela permet de réduire les éventuels coûts liés à une sédentarité (téléphonie mobile, carte téléphonique, téléphone d'hôtel...).

Les coûts de communication sont réduits grâce aux fournisseurs émergeants qui proposent, à prix réduit, les appels nationaux et internationaux, cela permet aussi de communiquer entre les filiales à moindre coût.

#### II.8.1.2 OPTIMIATION DES RESSOURCES

Il y a aussi une optimisation des ressources, car dans une communication traditionnelle, commutation de circuit (RTC), les ressources sont dédiées pour toute la durée de la conversation téléphonique. Ainsi, il y a deux canaux de communication téléphonique, un en émission et l'autre en réception (full-duplex) puisque deux personnes peuvent parler en même temps. Dans la pratique, il est rare que ce dernier cas se produise, car en réalité chaque personne se parle mutuellement, voire il y a présence de «

blancs » pendant les conversations. C'est pourquoi, la réservation de ressource effectuée dans un réseau RTC est nettement supérieure à celle d'un réseau IP.

### II.8.1.3 SIMPLIFICATION DE LA GESTION, D'ADMINISTRATION ET DE MIGRATION

Du fait d'une convergence vers un réseau unique, les procédures d'assistance, de configuration et d'intégration sont simplifiées (simplification de l'exploitation, unification des applications, etc....).

Les solutions de la téléphonie sur IP sont conçues pour dégager une stratégie de migration à faible risque à partir de l'infrastructure existante, car elles peuvent être installées en parallèle au réseau existant.

### II.8.1.4 AUGMENTATION DES SERVICES

Il y a une augmentation des services propres aux réseaux IP, comme notamment la détection de présence, c'est à dire savoir si l'utilisateur est en ligne ou non. Mais aussi les applications de l'entreprise peuvent intégrer les services téléphoniques, par exemple il y a une possibilité de téléphoner à un utilisateur en se servant des contacts du logiciel de messagerie.

## II.8.2 INCONVENIENTS

### II.8.2.1 PROBLEMES DE SECURITE

**Déni de service** : c'est l'une des attaques les plus répandues, le but étant de rendre le réseau téléphonique inopérant en surchargeant le PABX.

**Fraude téléphonique** : cela consiste par exemple à créer une cabine téléphonique sauvage, depuis laquelle on pourra passer des appels aux frais de l'entreprise.

**L'écoute** : permet d'écouter tout le trafic véhiculé, dans cette attaque le trafic n'est pas modifié.

**Accès au système d'information** : utiliser des failles d'un logiciel de communication (exemple Skype) pour accéder aux données de l'utilisateur.

**Vishing** : il s'agit de la contraction de VoIP et de phishing, c'est une attaque qui consiste à mettre en place un système de serveur composant de façon aléatoire des numéros. Lorsqu'une personne décroche, un serveur vocal par exemple se fait passer pour une banque des données et essaie de lui soutirer des informations.

### II.8.2.2 PROBLEME D'ENGORGEMENT DU RESEAU

Une dégradation d'une conversation téléphonique peut être due à une surcharge du réseau. La téléphonie nécessite peu de bande passante, mais requiert quand même un débit constant, ce besoin entre en contradiction avec la politique du protocole IP : "Best Effort".

## II.9 CONCLUSION

Dans ce chapitre, nous avons décrit la VoIP en tant que solution la plus rentable pour effectuer des communications téléphoniques en entreprise, mais aussi une bonne solution en matière d'intégration de services données et voix, fiable et à moindre coût.

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

Dans le chapitre qui suit, nous allons aborder les aspects liés aux vulnérabilités de cette nouvelle technologie de communication, ainsi que les mesures de sécurisation de services.

# III : VULNERABILITES DES RESEAUX VoIP ET MESURES DE SECURITE

## III.1 INTRODUCTION

L'opportunité de migrer de la téléphonie classique vers la téléphonie IP, a offert plusieurs avantages pour les entreprises, et les a permis de bénéficier de nouveaux services, tels que la vidéoconférence et la transmission des données. L'intégration de ces services dans une seule plateforme nécessite plus de sécurité.

Dans ce chapitre, nous allons décrire les attaques qui menacent la VoIP, et nous détaillerons quelques-unes. Nous finirons par une description des bonnes pratiques pour sécuriser les communications de type voix sur IP.

## III.2 APERCU SUR LES ATTAQUES DANS LES RESEAUX VoIP

Les attaques sur les réseaux VoIP peuvent être classées en deux types : les attaques internes et les attaques externes. Les attaques externes sont lancées par des personnes autres que celles qui participent aux appels, et ils se produisent généralement quand les paquets VoIP traversent un réseau peu fiable et/ou l'appel passe par un réseau tiers durant le transfert des paquets. Les attaques internes s'effectuent directement au réseau local dans lequel se trouve l'attaquant. Il existe deux principales classes des vulnérabilités sur un environnement VoIP. La première dépend des protocoles utilisés (SIP, H.323…) et la deuxième est liée aux systèmes sur lesquels les éléments VoIP sont implémentés. Chaque protocole ou service a ses propres attaques.

Dans le paragraphe qui suit, nous allons essayer de disséquer ces différentes attaques et certaines solutions disponibles.

### III.2.1 ATTAQUES SUR LES PROTOCOLES

Un appel téléphonique VoIP est constitué de deux parties : la signalisation, qui instaure l'appel, et les flux de media, qui transporte la voix.

La signalisation, en particulier SIP, transmet les entêtes et la charge utile (Payload) du paquet en texte clair, ce qui permet à un attaquant de lire et falsifier facilement les paquets. Elle est donc vulnérable aux attaques qui essaient de voler ou perturber le service téléphonique, et à l'écoute clandestine qui recherche des informations sur un compte utilisateur valide, pour passer des appels gratuits par exemple.

La signalisation utilise, en général, le port par défaut UDP/TCP 5060. Le firewall doit être capable d'inspecter les paquets de signalisation et d'ouvrir ce port afin de leurs autoriser l'accès au réseau. Un firewall qui n'est pas compatible aux protocoles de la VoIP doit être configuré manuellement pour laisser le port 5060 ouvert, créant un trou pour des attaques contre les éléments qui écoutent l'activité sur ce port.

Le protocole RTP utilisé pour le transport des flux multimédia, présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrement. Chaque entête d'un paquet RTP contient un numéro de séquence qui permet au destinataire de reconstituer les paquets de la voix dans l'ordre approprié. Cependant, un attaquant peut facilement injecter des paquets artificiels avec un numéro de séquence plus élevé. En conséquence, ces paquets seront diffusés à la place des vrais paquets.

Généralement, les flux multimédias contournent les serveurs proxy et circulent directement entre les points finaux. Les menaces habituelles conte le flux de la voix sont l'interruption de transport et l'écoute clandestine.

Les protocoles de la VoIP utilisent TCP et UDP comme moyen de transport et par conséquent sont aussi vulnérables à toutes les attaques contre ces protocoles, tel le détournement de session (TCP) (session Hijacking) et la mystification (UDP) (Spoofing), etc.

Les types d'attaques les plus fréquentes contre un système VoIP sont :

#### III.2.1.1 SNIFFING

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

Plusieurs outils requis pour le sniffing, y compris pour le protocole H.323 et des plugins SIP, sont disponibles en open source.

### III.2.1.2 SUIVI DES APPELS

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

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

### III.2.1.3 INJECTION DES PAQUETS RTP 13

Cette attaque se fait au niveau du réseau LAN/VPN. Elle cible le serveur register, et a pour but de perturber une communication en cours.

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

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

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

### III.2.1.4 LES SPAMS

Trois formes principales de Spams sont jusqu'à maintenant identifiés dans SIP :

**- Call Spam** : Ce type de spam est défini comme une masse de tentatives d'initiation de session (des requêtes INVITE) non sollicitées. Généralement, c'est un UAC (User Agent Client) qui lance, en parallèle, un grand nombre d'appels. Si l'appel est établi, l'application génère un ACK, rejoue une annonce préenregistrée, et ensuite termine l'appel.

**- IM** (Instant Message) **Spam** : Ce type de spam est semblable à celui de l'e-mail. Il est défini comme une masse de messages instantanés non sollicitées. Les IM spams sont pour la plupart envoyés sous forme de requête SIP. Ce pourraient être des requêtes INVITE avec un entête « Subject » très grand, ou des requêtes INVITE avec un corps en format texte ou HTML.

Bien-sûr, l'IM spam est beaucoup plus intrusif que le spam e-mail, car dans les systèmes actuels, les IMs apparaissent automatiquement sous forme de pop-up à l'utilisateur.

**- Présence Spam** : Ce type de spam est semblable à l'IM spam. Il est défini comme une masse de requêtes de présence (des requêtes SUBSCRIBE) non sollicitées. L'attaquant fait ceci dans le but d'appartenir à la " white list " d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier avec lui d'autres formes de communications. L'IM Spam est différent du Présence Spam du fait que ce dernier ne transmet pas réellement de contenus dans les messages.

### III.2.1.5 LE DENI DE SERVICE (DOS : Denial Of Service)

C'est d'une manière générale, l'attaque qui vise à rendre une application informatique ou un équipement informatique incapable de répondre aux requêtes de ses utilisateurs et donc le mettre hors d'usage.

Une machine serveur offrant des services à ses clients (par exemple un serveur web) doit traiter des requêtes provenant de plusieurs clients. Lorsque ces derniers ne peuvent en bénéficier, pour des raisons délibérément provoquées par un tiers, il y a déni de service. Dans une attaque de type DoS flood attack, les ressources d'un serveur ou d'un réseau sont épuisées par un flot de paquets. Un seul attaquant visant à envoyer un flot de paquets peut être identifié et isolé assez facilement. Cependant, l'approche de choix pour les attaquants a évolué vers un déni de service distribué (DDoS). Une attaque DDoS repose sur une distribution d'attaques DoS, simultanément menées par plusieurs systèmes contre un seul. Cela réduit le temps nécessaire à l'attaque et amplifie ses effets. Dans ce type d'attaque, les pirates se dissimulent parfois grâce à des machines-rebonds (ou machines zombies), utilisées à l'insu de leurs propriétaires. Un ensemble de machines-rebonds, est contrôlable par un pirate après infection de chacune d'elles par un programme de type porte dérobée (backdoor).

Une attaque de type DoS peut s'effectuer à plusieurs niveaux, soit : **A la couche réseau :**

- IP Flooding : Le but de l'IP Flooding est d'envoyer une multitude de paquets IP vers une même destination, de telle sorte que le traitement de ces paquets empêche une entité du réseau (un routeur ou la station destinatrice) de traiter les paquets IP légitimes. Si l'IP Flooding est combiné à l'IP Spoofing, il est impossible pour le destinataire de connaître l'adresse source exacte des paquets IP. De ce fait, à moins que le destinataire ne limite ses échanges avec certaines stations, il lui est impossible de contrer ce type d'attaques.

- Fragmentation des paquets IP : Par la fragmentation des paquets, il est possible de rendre hors service de nombreux systèmes d'exploitation et dispositif VoIP par le biais de la consommation des ressources. Il existe de

nombreuses variantes d'attaques par fragmentation, parmi les plus populaires, on a : tear drop, open tear, nestea, jolt, boink, et Ping of death.

**A la couche transport :**

- L'UDP Flooding Attacks : Le principe de cette attaque est qu'un attaquant envoie un grand nombre de requêtes UDP vers une machine. Le trafic UDP étant prioritaire sur le trafic TCP, ce type d'attaque peut vite troubler et saturer le trafic transitant sur le réseau et donc de perturber le plus la bande passante. Presque tous les dispositifs utilisant le protocole SIP fonctionnent au-dessus du protocole UDP, ce qui en fait d'elles des cibles. De nombreux dispositifs de VoIP et de systèmes d'exploitation peuvent être paralysés grâce à des paquets UDP Flooding visant l'écoute du port SIP (5060) ou d'autres ports.

- TCP SYN floods est une attaque visant le protocole TCP et plus exactement la phase d'établissement de connexion. Celle-ci se fait en trois sous étapes :

- Le client envoie un paquet SYN au serveur ;

- Le serveur répond avec un paquet SYN-ACK ; 1' Le client envoie un paquet ACK au serveur.

L'attaque consiste en l'envoie d'un grand nombre de paquets SYN. La victime va alors répondre par un message SYN-ACK d'acquittement. Pour terminer la connexion TCP, la victime ensuite va attendre pendant une période de temps la réponse par le biais d'un paquet ACK. C'est là le cœur de l'attaque parce que les ACK final ne sont jamais envoyés, et par la suite, la mémoire système se remplit rapidement et consomme toutes les ressources disponibles à ces demandes non valides. Le résultat final est que le serveur, le téléphone, ou le routeur ne sera pas en mesure de faire la distinction entre les faux SYN et les SYN légitimes d'une réelle connexion VoIP.

## A la couche applications :

SIP Flooding : Dans le cas de SIP, une attaque DoS peut être directement dirigée contre les utilisateurs finaux ou les dispositifs tels que les téléphones IP, les routeurs et les proxys SIP, ou contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques traditionnelles de DoS.

Les différentes formes d'attaque DoS sont :

## a) ATTAQUE PAR LA METHODE DU CANCEL

C'est un type de déni de service lancé contre l'utilisateur, l'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL. Cette requête produit une erreur sur le dispositif de l'appelé et annule l'appel. Ce type d'attaque est employé pour interrompre la communication. La figure III.1 représente une attaque DoS via une requête CANCEL.

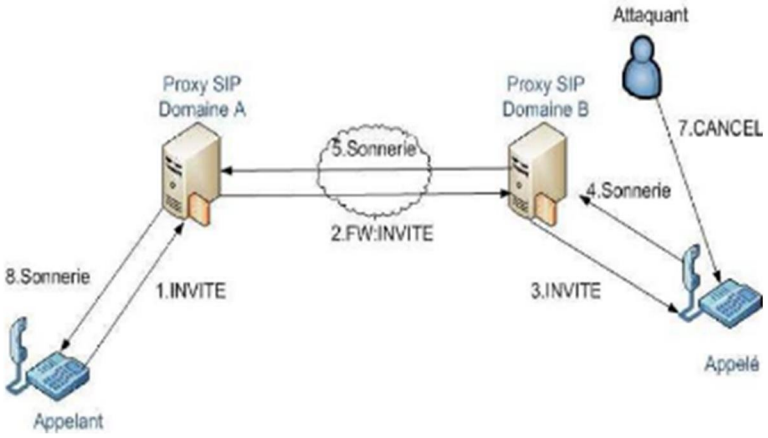



Figure III.1: Attaque DoS via une requête CANCEL

La figure suivante montre un scénario d'attaque DoS CANCEL, l'utilisateur toto initie l'appel, envoie une invitation (1) au proxy auquel il est rattaché. Le proxy du domaine A achemine la requête (2) au proxy qui est responsable de l'utilisateur titi. Ensuite c'est le proxy du domaine B qui prend le relais et achemine la requête INVITE (3) qui arrive enfin à destination. Le dispositif de titi, quand il reçoit l'invitation, sonne (4). Cette information est réacheminée

jusqu'au dispositif de toto. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que titi n'ait pu envoyer la réponse OK, qui accepte l'appel.

Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu.

### b) ATTAQUE PAR LA METHODE DU BYE

L'attaque par la méthode du BYE est dirigée contre les usagers. L'attaquant génère un BYE et interrompt une conversation. Pour réaliser cette attaque, le pirate écoute le trafic et prend les informations nécessaires (comme par exemple le Call-Id, le From ou encore le To) pour générer un BYE frauduleux correspondant à la session qui est injecté sur le réseau. Le BYE n'étant pas authentifié, celui qui reçoit l'information l'exécute. La figure III.2 représente une attaque DoS via une requête BYE.

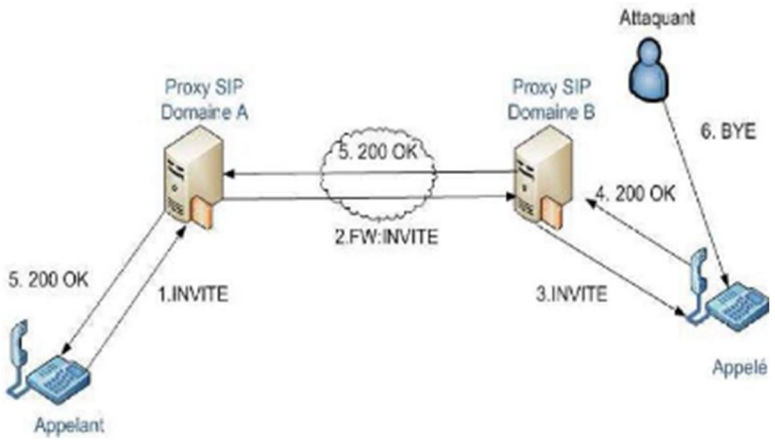



Figure III.2 : Attaque DoS via une requête BYE

### c) REGISTER

Le serveur d'enregistrement lui-même est une source potentielle de déni de service pour les utilisateurs. En effet, ce serveur peut accepter des enregistrements de tous les dispositifs. Un nouvel enregistrement avec une « * » dans l'entête remplacera tous les précédents enregistrements pour ce dispositif. Les attaquants, de cette façon, peuvent supprimer l'enregistrement de quelques-uns des utilisateurs, ou tous, dans un

domaine, empêchant ainsi ces utilisateurs d'être invités à de nouvelles sessions.

Notez que cette fonction de suppression d'enregistrement d'un dispositif, au profit d'un autre, est un comportement voulu en SIP afin de permettre le transfert d'appel. Le dispositif de l'utilisateur doit pouvoir devenir le dispositif principal quand il vient en ligne. C'est un mécanisme très pratique pour les utilisateurs mais également pour les pirates.

Figure III.3 : Mécanisme de l'attaque MIM

### III.2.1.6 DETOURNEMENT D'APPEL (CALL HIJACKING)

Le Call Hijacking consiste à détourner un appel. Plusieurs fournisseurs de service VoIP utilisent le web comme interface permettant à l'utilisateur d'accéder à son système téléphonique.

Un utilisateur authentifié peut changer les paramètres de ses transferts d'appel à travers cette interface web. C'est peut-être pratique, mais un utilisateur malveillant peut utiliser le même moyen pour mener une attaque.

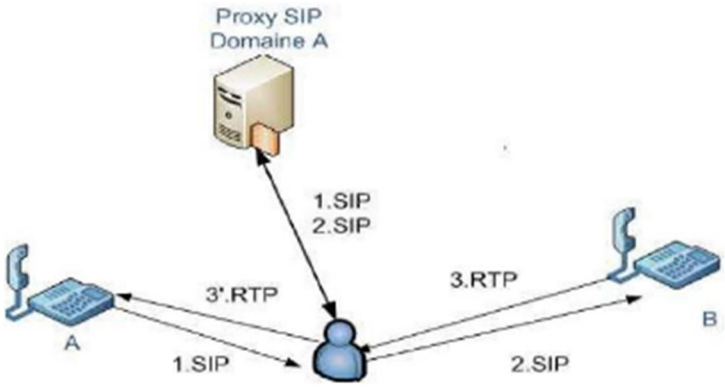
Exemple : quand un agent SIP envoie un message INVITE pour initier un appel, l'attaquant envoie un message de redirection 3xx indiquant que l'appelé s'est déplacé et par la même occasion, il donne sa propre adresse comme adresse de renvoi. A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit.

Un appel détourné en lui-même est un problème, mais c'est encore plus grave quand il est porteur d'informations sensibles et confidentielles.

### III.2.1.7 ATTAQUE PAR ECOUTE CLENDESTINE

Cette attaque consiste à écouter l'appel entre l'appelant et l'appelé, au moyen d'un empoisonnement ARP, dans le but de convaincre à la fois le serveur mandataire et les téléphones VoIP des deux utilisateurs, de communiquer

avec l'attaquant et non entre eux. La figure III.3 suivante illustre l'aspiration d'une transmission VoIP.




Tout d'abord, l'appel est paramétré. L'appelant A envoie la requête pour appeler B au serveur mandataire SIP. Ce message est intercepté puis transmis à la personne malveillante. Le serveur mandataire SIP tente désormais de joindre Bob pour lui indiquer que A souhaité l'appeler. Ce message est également intercepté puis transmis à la personne malveillante. Après une initialisation de l'appel réussie, l'appel actuel (qui a recours au protocole RTP) entre A et B commence. Cette communication RTP est également interceptée puis transmise par la personne malveillante. L'utilisation d'un outil comme Ethereal pour aspirer une communication, permet de recevoir également les données utiles RTP en continu.

### III.2.2 LES VULNERABILITES DE L'INFRASTRUCTURE (HARD ET SOFT)

Une infrastructure VoIP est composée de téléphones IP, Gateway, serveurs (proxy, register, etc.). Chaque élément, que ce soit un système embarqué ou un serveur standard tournant sur un système d'exploitation, est accessible via le réseau comme n'importe quel ordinateur.

Chacun comporte un processeur qui exécute des logiciels qui peuvent être attaqués ou employés en tant que points de lancement d'une attaque plus profonde.

#### III.2.2.1 INFRASTRUCTURE HARDWARE

## 1) LE TELEPHONE IP

Un pirate peut compromettre un dispositif de téléphonie sur IP, par exemple un téléphone IP, un Soft phone, ou d'autres programmes ou matériels client.

Généralement il obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif.

Compromettre un point final (téléphone IP) peut être fait à distance ou par un accès physique au dispositif.

Le pirate pourrait modifier les aspects opérationnels d'un tel dispositif :

V' La pile du système d'exploitation peut être changée pour masquer la présence de l'attaquant ;

V' Un Firmeware modifié de manière malveillante peut avoir été téléchargé et installé. Les modifications faites à la configuration des logiciels de téléphonie IP peuvent permettre :

- Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant ;

- Aux appels d'être surveillés ;

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

- De compromettre la disponibilité du point final.

Les softphones ne réagissent pas de la même façon aux attaques comparés à leur homologue téléphone IP. Ils sont plus susceptibles aux attaques dues au nombre de vecteur inclus dans le système, à savoir les vulnérabilités du système d'exploitation, les vulnérabilités de l'application, les vulnérabilités du service, des vers, des virus, etc... En plus, le softphone demeure sur le segment de données, il est ainsi sensible aux attaques lancées contre ce

segment et pas simplement contre l'hôte qui l'héberge. Les téléphones IP exécutent quant à eux leurs systèmes d'exploitation avec un nombre limité de services supportés, ils présentent donc moins de vulnérabilité.

### 2) LE SERVEUR VoIP

Un autre élément du réseau vulnérable est le serveur fournisseur du réseau de téléphonie sur IP, qui est peut-être la cible d'attaques pour mettre en péril tout le réseau.

Si un serveur de signalisation est compromis un attaquant peut contrôler totalement l'information de signalisation pour différents appels ce qui permettra à un attaquant de changer n'importe quel paramètre relatif à l'appel. Pour finir, il faut préciser qu'un serveur de téléphonie IP est installé sur un système d'exploitation, il peut donc être une cible pour les virus, les vers, ou n'importe quel code malveillant.

## III.2.2.2 INFRASTRUCTURE SOFTWARE

Une des principales vulnérabilités du système d'exploitation est le buffer overflow qui permet à un attaquant de prendre le contrôle partiel ou complet de la machine.

Elle n'est pas la seule vulnérabilité et elle varie selon le fabricant et la version de l'OS. Ces attaques visant l'OS, sont pour la plupart relative au manque de sécurité de la phase initiale de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit. Les dispositifs de la VoIP tels que les téléphonies IP, Call Managers, Gateway et les serveurs proxy,... héritent les mêmes vulnérabilités du système d'exploitation ou du firmware sur lequel ils tournent.

On déduira qu'une application de la VoIP est vulnérable dès que le système d'exploitation sur lequel elle tourne est compromis.

## III.3 MESURES DE SECURISATION

On a déjà vu que les vulnérabilités existent au niveau protocolaire, application et systèmes d'exploitation. Pour cela, on a découpé la sécurisation en trois niveaux : Sécurisation protocolaire, sécurisation de l'application et sécurisation du système de l'exploitation.

### III.3.1 SECURISATION AU NIVEAU DES PROTOCOLES

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

IPsec peut être utilisé pour réaliser deux objectifs : Garantir l'identité des deux points terminaux et protéger la voix une fois que les paquets quittent l'Intranet de l'entreprise. VoIPsec (VoIP utilisant IPsec) contribue à réduire les menaces, les sniffeurs de paquets, et de nombreux types de trafic « vocal analyze ». Combiné avec un pare-feu, IPsec fait que la VoIP soit plus sûr qu'une ligne téléphonique classique. Il est important de noter, toutefois, qu'IPsec n'est pas toujours un bon moyen pour certaines applications, et que certains protocoles doivent continuer à compter sur leurs propres dispositifs de sécurité. Dans la section qui suit, nous allons détaillés certaines bonnes pratiques de sécurité de VoIP au niveau des protocoles.

#### III.3.1.1 VoIP VPN

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

Vu que notre objectif est d'assurer la confidentialité et l'intégrité des clients, le mode choisi est donc le mode tunnel. Puisqu'il sécurise le paquet comme un tout (contrairement en mode transport qui ne sécurise que le payload IP).

Le mode tunnel se base sur l'encapsulation de tout le paquet IP et ajoute un nouvel entête pour l'acheminement de ce dernier. Ce mode est généralement utilisé pour les routeur-to-routeur. En plus du mode tunnel, on choisit le protocole ESP qui lui a son tour va assurer le cryptage des données et donc la confidentialité, contrairement au protocole AH qui lui ne permet que l'authentification des paquets et non le cryptage.

Dans ce cas, la solution qu'on propose est ESP mode tunnel qui sera appliqué uniquement sur les points de terminaison à la voix IP, c'est-à-dire le routeur. Ceci nous permettra donc de minimiser le nombre de machines qui seront impliquées dans le traitement engendré par la sécurité. De plus, le nombre des clés nécessaires sera réduit.

### III.3.1.2 SECURE RTP ou SRTP

SRTP est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPsec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il aussi est bâti sur le protocole temps réel RTP (Real Time Transport Protocol). Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP (Session Initiation Protocol), ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP (Real Time Streaming Protocol). Mais, surtout, il s'adjoint aux services du protocole de gestion de clé MIKEY (Multimédia Internet KEYing).

#### A. Services de sécurités offertes par SRTP

Les principaux services offerts par SRTP sont :

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

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

V' La protection contre le rejet des paquets. Chaque récepteur tient à jour la liste de tous les indices des paquets reçus et bien authentifiés.

## B. Principe de fonctionnement de SRTP

Avec une gestion de clé appropriée, SRTP est sécurisé pour les applications unicast et multicast de RTP. En théorie, SRTP est une extension du protocole RTP dans lequel a été rajoutée des options de sécurité. En effet, il a pour but d'offrir plusieurs implémentations de cryptographie tout en limitant l'overhead lié à l'utilisation de chiffrement. Il propose des algorithmes qui monopoliseront au minimum les ressources et l'utilisation de la mémoire.

Surtout, il permet de rendre RTP indépendant des autres couches en ce qui concerne l'application de mécanismes de sécurité.

Pour implémenter les différents services de sécurité précités, SRTP utilise les composants principaux suivants :

-**Une clé maîtresse** utilisée pour générer des clés de session ; Ces dernières seront utilisées pour chiffrer ou pour authentifier les paquets ;

-**Une fonction** utilisée pour calculer les clés de session à partir de la clé maîtresse ;

- **Des clés aléatoires** utilisées pour introduire une composante aléatoire afin de contrer les éventuels rejets ou effets de mémoire.

SRTP utilise deux types de clés : clef de session et clef maîtresse. Par « clef de session » nous entendons une clef utilisée directement dans les transformations cryptographiques ; et par « clef maîtresse », nous entendons une chaîne de bits aléatoires à partir desquelles les clefs de sessions sont dérivées par une voie sécurisée avec des mécanismes cryptographiques.

## C. Format du paquet SRTP

Un paquet SRTP est généré par transformation d'un paquet RTP grâce à des mécanismes de sécurité. Donc le protocole SRTP effectue une certaine mise en forme des paquets RTP avant qu'ils ne soient sur le réseau. La figure III.4 présente le format d'un paquet SRTP.

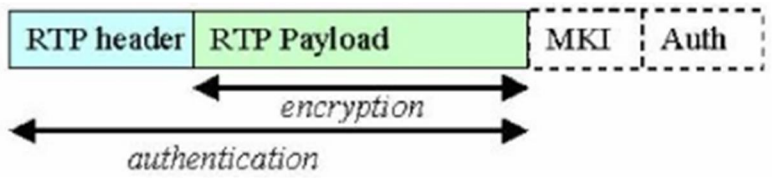



Figure III.4 : Format d'un paquet SRTP

On remarque que le paquet SRTP est réalisé en rajoutant deux champs au paquet RTP :

- SRTP MKI (SRTP Master Key Identifier) : sert à réidentifier une clef maîtresse particulière dans le contexte cryptographique. Le MKI peut être utilisé par le récepteur pour retrouver la clef primaire correcte quand le besoin d'un renouvellement de clefs survient ;

- Authentification tag : est un champ inséré lorsque le message a été authentifié. Il est recommandé d'en faire usage. Il fournit l'authentification des en-têtes et données RTP, et indirectement fournit une protection contre le rejet de paquets en authentifiant le numéro de séquence.

### III.3.1.3 LE PROTOCOLE TLS

C'est un protocole de sécurisation des échanges au niveau de la couche transport (TLS : Transport Layer Security). TLS, anciennement appelé Secure Sockets Layer (SSL), est un protocole de sécurisation des échanges sur Internet. C'est un protocole modulaire dont le but est de sécuriser les échanges Internet entre le client et le serveur indépendamment de tout type d'application. TLS agit comme une couche supplémentaire au-dessus de TCP.

Son utilisation est principalement associée à l'utilisation des certificats X.509 pour l'authentification des serveurs et le chiffrement des échanges (la signalisation).

### III.3.2 SECURISATION AU NIVEAU APPLICATION

Plusieurs méthodes peuvent être appliquées pour sécuriser l'application, ces méthodes varient selon le type d'application (serveur ou client). Pour sécuriser le serveur, il faut :

- L'utilisation d'une version stable, Il est bien connu que toute application non stable contient surement des erreurs et des vulnérabilités. Pour minimiser les risques, il est impératif d'utiliser une version stable ;
- Tester les mises à jour des softwares dans un laboratoire de test. Il est très important de tester toute mise à jour de l'application dans un laboratoire de test, avant de les appliquer sur le système en production ;
- Ne pas tester les correctifs sur le serveur lui-même ;
- Ne pas utiliser la configuration par défaut qui sert juste à établir des appels. Elle ne contient aucune protection contre les attaques ;
- Ne pas installer une application cliente dans le serveur.

Certains paramètres doivent être appliqués de manière sélective. Ces paramètres renforcent la sécurité de l'application, on peut les activer ou les interdire sur la configuration générale de l'application, comme on peut juste utiliser les paramètres nécessaires pour des clients bien déterminés et selon le besoin bien sûr. Ces paramètres protègent généralement contre le déni de service et ces différentes variantes. Il est conseiller d'utiliser les paramètres qui utilisent le hachage des mots de passe, cela assure la confidentialité de messages.

### III.3.3 SECURISATION DU SYSTEME D'EXPLOITATION

Il est très important de sécuriser le système sur lequel est implémenté le serveur de VoIP.

En effet, si le système est compromis, l'attaque peut se propager sur l'application serveur. Celle-ci risque d'affecter les fichiers de configuration contenant des informations sur les clients enregistrés.

Il y a plusieurs mesures de sécurités à prendre pour protéger le système d'exploitation :

- ✓ V' utiliser un système d'exploitation stable. Les nouvelles versions toujours contiennent des bugs et des failles qui doivent être corrigés et maîtrisés avant ;
- ✓ V' Mettre à jour le système d'exploitation en installant les correctifs de sécurité recommandé pour la sécurité ;
- ✓ V' Ne pas mettre des mots de passe simple et robuste. Ils sont fondamentaux contre les intrusions. Et ils ne doivent pas être des dates de naissances, des noms, ou des numéros de téléphones. Un mot de passe doit être assez long et former d'une combinaison de lettre, de chiffres et ponctuations ;
- ✓ V' Ne pas exécuter le serveur VoIP avec un utilisateur privilège. Si un utilisateur malveillant arrive à accéder au système via une exploitation de vulnérabilité sur le serveur VoIP, il héritera tous les privilèges de cet utilisateur ;
- ✓ V' Installer seulement les composants nécessaires : pour limiter les menaces sur le système d'exploitation. Il vaut mieux installer sur la machine le système d'exploitation et le serveur ;
- ✓ V' Supprimer tous programmes, logiciels ou des choses qui n'ont pas d'importance et qui peuvent être une cible d'attaque pour accéder au système ;
- ✓ V' Renforcer la sécurité du système d'exploitation en installant des patches qui permettent de renforcer la sécurité générale du noyau.

On peut aussi utiliser les pare feu ou/et les ACL pour limiter l'accès à des personnes bien déterminé et fermer les ports inutiles et ne laisser que les ports utilisés (5060, 5061, 4569...). Le pare feu (firewall) est un software ou hardware qui a pour fonction de sécuriser un réseau ou un ordinateur contre les intrusions venant d'autres machines. Le pare feu utilise le système de filtrage de paquet après analyse de l'entête des paquets IP qui s'échange entre les machines.

Le firewall peut être implémenté avec une ACL qui est une liste d'Access Control Entry (ACE) ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe. On aura besoin d'ACL pour donner des droits à des personnes bien déterminés selon leurs besoins et leurs autorités.

Pour un serveur VoIP, il est important d'implémenter les ACL pour sécuriser le serveur en limitant l'accès à des personnes indésirables. Par exemple, seuls les agents enregistrés peuvent envoyer des requêtes au serveur. Il existe trois catégories d'ACL :

La liste de contrôle d'accès peut être installée en réseau sur les pare feu ou les routeurs, mais aussi ils existent dans les systèmes d'exploitation.

# TROISIEME PARTIE

# MISE EN ŒUVRE

# DE LA

# SOLUTION

# TROISIEME PARTIE : Mise en œuvre de la solution

## Chapitre Cinquième : Choix des outils et des technologies d'implémentation

### Section 1 : Choix des équipements retenus et leurs caractéristiques

Cisco 2811 Integrated Services Router

Le routeur de services intégrés Cisco 2811 fait partie de la gamme de routeurs de services intégrés Cisco 2800 qui complète le portefeuille de routeurs de services intégrés.

Le routeur de services intégrés Cisco 2811 fournit le support suivant :

- Performances de vitesse par câble pour les services simultanés tels que la sécurité et la voix, et des services avancés à plusieurs taux WAN T1 / E1 / xDSL
- Amélioration de la protection des investissements grâce à des performances accrues et à la modularité
- Densité accrue grâce aux emplacements de carte d'interface WAN haute vitesse (quatre)
- Emplacement du module réseau amélioré

- Prise en charge de plus de 90 modules existants et nouveaux
- Prise en charge de la majorité des AIM, NM, WIC, VWIC et VIC existants
- Deux ports Fast Ethernet 10/100 Fast Ethernet
- Support de commutation de couche 2 en option avec Power over Ethernet (PoE) (en option)
- Sécurité
    - Cryptage à bord
    - Prise en charge de jusqu'à 1500 tunnels VPN avec le module AIM-EPII-PLUS
    - Support de défense antivirus grâce au contrôle d'admission réseau (NAC)
    - La prévention des intrusions ainsi que le support Cisco Firewall IOS et beaucoup d'autres fonctionnalités de sécurité essentielles
- Voix
    - Support d'appel vocal analogique et numérique
    - Support de messagerie vocale en option
    - Prise en charge facultative pour Cisco Call Manager Express (Cisco CME) pour le traitement local des appels en entreprise autonome pour jusqu'à 36 téléphones IP
    - Prise en charge facultative du support de téléphonie de site distant survivant pour le traitement d'appel local dans les succursales de petites entreprises pour un maximum de 36 téléphones IP

Commutateurs série Cisco Catalyst 2960

Permettra l'interconnexion des postes de communication sur chaque site

**L'IP phone** : C'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).

**Le soft phone** : C'est un logiciel qui assure toutes les fonction s téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC.

**Le serveur de communications** : il gère les autorisations d'appels entre les terminaux IP ou soft phones et les différentes signalisations du réseau. Il peut posséder des interfaces réseaux opérateurs (RTC-PSTN ou RNIS

## II- Architecture de mise en œuvre :

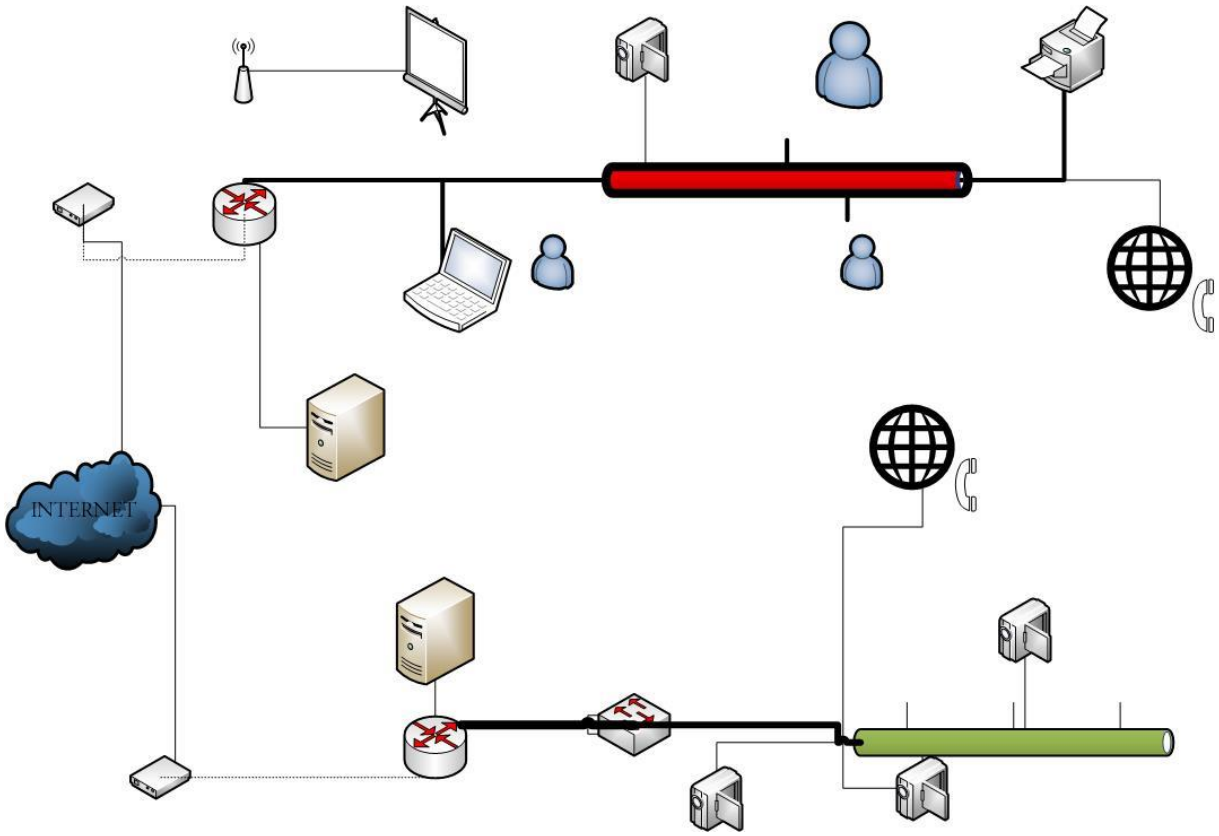



Figure 4.1 : Architecture de mise en œuvre

Ce schéma représente une architecture réseau multisite, représentant l'interconnexion entre deux sites de la gendarmerie.

A gauche nous avions le siège du Haut Commandement de la Gendarmerie Guinéenne et à droite nous avions la coordination des escadrons de la gendarmerie.

Les deux sites sont dotés de chacune d'un server de téléphonie et les deux sites sont liés.

# Chapitre Sixième : Implémentation de la Solution

## Section 1 : Maquette de test

Pour notre test sur Virtualbox, nous allons utiliser six machines virtuelles. Deux machines virtuelles, sous Debian 8 server une dans chaque site, pour l'installation et la configuration du server SIP Kamailio. Deux machines (Windows 7), pour installer le soft phone Jitsi, pour tester les fonctionnalités. L'autre machine (sous windows 7), nous l'utiliserons pour les tests de sécurité.

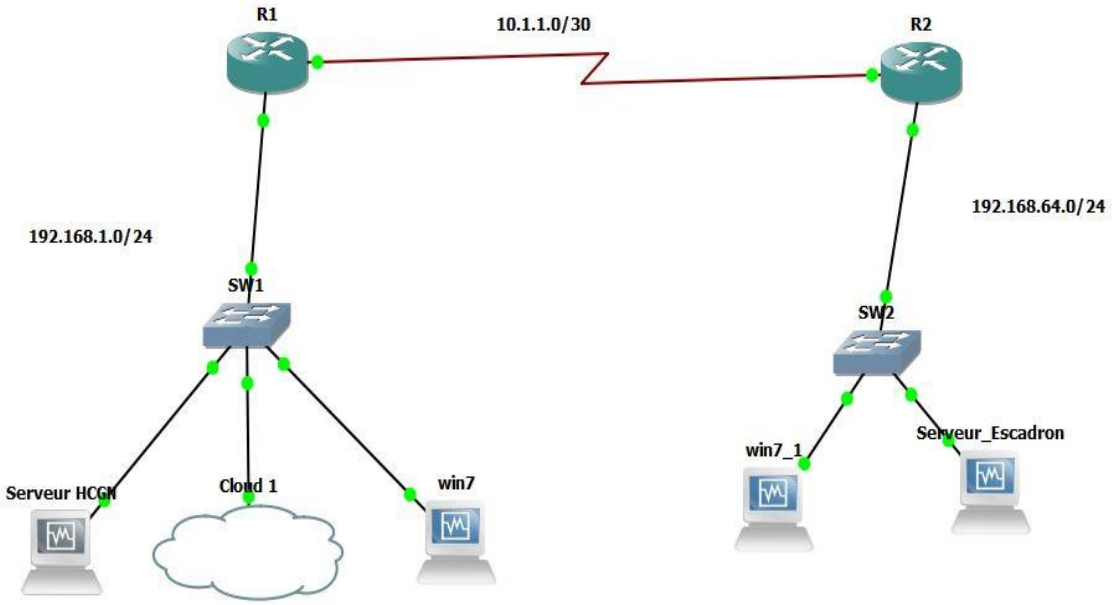



Figure 4.2 : Maquette de test

| Nom Machine | Adresse | Masque |
|---|---|---|
| Server HCGN | 192.168.1.20 | 255.255.255.0 |
| Cloud | DHCP CLIENT | |
| Win7 | 192.168.1.2 | 255.255.255.0 |
| Server Escadron | 192.168.64.30 | 255.255.255.0 |
| Win 7_1 | 192.168.64.2 | 255.255.255.0 |

### I. ESTIMATION FINANCIERE

| N : | Article | Quantité | Prix unitaire en FCFA HT-HD/DOLLARD | Montant en FCFA HTHD/DOLLARD |
|---|---|---|---|---|
| 1 | IPBX | 2 | 280 000 | 560 000 |
| 2 | ROUTEUR C2911 | 2 | 632 000 /1040 $ | 1 264 000 / 2080 |
| 3 | SOFT FONE | 10 | 58 000 / 100 $ | 580 000 /1000 $ |
| 4 | INTERNET | MOIS | 50 000 | 100 .000 |
| 5 | Main d'œuvre | 2 | 250 000 | 500 000 |
| | | TOTAL | | 3 004 000 /5180$ |

## Section 2 : Présentation de Kamailio

KAMAILIO est un serveur SIP Open Source lancé sous GPL crée en 2005 comme une division du projet SIP Express Router(SER) de FhG FOKUS Institute de Berlin(Allemagne). Ce projet visait à créer un environnement de développement ouvert pour créer un serveur SIP open source robuste et

évolutif. Son nom initial était OpenSER, mais en raison des allégations d'infraction de marque le nom est passé à Kamailio le 28 juillet 2008.

Il capable de gérer des milliers de configurations d'appel par seconde. C'est l'un des PBX les plus complets.

Il supporte des transactions asynchrone TCP, UDP et SCTP, l'encryptage des communications via TLS, la répartition de charge, un mécanisme natif Fail-over, l'authentification sur des backend Radius, MySQL, LDAP ou via transport XMLRCP

Il est utilisé aussi bien par des opérateurs télécoms comme plate-forme de service VoIP que pour les solutions classiques de téléphonie d'entreprise. C'est une alternative à Freeswitch et Asterisk les deux autres poids lourds du domaine.

## 1. Installation de Kamailio

Nous avions installé Kamailio sous une distribution linux notre choix a été porter sur Debian 8.

## 2. Prérequis

Apt-get upgrade (pour mettre à jour ces paquets.
Apt-get update (pour mettre notre cache à jour si ce n'est pas déjà fait).

Nous allons ajouter apt-key avec la commande :

**curl http://deb.kamailio.org/kamailiodebkey.gpg | apt-key add -**

On met à jour le dépôt source.list
Par défaut source.list ne contient pas URL de téléchargement de Kamailio

Nous utiliserons les commandes

**echo "deb http://deb.kamailio.org/kamailio jessie main" > /etc/apt/sources.list.d/kamailio.list**

**echo "deb-src http://deb.kamailio.org/kamailio jessie main" >> /etc/apt/sources.list.d/kamailio.list**

## 3. Installation

**apt-get update**

**apt-get -y install kamailio kamailio-extra-modules kamailio-ims-modules kamailio-mysql-modules kamailio-nth kamailio-presence-modules kamailio-tls-modules kamailio-websocket-modules kamailio-xml-modules kamailio-xmpp-modules**

## 4. Configuration

Après l'installation, nous allons éditer le fichier **/etc/default/kamailio.** Une fois dans ce fichier nous devons modifier les lignes suivantes :

| Numéro de la ligne à modifier | Instruction à modifier |
|---|---|
| N : 7 | **RUN_KAMAILIO=yes** |
| N : 10 | **USER=root** |
| N : 13 | **GROUP=root** |
| N : 21 | **CFGFILE=/etc/kamailio/kamailio.cfg** |
| N : 28 | **DUMP_CORE=yes** |

Après ces modifications, nous allons enregistrer le fichier le fichier puis redémarrer.

**Systemctl restart kamailio**

## 5. Installation de la base de la donnée MYSQL et création de la base de la donnée Kamailio

Pour installer la base de données MySql nous allons utiliser la commande

**Apt-get install mysql-server**

Nous allons éditer quelques lignes dans le fichier**/etc/kamailio/kamctl** pour connecter Kamailio avec mysql.

| Numéro de la ligne à modifier | Instruction à modifier |
|---|---|
| N :11 | **SIP_DOMAIN=sigma.sip** |
| N :21 | **DBENGINE=MYSQL** |
| N :24 | **DBHOST=localhost** |
| N :27 | **DBNAME=kamailio** |
| N :33 | **DBRWUSER="root"** |
| N :36 | **DBRWPW="pass"** |
| N :39 | **DBROUSER="root"** |
| N :42 | **DBROPW="pass"** |
| N :125 | **ALIASES_TYPE="DB"** |
| N :129 | **CTLENGINE="FIFO"** |
| N :142 | **VERBOSE=1** |
| N :149 | **PID_FILE=/var/run/kamailio/kamailio.pid** |

Nous allons procéder à la création de base de données Kamailio

**kamdbctl create**

Nous allons créer deux utilisateurs l'un se trouvant au siège de Haut commandement de la gendarmerie et l'autre se trouvant à la coordination des escadrons.

Pour créer un utilisateur nous allons taper la commande ci-dessous :

**kamctl add aicha pass**

**kamctl add kaba pass**

Deux utilisateurs (aicha et Kaba) les deux ayant comme mot de passe (pass).

Pour lister les comptes nous allons taper la commande :

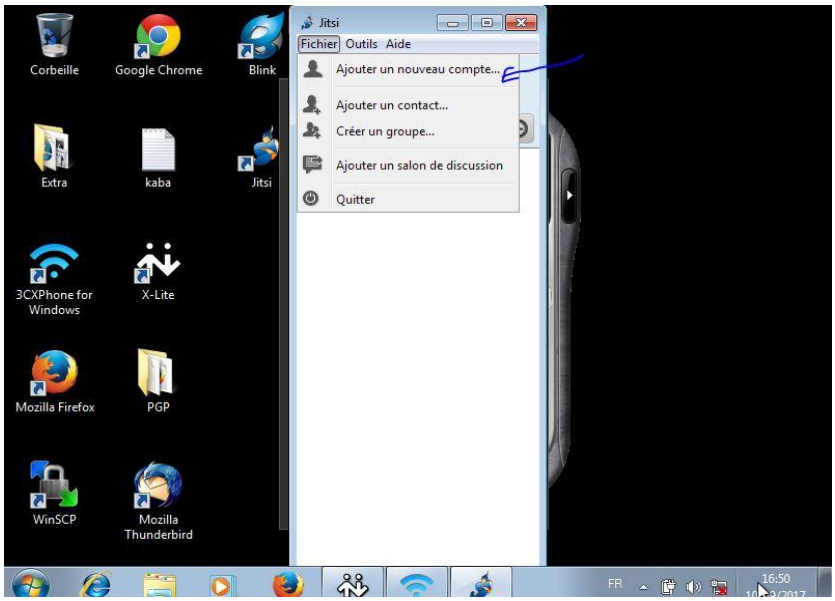
**kamctl db show subscriber**

# 6. Configuration des Softphones

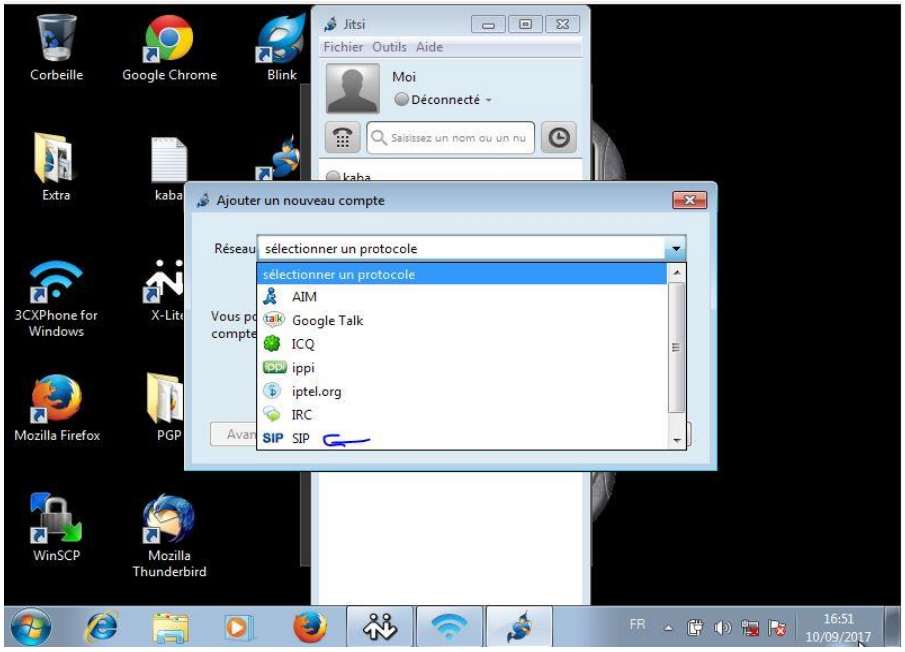
## 6.1 Softphones Jitsi

L'installation est simple et se fait comme tout logiciel.

Apres l'installation nous démarrerons le logiciel pour créer des comptes utilisateurs




Nous allons choisir le protocole qui sera utilisé pour la communication entre les utilisateurs.




Création des comptes utilisateurs

Utilisateur : Aicha

Protocole : SIP

Adresse ip du serveur : 192.168.1.20

Mot de passe : pass


## 6.2 Softphone Linphone

Linephone est un Sophone disponible sur Apple store et Google play

Pour configurer un utilisateur on fait comme suit :


Création des comptes utilisateurs

Utilisateur : Aicha

Protocole : SIP

Adresse ip du serveur : 192.168.1.20

Mot de passe : pass

## 7. Qualité de service sur la VoiP

La Qualité de Service (ou QoS pour Quality of Service), est un concept de gestion des différents types de flux sur un réseau, pour garantir de

bonnes performances des applications. La Qualité de Service va offrir des débits et des temps de réponse différenciés par type d'applications.

Typiquement, dans le cadre d'une mutualisation des applications Télécom (Voix) et Données (Data), la Voix sera rendue prioritaire car elle ne supporte aucun temps de latence. La Qualité de Service est ainsi garante de bonnes performances pour la mise en place d'une solution de Téléphonie sur IP.

Dans notre cas nous allons écrire un script Bash qui permettra d'assurer la qualité de service de notre VoiP.

## 7.1 Implémentation de la QOS.

La base de la commande tc est la Queuing Discipline (qdisc) qui représente la politique de « scheduling » (ordonnacement) appliquée à une queue. La politique qdisc par défaut sous Linux est FIFO.

Pour mettre en place notre QoS, nous allons utiliser HTB (Hierarchical Token Bucket) qui est en fait un Token Bucket Filter (on attend d'avoir un jeton disponible pour transmettre) amélioré grâce à la mise en place de filtres permettant une meilleure granularité/complexité.

Nous allons donc créer plusieurs classes :

- ✓ Une classe, d'identifiant 10, avec la plus haute priorité pour le streaming avec un débit (rate) garanti de 8 Mbit.
- ✓ Une classe, d'identifiant 20, pour tous les autres types de flux.

On marque ces paquets grâce à la commande iptables en précisant que seules les machines du réseau local sont concernées par ce filtre.

Ensuite en jouant sur les ports sources ou les ports de destination on marque les paquets.

Enfin, grâce à la commande tc filter on peut relier l'arbre de contrôle de trafic et le marquage des paquets : ce sont les règles de filtrage.

## SERVEUR DU HCGN

```
#!/bin/bash
#####installation nettoyage #######

#Adresse du reseau local  (254 machines )
LAN=192.168.1.0/24
# Reset root
iptables -t mangle -F

#### CREATION DISCIPLINE ####
#CREATION DISCIPLINE POLITIQUE HTB, tout trafic qui n'est pas VOIP ira dans la calsse par defaut

tc qdisc add dev eth1 root handle 1 : htb default 40

#Classe file VOIP

tc class add dev eth1 parent 1:0 classid 1:10 htb rate 8mbit prio 1

# classe file par defaut pour le reste

tc class add dev eth1 parent 1:0 classid 1:40 htb rate 100mbit prio 4

##MARQUAGE DES PAQUETS####

# Marquage des apquets sortant dont le port source est 5060 (VOIP) ####
iptables -t mangle -A  OUTPUT -o eth1 -p udp -d $LAN --dport 5060 -j MARK --set-mark 1

#######FILTRAGE DES PAQUETS #########

# on relie le controle de trafic  avec le marquage de paquets

tc filter add dev eth1 parent 1:0 protocol ip prio 1 handle 1 fw flowid 1:10
```

## SERVEUR ESCADRON

```
#!/bin/bash
#####installation nettoyage #######

#Adresse du reseau local  (254 machines )
LAN=192.168.64.0/24
# Reset root
iptables -t mangle -F

#### CREATION DISCIPLINE ####
#CREATION DISCIPLINE POLITIQUE HTB, tout trafic qui n'est pas VOIP ira dans la calsse par defaut

tc qdisc add dev eth1 root handle 1 : htb default 40

#Classe file VOIP

tc class add dev eth1 parent 1:0 classid 1:10 htb rate 8mbit prio 1

# classe file par defaut pour le reste

tc class add dev eth1 parent 1:0 classid 1:40 htb rate 100mbit prio 4

##MARQUAGE DES PAQUETS####

# Marquage des apquets sortant dont le port source est 5060 (VOIP) ####
iptables -t mangle -A  OUTPUT -o eth1 -p udp -d $LAN --dport 5060 -j MARK --set-mark 1

#######FILTRAGE DES PAQUETS #########

# on relie le controle de trafic  avec le marquage de paquets

tc filter add dev eth1 parent 1:0 protocol ip prio 1 handle 1 fw flowid 1:10
```

## 8. SECURITE DE LA VOIP

Alors que les attaques sur les systèmes de VoIP sont en constantes augmentation, les vulnérabilités observées augmentent elles aussi de manière exponentielle.

Nous pouvons citer entre autres les attaques protocolaires (usurpation d'identité, détournement de compte SIP, replay, déni de service et les attaques applicatives.

Dans notre cas nous allons utiliser deux types de sécurités :

- La Sécurité dans le LAN (entre les utilisateurs d'un même site)
- La Sécurité WAN (entre les deux sites)

### 8.1 SECURITE LAN

*Transport Layer Security* (TLS), et son prédécesseur *Secure Sockets Layer* (SSL), sont des protocoles de sécurisation des

échanges sur Internet. Le protocole SSL a été développé à l'origine par Netscape. L'IETF en a poursuivi le développement en le rebaptisant *Transport Layer Security* (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.
TLS (ou SSL) fonctionne suivant un mode client-serveur. Il permet de satisfaire aux objectifs de sécurité suivants :

- ✓ L'authentification du serveur ;
- ✓ La confidentialité des données échangées (ou session chiffrée) ;
- ✓ L'intégrité des données échangées.

L'implémentation du protocole TLS se fait comme suit :

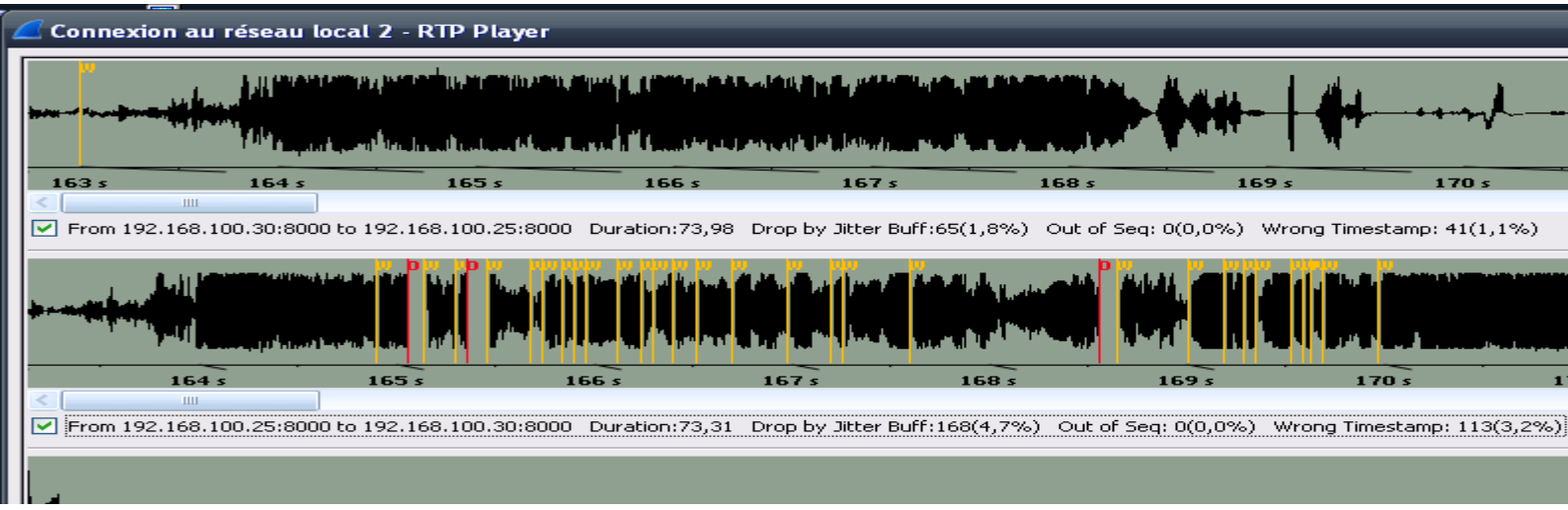
On édite le fichier **/etc/kamailio/kamailio.cfg**

| Numéro de la ligne | Instruction à ajouter |
|---|---|
| N : 1 | #!define WITH_TLS |

Puis on redémarre le serveur Kamailio

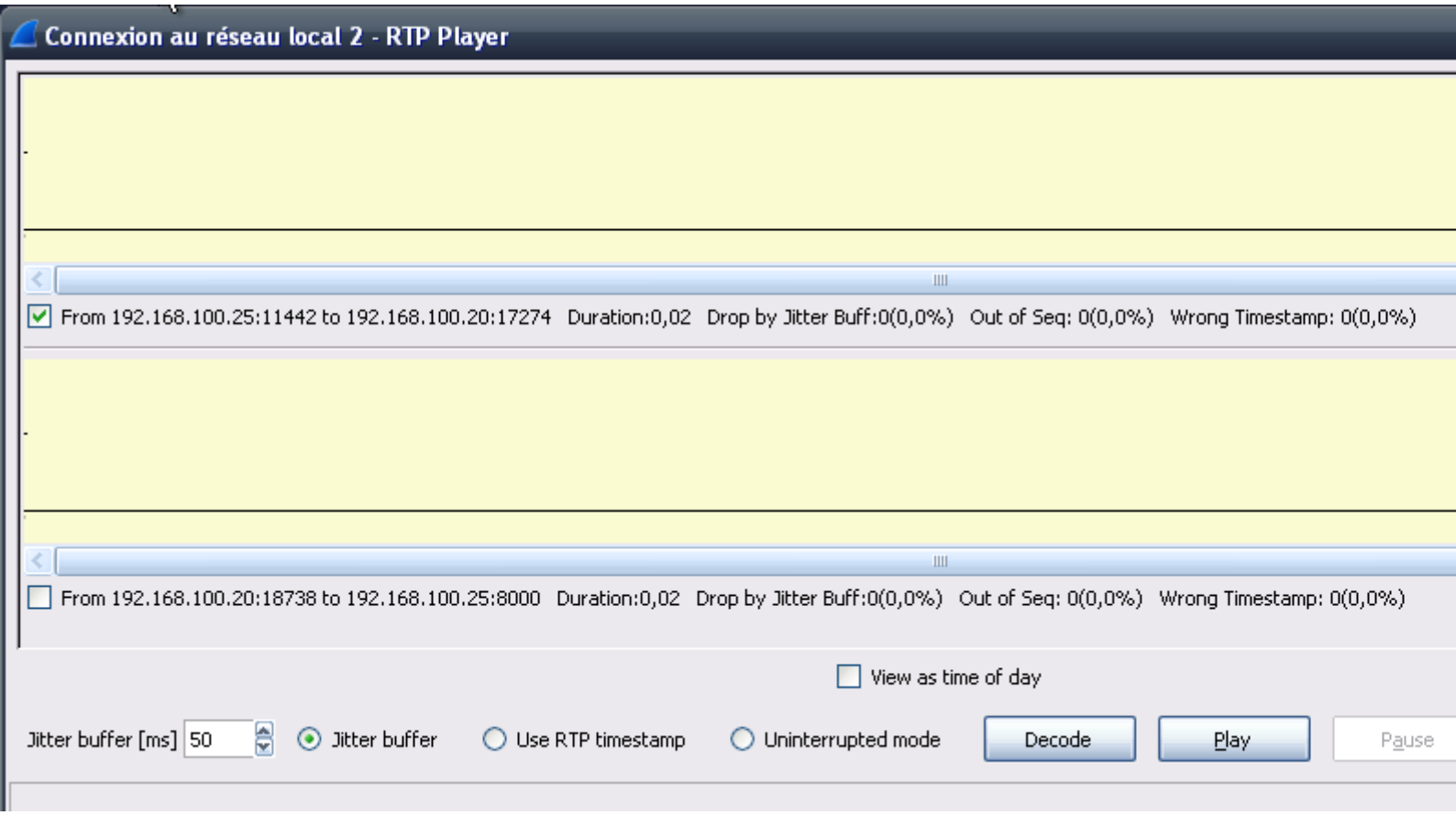
## AVANT LA SECURITE

Avant la sécurité nous pouvons intercepter , écouter et enregistrer les conversations avec l'outil wireshark



APRES LA SECURITE

Nous allons constater que nous ne voyons plus les appels .




## 8.2 SECURITE WAN

Nous allons implémenter une solution VPN SITE-TO-SITE IPSEC.

ROUTER DU HCGN (Haut commandement de la Gendarmerie Nationale) :

NB : Avant la mise en place de la sécurité nous devons nous assurer que la connectivité est normale ce qui implique que le routage marche normalement.

Nous devons taper les commandes suivantes :

Configurons la liste de contrôle d'accès 110 afin d'identifier le trafic issu du LAN sur **HCGN** vers le LAN sur **ESCADRON** comme étant le trafic intéressant. Ce trafic intéressant déclenchera le réseau privé virtuel IPsec à implémenter, pour autant qu'il y ait du trafic entre les LAN de **HCGN** et d'ESCADRON. Tout autre trafic provenant des LAN ne sera pas chiffré. En raison de l'instruction deny any implicite, il n'est pas nécessaire d'ajouter l'instruction à la liste.

```
CGN(config)#access-list 110 pe
CGN(config)#$ 110 permit ip 192.168.1.0 0.0.0.255 192.168.64.0 0.0.0.255
CGN(config)#
```

Configurons les propriétés **10** de la stratégie de chiffrement ISAKMP sur **HCGN** avec la clé de chiffrement partagée **cisco**. Référez-vous au tableau ISAKMP de phase 1 pour connaître les paramètres spécifiques à configurer. Les valeurs par défaut ne doivent pas être configurées et par conséquent seules les méthodes de chiffrement, d'échange de clés et DH doivent être configurées.

```
HCGN(config)#crypto isakmp policy 10
HCGN(config-isakmp)#encryption aes
HCGN(config-isakmp)#authentication pre-share
HCGN(config-isakmp)#group 2
HCGN(config-isakmp)#exit
```

L'adresse 10.1.1.2 represente l'adresse Ip du port serial du routeur **ESCADRON**

```
Router(config)#crypto isakmp key cisco address 10.1.1.2
```

Créons le transform-set **VPN-SET** de manière à utiliser **esp-3des** et **esp-sha-hmac**. Créons ensuite la carte de chiffrement **VPN-MAP** qui lie ensemble tous les paramètres. Utilisons le numéro d'ordre **10** et identifions-le comme étant une carte **ipsec-isakmp**.

```
outer(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
outer(cfg-crypto-trans)#exit
```

```
outer(config-crypto-map)#set peer 10.1.1.2
```

```
-crypto-map)#set transform-set VPN-SET
-crypto-map)#match address 110
-crypto-map)#exit
```

Enfin, lions la carte de chiffrement **VPN-MAP** à l'interface Serial 1/1 de sortie

```
HCGN(config)#int s1/1
HCGN(config-if)#crypto map VPN-MAP
HCGN(config-if)#
*Oct  5 13:24:00.899: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

ROUTER ESCADRON :

NB : Les instructions sont les mêmes à part ACL et l'adresse qui change.

```
ESCADRON(config)#$ 110 permit ip 192.168.64.0 0.0.0.255 192.168.1.0 0.0.0.255
ESCADRON(config)#
```

```
ESCADRON(config)#crypto isakmp policy 10
ESCADRON(config-isakmp)#encryption aes
ESCADRON(config-isakmp)#authentication pre-share
ESCADRON(config-isakmp)#group 2
ESCADRON(config-isakmp)#exit
```

```
outer(config)#crypto isakmp key cisco address 10.1.1.1
```

```
ESCADRON(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
ESCADRON(cfg-crypto-trans)#exit
ESCADRON(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
ESCADRON(config-crypto-map)#description VPN connection to HCGN
```

```
Router(config-crypto-map)#set peer 10.1.1.1
```

```
-crypto-map)#set transform-set VPN-SET
-crypto-map)#match address 110
-crypto-map)#exit
```

Après les pings, nous allons tester si la connexion fonctionne.

Nous constatons qu'il y a 8 paquets encapsulés et désencapsulés

Router HCGN

```
Router#sh crypto ipsec sa

interface: Serial1/1
    Crypto map tag: VPN-MAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.64.0/255.255.255.0/0/0)
   current_peer 10.1.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/1
     current outbound spi: 0x9D7CA08B(2642190475)

     inbound esp sas:
      spi: 0x5130384A(1362114634)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4522939/3362)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
```

Router Escadron

```
Router#sh  cry
Router#sh  crypto ip
Router#sh  crypto ipsec sa
Router#sh  crypto ipsec sa

interface: Serial1/2
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.64.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 85, #pkts encrypt: 85, #pkts digest: 85
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/2
     current outbound spi: 0x5130384A(1362114634)

     inbound esp sas:
      spi: 0x9D7CA08B(2642190475)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4537886/3300)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x5130384A(1362114634)
```

## Conclusion :

En somme, la téléphonie sur IP est une technologie révolutionnaire qui défie les règles édictées par la téléphonie RTC. Elle est plus souple, conviviale, ne nécessite pas un investissement lourd, coûte moins chère, propose de nouveaux services et beaucoup d'autres avantages, si bien que toute entreprise qui se veut compétitive et moderne aujourd'hui, jette son dévolu sur la téléphonie sur IP pour gérer ses communications tant internes qu'externes. Elle vise principalement à améliorer le cadre de travail des employés de l'entreprise en libérant l'utilisateur du lieu 'implantation du poste téléphonique.

Actuellement, il est évident que la téléphonie sur IP va continuer à se développer dans les prochaines années. Le marché de la téléphonie sur IP bien que jeune encore se développe à une vitesse fulgurante. C'est la raison pour laquelle plusieurs entreprises dans leurs stratégies de développement investissent maintenant dans la téléphonie sur IP. Cela leur permettra à coup sûr de jouer un rôle majeur. La téléphonie sur IP ouvre aujourd'hui la voie de la convergence voix/données/image et celle de l'explosion de nouveaux services tels que les centres d'appels actifs ou réactifs. Elle paraît comme une bonne solution en matière d'intégration, de fiabilité, d'évolutivité et de coût. Elle fait partie intégrante de l'Intranet de l'entreprise et permet des communications à moindre coût.

On peut ainsi vraisemblablement penser que le protocole IP deviendra un jour un standard unique permettant l'interopérabilité des réseaux mondialisés. C'est pourquoi l'intégration de la voix sur IP n'est qu'une étape vers l'**EoIP** : Everything over IP.

# BIBLIOGRAPHIE


- Téléphonie sur IP (TOIP) vers la convergence des réseaux dédiés (voix/video/données)
- Claude Servin, Réseaux & Télécoms, 1ere édition, Dunod, Paris, 2003
- Jean-François Susbielle, Internet multimédia et temps réel, paris 2000
- Laurent OUAKIL, GUY PUJOLLE, Téléphonie sur IP, Eyrolles, Paris, 2008
- Guy PUJOLLE, Les Réseaux, Eyrolles, Paris, 2003.
- Peter Thermos and Ari Takanen, Securing VoIP networks threats, vulnerabilities, and counter measures, (Addison-Wesley (c) 2007)
- David Endler et Mark Collier, Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions, (McGraw-Hill/Osborne (c) 2007)


## WEBOGRAPHIE


Page visitées entre Mars et Octobre 2017

http://www.asipto.com/pub/kamailio-devel-guide/ Consulté le 9 Juillet à 03 h 30

https://sonnguyen.ws/tag/kamailio/ Consulté le 10 Juillet à 10 h

https://medium.com/southbridge-io/kamailio-sip-proxy-installation-and-minimal-configuration-example-c96b5729853a Consulté le 27 Aout à 15 h

https://sonnguyen.ws/install-kamailio-debianubuntu/ Consulté le 15 Mai à 21 h

# Table des matières

Mots clés

ToIP ï SIP ï H323 ï MGCP ï VoIP ï téléphonie ï IP ï IPBX ï PABX ï Réseau ï Communications ï RTP ï SRTP ï RTC ï paquet ï Codec ï Protocole ï Configuration ï Sécurisation ï KAMAILIO ï Fonctionnalités ï Solution ï Outil ï Installation ï Soft phone ï Chiffrement-HCGN

KEYWORDS

ToIP ï SIP ï H323 ï MGCP ï VoIP ï téléphonie ï IP ï IPBX ï PABX ï Réseau ï Communications ï RTP ï SRTP ï RTC ï paquet ï Codec ï Protocole ï Configuration ï Sécurisation ï KAMAILIO ï Fonctionnalités ï Solution ï Outil ï Installation ï Soft phone ï Chiffrement-HCGN

## Résumé

Ce document est destiné à toute personne ayant des connaissances en réseaux, télécoms et sécurité informatique et désirant s'améliorer dans ces domaines en général et dans la téléphonie sur IP en particulier. Il nous a permis de revenir sur les notions de base des réseaux, des télécoms et de la sécurité informatique. Ensuite nous avons étudié, en détail, la VOIP et passer en revue notre solution. Enfin nous avons installé, configuré et sécurisé notre solution VOIP open source, kamailio.

## ABSTRACT

This document is intended for anyone with knowledge of networks, telecommunications and computer security and who wish to improve in these areas in general and in IP telephony in particular. It allowed us to go back to the basics of networks, telecoms and computer security. Then we studied VOIP in detail and reviewed our solution. Finally, we have installed, configured and secured our open source VOIP solution, kamailio.