

République Algérienne Démocratique et Populaire

Université SAAD DAHLAB Blida

Faculté des Sciences
Département Informatique

Mémoire de Fin d'études

Pour L'obtention du diplôme de Master (2) En Informatique

Option : Sécurité des systèmes information (SSI)

Intitulé :

**Etude et Déploiement d'une Solution VoIP Sécurisée Dans
L'infrastructure Réseau Air Algérie Catering**

Promoteur : BENBLIDIA Nadja

Encadreur : KELKOULI Farida

President : DOUCIA YASSINE

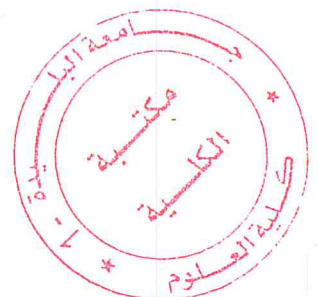
Présenté Par :

Mr. MEZAOUROU BILLEL

Mr. REZIG MOHAMED RAFIK

Organisme d'accueil : Air Algérie Catering

Année universitaire : 2017-2018



Remerciements

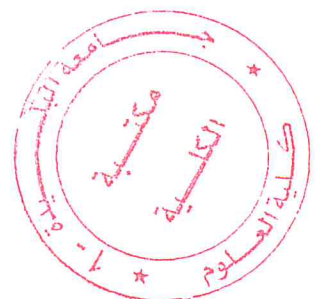
Nous remercions, d'abord ALLAH, tout puissant, de nous avoir donné le courage et la patience pour bien mener ce travail durant cette année.

Nous tenons exprimer notre profonde gratitude à et notre reconnaissance à Mme **Kelkouli Farida** qui a accepté de nous encadrer, ainsi que notre promotrice Mme **Benblidia Nadjia**, pour leurs encouragements, leur accompagnement et suivi durant toute la période de préparation de ce mémoire ainsi que leurs précieux conseils. Sans leur appui, il aurait été impossible, pour nous, de mener à bien ce travail.

Un Grand merci à nos familles surtout nos parents pour nous avoir soutenue tout le long de cette année d'étude, pour avoir été présent et réconfortant.

Mes sincères remerciements s'adressent également aux de jury d'avoir accepté d'évaluer ce travail.

Enfin, nous exprimons notre profonde gratitude à Mr Jeremy Cioara, Mr Keith Barker et Mr Kevin Wallace pour leur soutien et leur aide, de près ou de loin, pour réaliser ce projet.



RESUME

La téléphonie sur IP est devenue un nouveau paradigme pour établir et transmettre les communications téléphoniques directement sur les réseaux IP de manière flexible et à faible coût. Toutefois, les services VoIP sont confrontés à plusieurs problèmes de sécurité qui sont soit hérités de la couche IP soit spécifiques au service lui-même. Une grande variété de mécanismes de protection sont disponibles pour y faire face. Cependant, ces services nécessitent des performances et une disponibilité du réseau élevées, et les mécanismes de protection peuvent nuire à ces performances.

L'objectif principal du stage étant la mise en place d'une infrastructure VoIP en prenant en considération la sécurité des systèmes Voix sur IP.

- La réalisation d'une étude détaillée sur la VoIP.
- La réalisation d'une étude sur la sécurité dans le monde de la VoIP.
- La conception et la mise en place d'une architecture VoIP.
- La simulation des attaques les plus connues sur la VoIP.
- L'application des politiques de sécurité nécessaires pour protéger notre architecture.

Mots Clés : VoIP, SIP, RTP, CUCM, Sécurité VoIP.

ABSTRACT

IP telephony has become a new paradigm that permits to establish and transmit voice communications with IP networks. Its deployment has been accelerated by the standardization of dedicated signaling protocols. However, VoIP services are faced to several security issues, which are inherited, from the IP layer or specific to the service. A large variety of protection mechanisms are available to deal with them. However, IP telephony is a real-time service, which requires high network performance.

The main objective of the internship is the establishment of a VoIP infrastructure taking into consideration the security of Voice over IP systems.

- Conducting a detailed study on VoIP.
- Conducting a study on security in the world of VoIP.
- The design and implementation of a VoIP architecture.
- Simulation of the most known attacks on VoIP.
- Applying the security policies needed to protect our architecture.

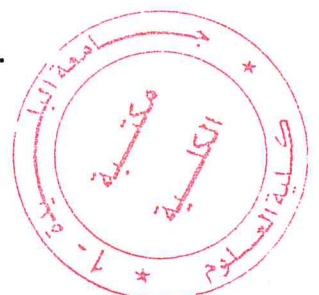


Table des Matières

Introduction Générale	1
-----------------------------	---

CHAPITRE 1 : SYSTEME TELEPHONIQUE

1. Introduction	3
2. Présentation générale de la compagnie air Algérie	3
2.1. Présentation de la filiale Catering.....	5
2.2. Organisation « Catering »	5
3. Historique du RTC.....	7
4. Téléphonie d'entreprise.....	7
4.1. Pourquoi migrer du RTPC vers la VoIP	8
4.2. Principe de fonctionnement du RTC.....	8
4.3. RTC analogique	9
5. problématique de base de la téléphonie	9
6. Comparaison de la VoIP avec la téléphonie classique.....	10
7. Avantages de la VoIP	11
8. Repenser son système de communication	11
Conclusion	12

CHAPITRE 2 : ETUDE GENERALE DE LA VOIX SUR IP

1. Introduction	14
2. Présentation de la voix sur IP	14
2.1. Architecture d'une infrastructure VoIP	14
2.1.1. Architecture de VoIP hybride.....	14
2.1.2. Architecture de VoIP « full IP »	15
2.2. Processus de traitement de la VoIP	16
2.2.1. Principe du transfert de la VoIP	16
2.2.2. Principaux codecs de la VoIP.....	17
2.3. Protocoles de la VoIP dans le modèle OSI	17
2.3.1. Protocoles de transport RTP (Real-Time Transport Protocol)	18
2.3.2. Description générale de protocole RTCP	18
3. Les standards de la VoIP	18
3.1. Protocole H.323	18
3.1.1. Architecture de H.323.....	19
3.1.2. Architecture protocolaire de H.323	20
3.1.4. Etablissement d'une connexion H.323	20

3.2. Protocole SIP	21
3.2.1. Architecture SIP	22
3.2.2. Architecture protocolaire de SIP	23
3.2.3. Initiation d'un appel SIP	24
3.4. Etude comparative entre SIP et H.323	25
3.5. Skinny Client Control Protocol	26
4. Les différents éléments d'un réseau VoIP	26
Conclusion	27

CHAPITRE 3 : LES VULNERABILITES DE L'INFRASTRUCTURE ET LES PROTOCOLES VOIP

1. Introduction	29
2. Présentation de l'existant	29
2.1. Présentation du réseau Catering	29
2.2. L'inventaire des équipements	31
3. Conception de l'infrastructure	33
3.1. Indicateurs clés de performance du réseau	33
3.2. Présentation de l'architecture à trois niveaux	34
3.3. Conception hiérarchique à deux niveaux	36
4. Vulnérabilités de l'infrastructure	37
4.1. Faiblesse du softphone	37
4.2. Latence sur la VoIP	38
4.3. Cryptage des protocoles de signalisation	38
4.4. Faiblesses de configuration des dispositifs VoIP	38
5. Sécurité des protocoles de signalisation	39
5.1. Attaques de sécurité sur le protocole SIP	39
5.2. Enumération	40
5.3. Récupération du mot de passe	41
5.4. Collecte de données pour les attaques d'authentification SIP	42
6. Attaque de l'homme au milieu	43
7. Enregistrement Hijacking	44
8. Déné de service	45
9. SIP Fuzzing	46
10. Attaques de sécurité sur le protocole RTP	46
10.1. Écoute passive	47
11. Vulnérabilité spécifique au fournisseur de Téléphones IP	50
11.1. Compromettre le fichier de configuration du téléphone	50

Conclusion	51
CHAPITRE 4 : DEPLOIEMENT ET MECANISME DE SECURITE	
1. Introduction	53
2. Environnement de travail	53
2.1. Environnement Matériel.....	53
2.2. Environnement logiciel	53
3. Architecture Réseau Déployée	54
3.1. Adressage et réseaux virtuels	55
3.2. Configuration des équipements	56
4. Sécurité de call manager	59
4.1. Utilisation du protocole TLS pour la signalisation	59
4.2. Implémentation du protocole SRTP	60
4.3. Configuration des paramètres des téléphones IP	60
5. Les éléments de sécurité de l'infrastructure	60
5.1. Gestion de l'accès à l'infrastructure	61
5.1.1 Fonction dans les commutateurs.....	61
5.1.2. Serveurs de traitement des communications (CUCM)	62
5.1.3. Flux signalisation et média chiffrées.....	62
5.1.4. Implémentation du Cisco ASA Firewall	63
5. Surveillance de la qualité de service	64
6. Sécurisation protocolaire	65
6.1. Secure RTP (SRTP)	65
6.1.1. Service de sécurités offertes par SRTP	65
6.1.2. Format du paquet SRTP	66
6.2. Sécurité du protocole SIP.....	66
6.3.1.TLS et SIPS.....	67
6.3.2. IPSec.....	69
7. Système de Contrôle d'accès AAA	70
7.1. Filtrage du Trafic sur les routeurs Avec des ACLs	74
Conclusion	74
Conclusion générale	75
Références Bibliographiques	76

Table des Figures

Figure 1 : Organigramme d'Air Algérie.....	4
Figure 2 : Organigramme Air Algérie Catering	6
Figure 3 : Principe de la téléphonie traditionnelle.....	8
Figure 4 : Schéma RTC.....	9
Figure 5: les communications unifiées.....	12
Figure 6 : Architecture de la téléphonie classique	14
Figure 7 : Architecture hybride de Téléphonie sur IP	15
Figure 8 : Architecture de Téléphonie sur IP « Full IP »	15
Figure 9 : Processus de traitement de la voix	16
Figure 10 : Architecture de H323	19
Figure 11 : Architecture protocolaire de H323	20
Figure 12 : Etablissement d'une connexion H.323.....	21
Figure 13: Architecture de SIP.....	22
Figure 14: Architecture protocolaire de SIP.....	23
Figure 15: Initiation d'un appel SIP.	24
Figure 16 : les blocs du site d'air Algérie Catering.	29
Figure 17 : Architecture réseau existant	30
Figure 18 : Indicateurs de performance du réseau	33
Figure 19 : Exemple d'une mauvaise conception réseau.....	34
Figure 20 : Architecture à trois niveaux selon Cisco	35
Figure 21 : Conception hiérarchique à deux niveaux.....	37
Figure 22 : Classification des attaques par protocole cible	39
Figure 23 : Enumeration des équipements sip sur le réseau.....	40
Figure 24 : Enumération d'extension avec Swar.	40
Figure 25 : nom d'utilisateur SIP dans Wireshark.....	41
Figure 26 : teste du mot de passe SIP.	42
Figure 27 : attaque homme au milieu avec l'authentification SIP	43
Figure 28 : Usurpation d'enregistrement SIP avec SiVuS.....	44
Figure 29 : Attaque par le BYE.....	45
Figure 30 : Attaque sur le REGISTER.....	46
Figure 31 : résultats des Adresses MAC scanner.	47
Figure 32 : les victimes de l'attaque (Man-In-The-Middle).....	48
Figure 33 : lancement d'empoisonnement ARP.	48
Figure 34 : capture de communication VoIP via RTP.	49
Figure 35 : Communication VoIP capturée par des paquets RTP via Wireshark.	49
Figure 36 : Architecture Réseaux VoIP Déployer.	54
Figure 37 : Création des Vlans.....	55
Figure 38 : Activation de la sécurité des ports.....	56
Figure 39 : Mécanisme de prévention contre les serveurs DHCP indésirable.	56
Figure 40 : Port désactivé par erreur.	57
Figure 41 : Interface Web de CUCM.	57
Figure 42 : Paramétrage du CIPC.	58
Figure 43 : Enregistrement des CIPCs.	58
Figure 44 : Etablissement d'une conversation entre les CIPCs.	59
Figure 45 : Configuration du TLS dans le Profil de Sécurité du CIPC.....	59

Figure 46 : La nouvelle Configuration des CIPCs.....	60
Figure 47 : Filtrage de La Voix encryptée.....	62
Figure 48 : Interface Web de Firewall ASA.....	63
Figure 49 : Commande “Show ip” dans Firewall ASA.....	63
Figure 50 : Configuration L'IDS dans ASA.....	64
Figure 51 : Paramétrage de la qualité de service.....	64
Figure 52 : Test de la qualité de service.....	65
Figure 53 : Format d'un Paquet SRTP.....	66
Figure 54 : Mécanismes des Sécurités SIP	66
Figure 55 : Pile protocolaire SIP avec les éléments de sécurité.....	67
Figure 56 : Échange des Messages TLS.	68
Figure 57 : Exemple d'échanges TLS pour SIP.	68
Figure 58 : IPSec en mode AH.	69
Figure 59 : IPSec en mode ESP.	70
Figure 60 : Ajout d'un client Radius Standard.....	71
Figure 61 : Stratégie d'authentification selon le nom du Client Radius.....	72
Figure 62 : Condition de notre stratégie d'authentification.	72
Figure 63 : Mécanisme d'authentification selon le standard 802.1x.....	73
Figure 64 : Phase d'authentification de l'utilisateur.....	73
Figure 65 : Configuration AAA dans Le Commutateur	74
Figure 66 : ACL Interdisant le Trafic Http et Https entrant.	74
Figure 67 : ACL Autorisant le Trafic SIP des CIPCs uniquement vers le CUCM.	74

Liste Des Tableaux

Tableau 1 : Codecs audio	17
Tableau 2 : Relation entre le modèle de référence OSI et les protocoles VoIP.....	17
Tableau 3 : Comparaison de caractéristiques entre SIP et H.323.....	25
Tableau 4: Bloc n° 1 Cellule informatique.....	31
Tableau 5 : Bloc n° 2 magasin armoire d'étage 22 U.	31
Tableau 6: Bloc n° 3 département production armoire principale 42 U.	31
Tableau 7 : Bloc n° 4 service de coordination armoire d'étage 15 U.....	31
Tableau 8: Bloc n° 5 Centre d'exploitation armoire d'étage 32 U.	32
Tableau 9 : Bloc n° 6 Technique Armoire d'étage 22 U.	32
Tableau 10 : Bloc n° 7 département handling armoire d'étage 16 U.	32
Tableau 11 : Bloc n° 8 laboratoire armoire d'étage 15 U.....	32
Tableau 12 : Recommandations d'atténuation et outils de test.	51
Tableau 13 : Les Logiciels utilisés pour la simulation.....	53
Tableau 14 : Liste des VLANs.	55

Acronymes

A

AAA: Authentication, Authorization and Accounting

ACL: Access Control List

AES: Advanced Encryption Standard

ARP: Address Resolution Protocol

C

CAN: Convertisseur Analogique Numérique

CBC: Cipher Block Chaining

CDP: Cisco Datagram Protocol

CIPC: Cisco IP Communicator

CUCM: Cisco Unified Communications Manager

D

DDoS: Distributed Denial of Service

DoS: Denial of Service

DMZ: Démilitarized Zone

DiffServ: Diffetiel Service

G

GARP: Gratuitous Address Resolution Protocol

GK: Gatekeeper

H

HIDS: Host Intrusion System Detection

HTTP: Hyper Text Transfert Protocol

I

ICMP: Internet Control Message Protocol

IDS: Intrusion Detection System

IETF: Internet Engineering Task Force

IP: Internet Protocol

IP-PBX: Internet Protocol Private Automatic eXchange

IPsec: Internet Protocol Security

ITU-T: International Telecommunications Union

L

LDAP: Lightweight Directory Access Protocol

M

MC: Multipoint Controller

MCU: Multipoint Control Unit

MIME: Multipurpose Internet Mail Extensions

MIKEY: Multimedia Internet KEYing

MITM: Man in the Middle

MKI: Master Key Identifier

N

NAT: Network Address Translation

NIDS: Network Intrusion System Detection

P

PABX: Private Automatic Branch eXchange

PBX: Private Automatic eXchange

PKI: Public Key Infrastructure

PoE: Power over Ethernet

PSK: Pre Shared Key

PSTN: Public Switched Telephone Network

Q

QoS: Quality of Service

R

RADIUS: Remote Authentication Dial in User Service

RAS: Registration Admission Status

RNIS: Réseau Numérique à Intégration de Service

RS: Redirect Server

RSVP: Resource Reservation Protocol

RTCP: Real Time Control Protocol

RTP: Real Time Protocol

RTPC: Réseau Téléphonique Public Commuté

RTSP: Real Time Streaming Protocol

RR: Receiver Report

S

SCCP: Skinny Client Control Protocol

SDP: Session Description Protocol

SHA-1: Secure Hash Algorithm 1

SIP: Session Initiation Protocol

SNMP: Simple Network Manager Protocol

SR: Sender Report

SRTCP: Secure Real-time Transport Control Protocol

SRTP: Secure RTP

SSH: Secure Shell

SSL: Secure Socket Layer

T

TCP: Transmission Control Protocol

TFTP: Trivial File Transfer Protocol

TLS: Transport Layer Security

ToIP: Telephony over IP

U

UA: User Agent

UAC: User Agent Client

UAS: User Agent Server

UDP: User Datagram Protocol

URI: Uniform Resource Identifier

V

VLAN: Virtual Local Area Network

VoIP: Voice over IP

VPN: Virtual Private Network

Introduction Générale

La téléphonie sur IP constitue actuellement une des plus importantes évolutions dans le domaine des Télécommunications. Il y a quelques années, la transmission de la voix sur le réseau téléphonique classique ou RTC constituait l'exclusivité des télécommunications. Aujourd'hui, la donne a changé. La transmission de la voix via les réseaux IP constitue une nouvelle évolution majeure comparable à la précédente. Au-delà de la nouveauté technique, la possibilité de fusion des réseaux IP et téléphoniques entraîne non seulement une diminution de la logistique nécessaire à la gestion des deux réseaux, mais aussi une baisse importante des coûts de communication ainsi que la possibilité de mise en place de nouveaux services utilisant simultanément la voix et les données.

Cette solution, qui est totalement basée sur la technologie IP, est donc affectée par les vulnérabilités qui menacent la sécurité de ce protocole et l'infrastructure réseau sur laquelle elle est déployée. Cette dernière est le majeur problème pour les entreprises et un grand défi pour les développeurs.

Pour cela la sécurité du réseau VoIP n'est pas seulement une nécessité mais plutôt une obligation, avec laquelle on peut réduire, au maximum, le risque d'attaques sur les réseaux VoIP.

La sécurité d'une solution de VoIP doit couvrir toute l'infrastructure réseau, incluant les outils et les équipements de gestion des communications et des utilisateurs, le système d'exploitation sur lesquels sont installés ces outils, et les protocoles de signalisation et de transport de données. Il faut même se protéger contre les personnes malveillantes. Mieux on sécurise, moins il y a de risques.

Le travail présenté dans ce rapport entre dans le cadre de notre projet de fin d'études en cycle master, option sécurité des systèmes d'information, à l'université de Saad Dahlab Blida, a été menée à la filiale CATERING d'Air Algérie. Le sujet était. Au long de ce rapport, on va résumer notre stage en 4 chapitres principaux.

Chapitre 1 : Système Téléphonique

Chapitre 2 : Etude Générale De La Voix Sur IP

Chapitre 3 : Les Vulnérabilités De L'infrastructure et Les Protocoles VoIP

Chapitre 4 : Déploiement Et Mécanisme de Sécurité

CHAPITRE 1

SYSTEME TELEPHONIQUE

1. Introduction

Le réseau téléphonique public commuté (RTPC) en anglais PSTN a évolué depuis qu'Alexander Graham Bell a fait la première transmission vocale sur fil en 1876. Mais, avant d'expliquer l'état actuel du RTPC et ce qu'il y a dans l'avenir, il est important que vous compreniez l'histoire du RTPC et ses bases. En tant que tel, ce chapitre discute des débuts du RTPC et explique pourquoi le RTPC existe dans son état actuel. Ce dernier couvre également les bases, les composants et les services du RTPC pour vous donner une bonne introduction à la façon dont le RTPC fonctionne aujourd'hui. Enfin, il explique comment celui-ci et d'autres réseaux vocaux évoluent au point de combiner les données, la vidéo et la voix. Mais avant d'entamer la partie technique en commencera par la présentation de notre organisme d'accueil.

2. Présentation générale de la compagnie air Algérie

Air Algérie est la compagnie nationale de transport aérien en Algérie. Elle a par conséquent des responsabilités à assurer et de devoirs à remplir tout vis-à-vis de la nation.

Air Algérie est à la fois une compagnie nationale au service de l'état et de la collectivité algérienne et une entreprise autonome dotée d'objectifs qui lui sont propres. En tant que société nationale de transport aérien air Algérie est l'instrument privilégié des échanges et du rayonnement extérieur du pays.

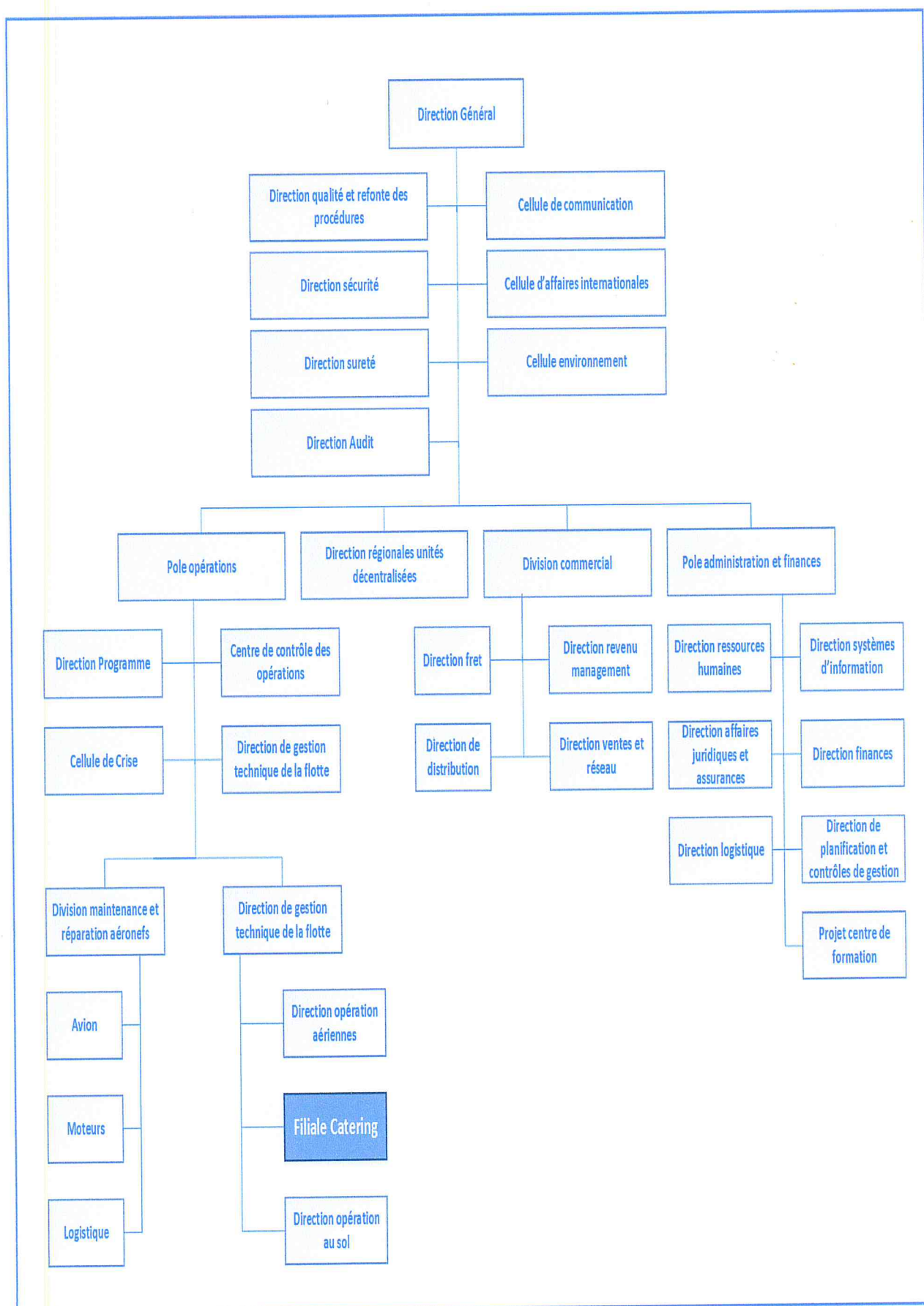


Figure 1 :Organigramme d'Air Algérie.

2.1. Présentation de la filiale Catering

Le mot Catering vient du verbe anglais *TO CATER* ce qui signifie fournir ou s'occuper de la nourriture, En Algérie comme en France ce mot est utilisé pour la prestation à bord, la fourniture des plateaux repas dans les avions, on parle alors de Catering aérien et on peut aussi trouver le Catering dans les bases de vie.

2.2. Organisation « Catering »

Pour l'accomplissement de ces opérations tant au niveau du centre exploitation (*filiale Catering*) que des escales nationales ou Internationales, une organisation a été mise en place et couvre avec efficacité toutes les étapes opérationnelles.

Elle s'articule autour de :

Deux structures opérationnelles :

- Centre exploitation composé des départements (production Food, Handling, économat, vente à bord, technique pour la gestion et l'entretien du matériel Catering et roulant).
- Sous-direction approvisionnement et magasin central (gestion des stocks, gestion des magasins, gestion des achats, transit).

Deux structures de soutien :

- Sous-direction administration et finances composé des départements (contrôle de gestion, finance et comptabilité, administration et formation).
- Sous-direction conception (suivi des escales, marketing).

Trois structures de veille technologique et de qualité :

- Informatique/tic.
- Contrôle qualité.
- QHSE.

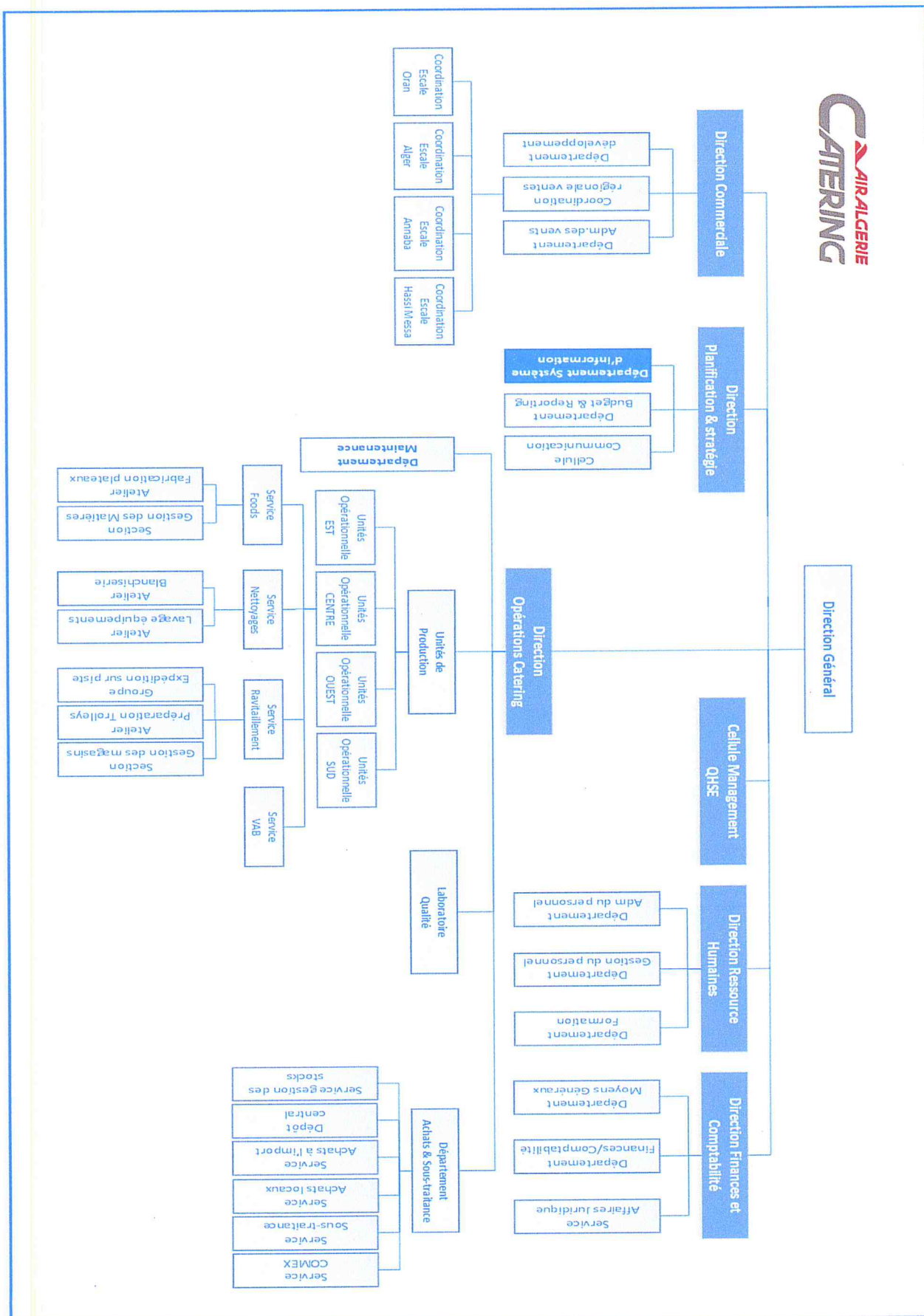


Figure 2 : Organigramme Air Algérie Catering .

3. Historique du RTC

Transmettre la voix s'avère nettement plus délicat. L'innovation vint des Etats-Unis, où Graham Bell déposa, en 1877, un brevet de système téléphonique. L'utilisation du téléphone se diffusa alors très rapidement, bénéficiant de multiples améliorations au fil des années. En 1896, l'ingénieur russe Popov réalisa la première transmission télégraphique sans fil, ouvrant ainsi la voie à la radio.

A partir des années 1910, l'évolution technologique s'accéléra considérablement avec l'apparition de l'électronique, la téléphonie devint la première activité à utiliser commercialement les nouvelles possibilités offertes par les tubes à vide. Pendant la première guerre mondiale, les différentes armées furent ainsi équipées de matériel radioélectrique utilisant des composants électroniques.

En 1926, les liaisons à ondes courtes permirent d'ouvrir un nouveau type de service commercial : les liaisons téléphoniques intercontinentales. Pour la première fois, il devenait possible de téléphoner entre Paris et New York. C'est à la même époque que furent installés les premiers câbles téléphoniques sous-marins, comme entre la France et l'Angleterre en 1927.

Dans les années 1960, l'espace apparut comme un nouveau domaine d'applications des télécommunications. Le 10 juillet 1962, le satellite de télécommunication Tel star 1 permit de réaliser la première transmission transatlantique d'image de télévision.

Dans les années 1970 sont apparus de nouveaux modes de télécommunications comme la télécopie ou encore le Minitel, favorisés par le développement de l'informatique et plus précisément de la télématique.

La dernière décennie a été marquée par l'arrivée des technologies numériques des transmissions, qui ont multiplié les possibilités de communication en s'appuyant sur le développement des semi-conducteurs dans l'électronique.

Aujourd'hui, les fibres optiques présentent des capacités considérables de transport de l'information, tandis que de nouvelles applications sont apparues : téléphonie cellulaire, télévision par satellite, réseaux télématiques tels qu'Internet, etc [1].

4. Téléphonie d'entreprise

Selon les déclarations des entreprises, 98 % d'entre elles disposent d'un ou plusieurs abonnements de téléphonie fixe. Et 2 % seulement s'appuient exclusivement sur des accès VoIP pour téléphoner.

- Une majorité d'entreprises (51 %) disposent d'installations téléphoniques hybrides avec des accès Voix sur IP, mais aussi des lignes analogiques ou numériques pour téléphoner. Il faut rappeler que même si les entreprises passent à l'IP, elles tendent généralement à garder des accès classiques en cas de défaillance du système et pour continuer à recevoir des appels entrants.

- Une grosse partie des entreprises (45 %) ne disposent que d'accès analogiques ou numériques pour téléphoner.
- Enfin, 12 % d'entreprises déclarent posséder des lignes téléphoniques dites d'urgence que ce soit des lignes pour des appels d'urgence (9 %), des lignes pour la maintenance et l'entretien des équipements (6 %), ou des lignes téléphoniques isolées dans des entrepôts (4 %) [2].

4.1. Pourquoi migrer du RTPC vers la VoIP

Les appareils VoIP sont plus faciles et moins coûteux à maintenir parce qu'ils tirent parti du réseau de données d'entreprise plutôt que de leur propre réseau vocal à usage unique.

- ✓ La VoIP augmente la valeur d'Internet en l'utilisant pour les communications vocales.
- ✓ L'intégration de la téléphonie avec des applications informatiques est beaucoup plus facile avec la VoIP qu'avec les systèmes vocaux traditionnels, car dans les paramètres VoIP, la gestion des appels a tendance à être plus ouverte, standardisée et pilotée par logiciel.
- ✓ La VoIP peut évoluer à moindre coût que les systèmes vocaux traditionnels, car elle utilise souvent du matériel PC prêt à l'emploi et fréquemment mis à jour.
- ✓ La facilité de survie contre les catastrophes et les pannes de réseau est plus facile à réaliser avec TCP / IP qu'avec les systèmes vocaux traditionnels, grâce à ses logiciels et aux remarquables mesures de résilience et protocoles de routage de TCP / IP.

4.2. Principe de fonctionnement du RTC

Utilisant le principe de la commutation de circuits, le réseau téléphonique met en relation deux abonnés à travers une liaison dédiée pendant tout l'échange voir figure 3

Un canal de communication est ouvert entre eux et l'intégralité de cette bande passante est réservée à ces deux interlocuteurs. Même s'ils ne parlent pas, la bande passante est utilisée et elle est perdue.

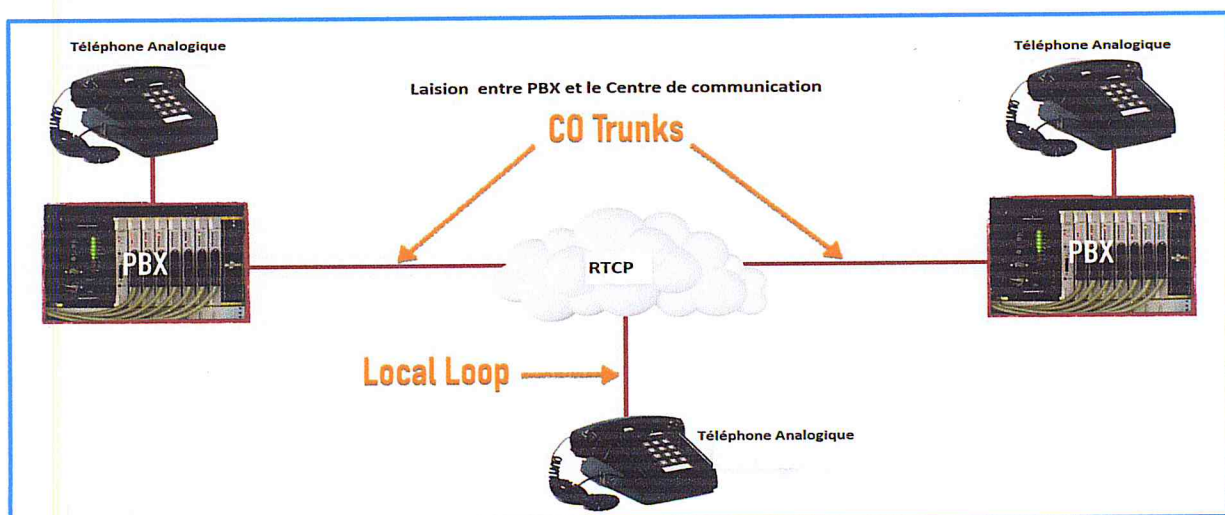


Figure 3 : Principe de la téléphonie traditionnelle.

4.3. RTC analogique

Le réseau téléphonique public commuté (RTPC) est la collection mondiale de réseaux téléphoniques publics interconnectés conçue principalement pour le trafic vocal. Le RTPC est un réseau à commutation de circuits. C'est-à-dire qu'un circuit dédié (également appelé canal) est établi pendant la durée d'une transmission, telle qu'un appel téléphonique. Cela contraste avec les réseaux de commutation de paquets, dans lesquels les messages sont divisés en petits segments appelés paquets et chaque paquet est envoyé individuellement. Internet est basé sur un protocole de commutation de paquets, TCP / IP. A l'origine seulement un système analogique, le RTPC est maintenant presque entièrement numérique, même si la plupart des abonnés sont connectés via des circuits analogiques, et il inclut maintenant les téléphones mobiles en plus des téléphones fixes. Seules les parties les plus anciennes et les plus rétrogrades du RTPC utilisent encore la technologie analogique pour tout autre chose que les connexions finales à des foyers individuels et à d'autres utilisateurs finaux. Ces dernières années, les connexions numériques ont été de plus en plus mises à la disposition des utilisateurs finaux grâce à des services tels que le RNIS (réseau numérique à intégration de services), le DSL (ligne d'abonné numérique) et le câble. Il existe de nombreux réseaux téléphoniques privés qui ne sont pas reliés au RTPC, généralement à des fins militaires. Il existe également de nombreux réseaux d'entreprise liés au RTPC uniquement par le biais de passerelles limitées.

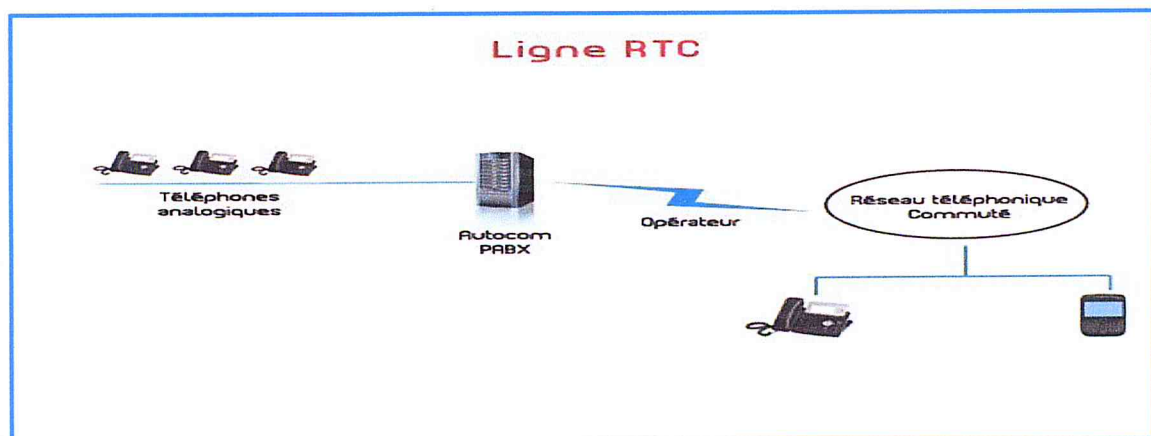


Figure 4 : Schéma RTC [2].

5. problématique de base de la téléphonie

La voix sur IP adresse deux types d'applications : celles qui, comme la téléphonie, mettent en jeu une interaction humaine, laquelle implique un temps de transit très court, et celles qui transportent des paroles unidirectionnelles, qui n'exigent pas de temps réel. Cette dernière catégorie rassemble essentiellement des transferts de fichiers contenant de la parole.

La téléphonie transportée par paquets, et plus particulièrement par paquet IP, permet d'intégrer dans un même réseau les services de données et la téléphonie. Les entreprises sont de plus en plus nombreuses à intégrer leur environnement téléphonique dans leur réseau à

transfert de paquets. Les avantages de cette intégration sont, bien sûr, la baisse des frais de communication, mais aussi la simplification de la maintenance de leurs réseaux, qui passent de deux (téléphonie et données) à un seul (données).

La difficulté de la téléphonie par paquets réside dans la très forte contrainte temporelle due à l'interaction entre individus. Le temps de latence doit être inférieur à 300 ms si l'on veut garder une interaction humaine acceptable. Si l'on souhaite une bonne qualité de la conversation, la latence ne doit pas dépasser 150 ms.

Un cas encore plus complexe se produit lorsqu'il y a un écho, c'est-à-dire un signal qui revient dans l'oreille de l'émetteur. L'écho se produit lorsque le signal rencontre un obstacle, comme l'arrivée sur le combiné téléphonique. L'écho qui repart en sens inverse est numérisé par un codec (codeur-décodeur) et traverse sans problème un réseau numérique. La valeur normalisée de la latence de l'écho étant de 56 ms, pour que l'écho ne soit pas gênant à l'oreille, il faut que le temps allé ne dépasse pas 28 ms, en supposant un réseau symétrique prenant le même temps de transit à l'aller qu'au retour. Il faut donc que, dans les équipements terminaux, les logiciels extrémité soient capables de gérer les retards et de resynchroniser les octets qui arrivent. Les équipements modernes, comme les terminaux GSM, possèdent des supprimeurs d'écho évitant cette contrainte temporelle forte.

Une autre caractéristique essentielle de la téléphonie provient du besoin d'avertir par une sonnerie la personne qui est appelée. La communication téléphonique est pour cela décomposée en deux phases : une première permettant d'avertir le destinataire, et une seconde correspondant au transport de la parole proprement dite. Il existe en réalité une troisième phase, qui consiste en la finalisation de la communication lorsqu'un des deux terminaux raccroche. Cette phase utilise le même type de protocole que la première : un protocole de signalisation.

6. Comparaison de la VoIP avec la téléphonie classique

La téléphonie classique, dite par circuit, présente les mêmes contraintes temporelles que la téléphonie par paquet. Le temps de transit doit être limité pour satisfaire le besoin d'interactivité entre individus. La limitation du temps de transit entre l'émetteur et le récepteur est relativement simple à réaliser dans une technologie circuit.

Les ressources étant réservées, la voie est toujours dégagée sur le circuit, et les ressources appartiennent uniquement aux signaux qui transitent entre l'émetteur et le récepteur. En revanche, dans un transfert de paquets, aucune ressource n'est réservée, et il est impossible de savoir quel sera le temps d'attente des paquets dans les nœuds de transfert.

7. Avantages de la VoIP

La téléphonie n'a jamais été une application simple. Les contraintes temps réel et de synchronisation pèsent lourdement sur sa mise en œuvre, et la téléphonie par paquet ne fait que compliquer le transport.

Cependant, plusieurs raisons expliquent le succès de la téléphonie par paquet, et plus spécifiquement de la téléphonie sur IP :

- **Convergence** Quel que soit le type de données véhiculées, le réseau est unique : les flux de voix, de vidéo, de textes et d'applicatifs transitent sur le même réseau. Pour les administrateurs, un seul réseau est à administrer, ce qui simplifie grandement la gestion.
- **Optimisation des ressources** Le réseau IP utilisant un transfert de paquets, l'utilisation des ressources est optimisée en comparaison des solutions de type commutation de circuits. Dans le réseau RTC, qui est à commutation de circuits, des ressources sont dédiées pour toute la durée de la communication, qu'elles soient utilisées ou non. Or les très nombreux silences d'une conversation téléphonique rendent le dimensionnement du canal réservé systématiquement trop grand.
- **Coût de transport quasiment nul** Grâce à l'intégration de la téléphonie parmi de nombreuses autres applications, le coût du transport devient pratiquement nul. L'intégration supplémentaire de la télévision dans le réseau de données fait également chuter les coûts de transport de cette application.
- **Services exclusifs** Certains services sont propres aux réseaux IP. Par exemple, le service de présence, consistant à détecter si un utilisateur est connecté au réseau ou non, ne nécessite aucune réservation de ressources dans un réseau IP, à la différence du réseau RTC. De façon analogue, pour le nomadisme des utilisateurs, il est plus simple de passer, partout dans le monde, par le réseau IP plutôt que par le réseau RTC.
- **Disparition des commutateurs locaux** Liée à la précédente, cette nouvelle donne résulte de la possibilité de gérer les téléphones depuis le réseau de l'opérateur (*système Centrex*). Des solutions intermédiaires, comme les PBX-IP, permettent de passer petit à petit des circuits numériques aux liaisons paquet IP.

8. Repenser son système de communication

De multiples technologies de substitution existent pour passer le système de communication en voix sur IP.

Parce que la communication est désormais IP de bout en bout via le Trunk SIP, il devient possible d'enrichir le service de téléphonie classique (communication voix) d'autres services complémentaires au sein de ce qu'on appelle les communications unifiées : présentiel (indicateur de présence), messagerie instantanée, outils de téléconférence (audio. Web. Et visio-conférence), outils collaboratifs, etc. Une seule interface permet alors d'atteindre les

interlocuteurs via de multiples canaux, au sein desquels la Voix devient un médium parmi d'autres.

Dans ce cas de figure, il s'agit moins de faire des économies que d'enrichir le système de communication de l'entreprise.

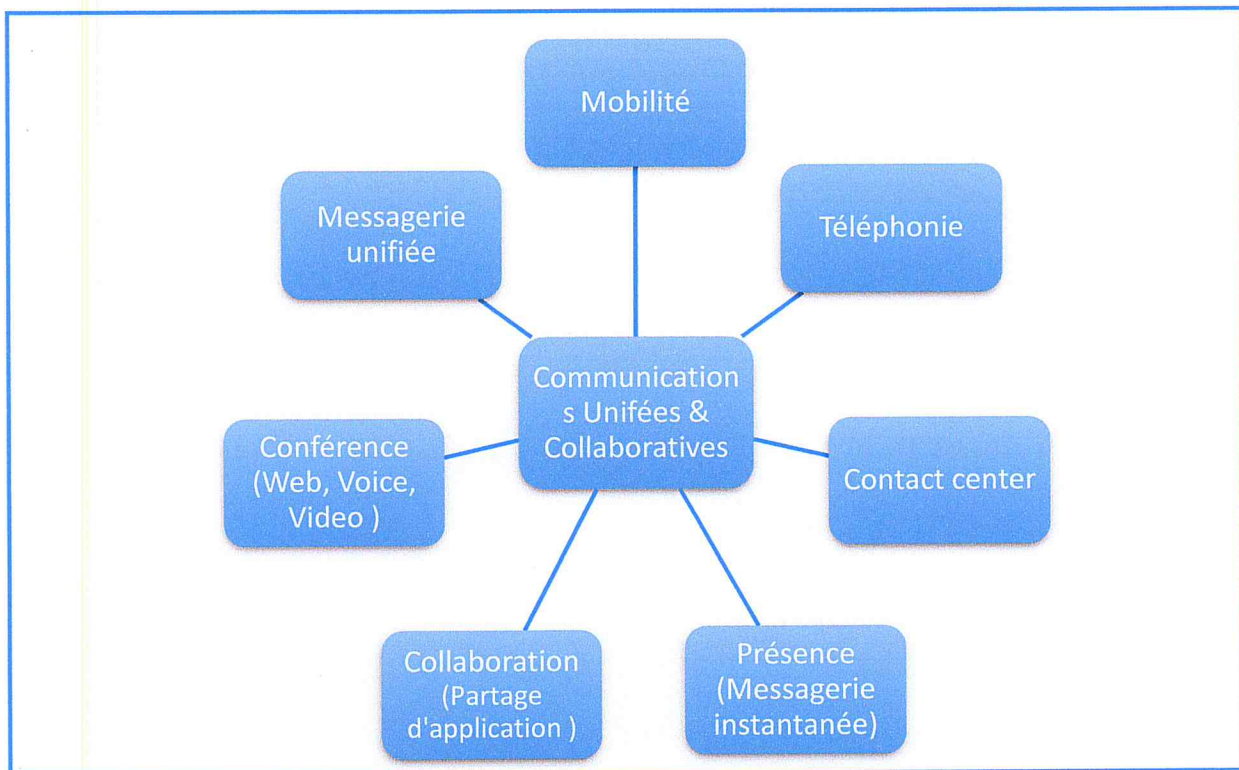


Figure 5: les communications unifiées [2].

Conclusion

Ce chapitre introductif a été consacré essentiellement à la présentation de notre organisme d'accueil et leur système de téléphonie actuelle son principe de fonctionnement et son évolution et ces limites on aussi propose notre solution de transité vers le tout IP.

Dans le deuxième Chapitre, on va faire une étude générale sur VoIP concernant L'architecture, les protocoles de signalisation et enfin en terminera par cité les différents éléments d'un réseau VoIP.

CHAPITRE 2

ETUDE GENERALE DE LA VOIX SUR IP

1. Introduction

La Voix sur IP est une technologie de communication vocale en pleine émergence. Elle fait partie d'un tournant dans le monde de la communication. En effet, la convergence du triple Play (voix, données et vidéo) fait partie des enjeux principaux des acteurs de la télécommunication aujourd'hui.

L'objectif de ce chapitre est l'étude de cette technologie et de ses différents aspects. On parlera en détail de l'architecture de la VoIP, ses éléments et son principe de fonctionnement. On détaillera aussi des protocoles VoIP de signalisation et de transport ainsi que leurs principes de fonctionnement et de leurs principaux avantages et inconvénients.

2. Présentation de la voix sur IP

La VoIP est un acronyme qui signifie *Voice Over Internet Protocol*, ou en d'autres termes, la transmission de la voix via Internet. C'est une technologie qui permet de délivrer des communications vocales ou multimédia (vidéo par exemple) via le réseau Internet (IP).

2.1. Architecture d'une infrastructure VoIP

L'architecture d'une infrastructure voix sur IP reflète le degré de convergence entre réseaux. Il existe ainsi trois scénarios de mise en œuvre de la téléphonie sur IP en entreprise

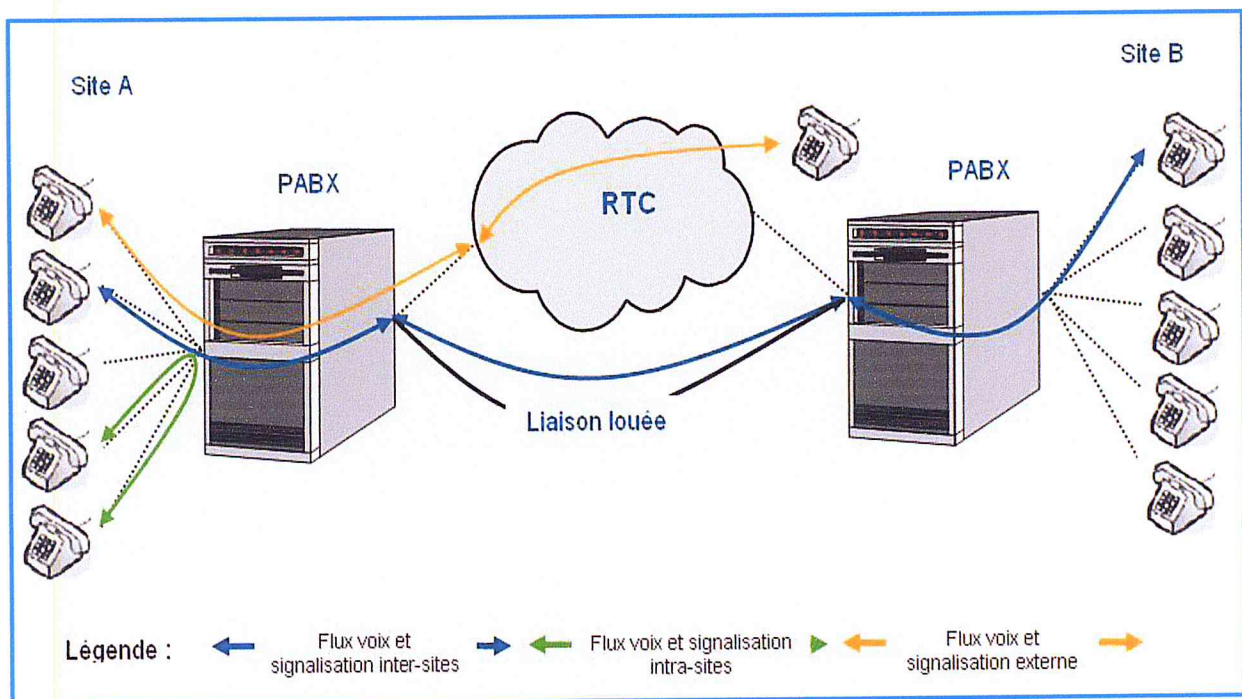


Figure 6 : Architecture de la téléphonie classique [29].

2.1.1. Architecture de VoIP hybride

Cette solution présente l'avantage de ne pas remettre en cause l'infrastructure existante (terminaux et réseau téléphonique interne équipé PABX) tout en bénéficiant des avantages du transport de la voix sur IP pour les communications inter sites. La mise en œuvre d'une solution de voix sur IP peut se faire :

- soit par l'ajout d'une carte IP sur un PABX si celui-ci est évolutif en IP
- soit, par l'ajout d'un Gateway externe au PABX
- soit, par un recours aux fonctionnalités de Gateway intégrées aux routeurs de dernière génération.

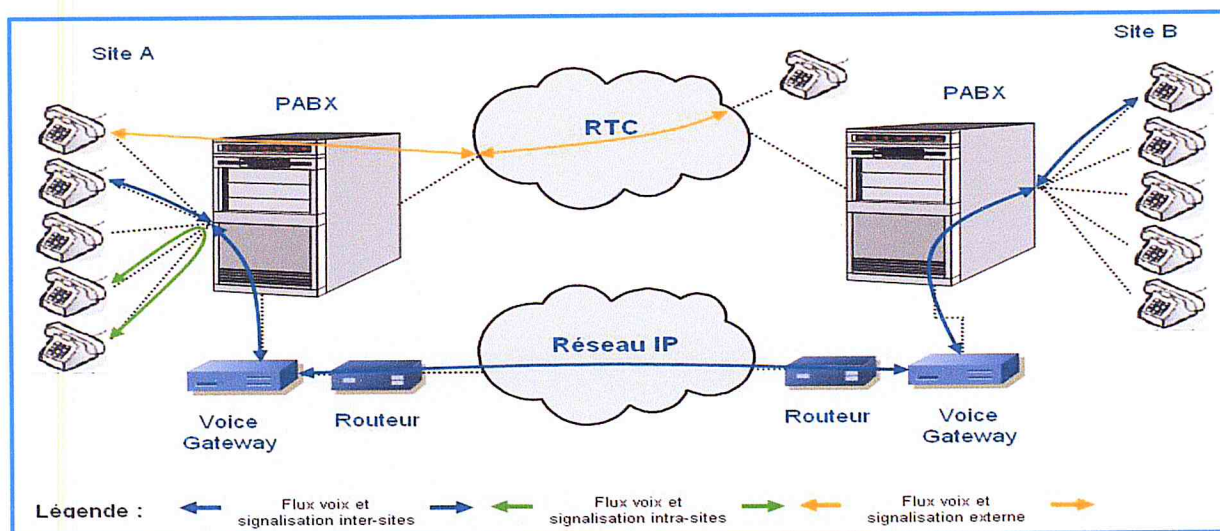


Figure 7 : Architecture hybride de Téléphonie sur IP [29].

2.1.2. Architecture de VoIP « full IP »

Ce scénario constitue une migration complète de la téléphonie de l'entreprise sur IP, incluant les terminaux téléphoniques. Plus lourde qu'une solution hybride, une telle migration s'accompagne aussi de nombreux bénéfices en posant les bases de la convergence entre le système d'information et la téléphonie de l'entreprise (voir figure8).

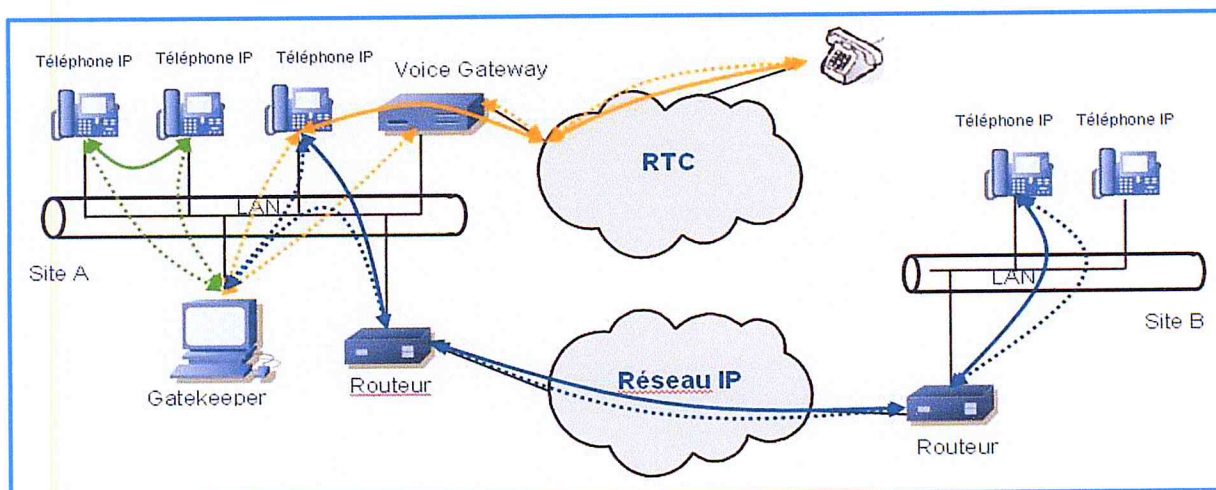


Figure 8 : Architecture de Téléphonie sur IP « Full IP » [29].

Cette représentation montre que, lors d'une communication IP inter ou intra-site, seuls les flux de signalisation transitent par le gatekeeper. Celui-ci assure la mise en relation des téléphones IP sans constituer un point de passage obligé des flux voix. La Voice Gateway est la passerelle d'accès aux réseaux publics.

2.2. Processus de traitement de la VoIP

Dans cette partie, on va représenter le principe de traitement de la VoIP, et les standards qui permettent de véhiculer la VoIP.

2.2.1. Principe du transfert de la VoIP

Le codec audio de l'émetteur numérise et compresse la voix. Ces données numériques, après la suppression de silence et l'ajout des entêtes, sont acheminées jusqu'au destinataire dans des paquets IP. Ce processus est représenté par la figure 9

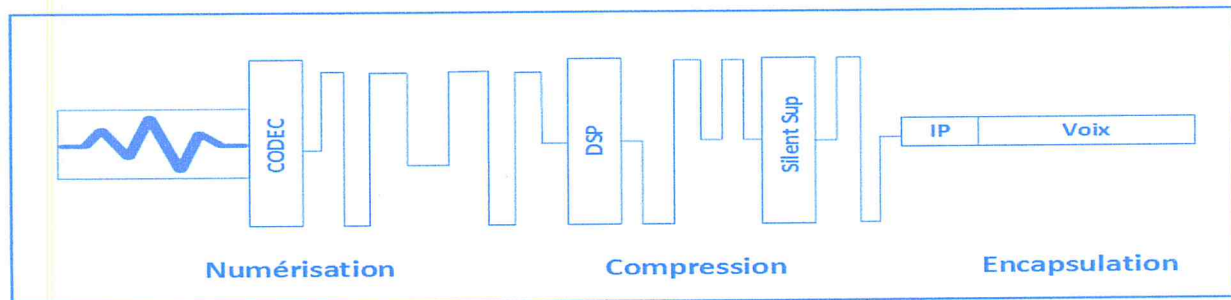


Figure 9 : Processus de traitement de la voix [3].

- La numérisation : La bande voix qui est un signal électrique analogique utilisant une bande de fréquence de 300 à 3400 Hz. Ce signal doit d'abord être converti sous forme numérique suivant le format PCM (*Pulse Code Modulation*) ou G.711 à 64 Kbps. Si l'interface téléphonique est numérique (*accès RNIS*, par exemple), cette fonction est omise. En effet, le signal est échantillonné à 8 kHz selon la théorie de Shannon, soit un échantillon toutes les 125 ms. Chaque échantillon est ensuite codé sur 8 bits, ce qui donne un débit binaire de $8 \times 8000 = 64$ kbit/s. Ce débit binaire correspond à une voix numérique non compressée.
- Compression numérique : De nombreux algorithmes permettent de réduire le besoin en bande passante à des débits nettement inférieurs (16, 8 et même 4kbit/s) et d'augmenter ainsi l'efficacité du transport de la voix sur les réseaux informatiques orientés paquets.
- La fonction de codec est le plus souvent réalisée par un DSP (*Digital Signal Processor*).

Généralement, plus le taux de compression est élevé par rapport à la référence de 64 kbit/s, 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 Operational Score*), défini par l'organisme de normalisation international ITU [3].

Pour la voix, le codec le plus utilisé est le G.711.

2.2.2. Principaux codecs de la VoIP

CODEC	Algorithme de codage	DEBIT	SCORE D'ECOUTE
G711	PCM	64 Kb/S	82%
G726	ADPCM	32Kb/S	77%
G728	LD-CELP	16Kb/S	72%
G729	CS-ACELP	8Kb/S	78%
G723.1	MPLQ	6.3Kb/S	78%
G723.1	ACELP	5.3Kb/S	73%

Tableau 1 : Codecs audio [3]

Le signal numérisé et compressé va être après découpé, on ajoute des entêtes, et on les achemine jusqu'au destinataire dans des paquets IP.

2.3. Protocoles de la VoIP dans le modèle OSI

VoIP est un protocole réseau de couche 3 qui utilise divers protocoles de couche 2 point à point ou de couche liaison tels que PPP, Frame Relay ou ATM pour son transport. VoIP active les routeurs Cisco, les serveurs d'accès et concentrateurs d'accès multiservices pour acheminer et envoyer du trafic vocal et de télécopie sur un réseau IP. En VoIP, Les processeurs de signaux numériques (DSP) segmentent le signal vocal en trames et les stockent dans des paquets vocaux. Ces paquets vocaux sont transportés via IP conformément à un protocole de communication vocale ou standard tel que H.323, protocole de contrôle de passerelle média (MGCP), ou protocole d'initialisation de session (SIP) [4].

Le tableau 2 montre la relation entre le modèle de référence OSI (*Open System Interconnection*) et les protocoles et fonctions des éléments de réseau VoIP.

Numéro de couche OSI	Nom du couche OSI	Protocoles VoIP et fonctions
7	Application	NetMeeting/Applications
6	Presentation	Codecs
5	Session	H.323/MGCP/SIP
4	Transport	RTP/TCP/UDP
3	Network	IP
2	Data Link	Frame Relay, ATM, Ethernet, PPP, MLP

Tableau 2 : Relation entre le modèle de référence OSI et les protocoles VoIP.

2.3.1. Protocoles de transport RTP (Real-Time Transport Protocol)

Le but de RTP est de fournir un moyen uniforme de transmettre sur IP des données soumises à des contraintes de temps réel (audio, vidéo, etc.). RTP permet :

- D'identifier le type de l'information transportée,
- D'ajouter des marqueurs temporels permettant d'indiquer l'instant d'émission du paquet. L'application destinataire peut alors synchroniser les flux et mesurer les délais et la gigue.
- D'inclure des numéros de séquence à l'information transportée afin de détecter l'occurrence de paquets perdus et de délivrer les paquets en séquence à l'application destinataire.

De plus, RTP peut être véhiculé par des paquets multicast afin d'acheminer des conversations vers des destinataires multiples.

Mais, RTP n'a pas été conçu pour effectuer des réservations de ressources ou contrôler la qualité de service et ne garantit pas la livraison du paquet à l'arrivée.

2.3.2. Description générale de protocole RTCP

Le protocole RTCP est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. C'est un protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service. Il existe cinq types différents de paquets RTCP pour chaque type d'information :

- SR (Sender Report) contient des statistiques de transmission et de réception pour les participants qui sont des émetteurs actifs.
- RR (Receiver Report) contient des statistiques de réception pour les participants qui ne sont pas des émetteurs actifs mais récepteurs d'une session.
- SDP (Source Description) décrit la source : nom, email, tél, etc.
- BYE permet à une station d'indiquer la fin de sa participation à une session.
- APP est un paquet de signalisation spécifique à une application.

3. Les standards de la VoIP

La VoIP n'a pas de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Il existe trois principaux standards qui sont H.323, SIP et MGCP/MEGACO. Tous les acteurs de ce marché utilisent comme base pour leur produit une ou plusieurs de ces trois architectures [5].

3.1. Protocole H.323

H.323 est un ensemble de protocoles développé par l'ITU pour les applications voix et vidéo à travers un réseau à commutation de paquets. Il a été conçu de sorte à être utilisé au-dessus de n'importe quel protocole de transport tel que TCP ou UDP. H.323 est une suite de protocoles intégrés de manière verticale. Il utilise les protocoles suivants : Q.931 pour l'établissement des appels, H.225 pour la signalisation des appels, H.245 pour les négociations

des paramètres entre les terminaux, RAS (*Registration Admission Status*) qui est chargé par l'enregistrement et admission, RTP/ RTCP, et des codecs audio ou vidéo.

3.1.1. Architecture de H.323

Plusieurs entités sont nécessaires à la réalisation d'un service de communication multimédia sur des réseaux de données. Ils sont représentés dans la figure 10.

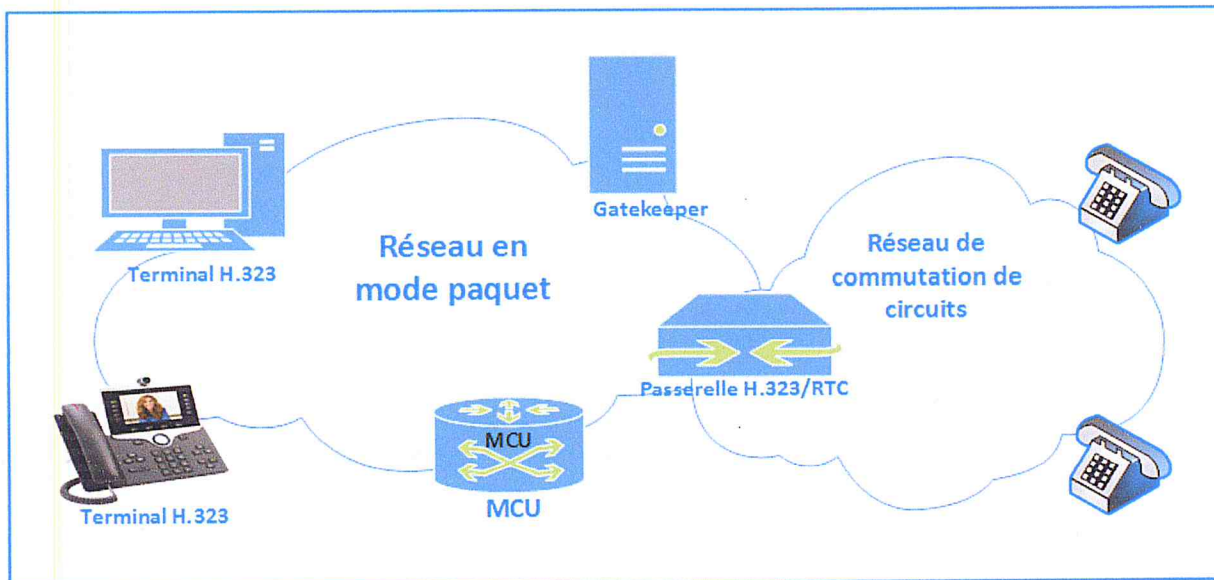


Figure 10 : Architecture de H323 [30].

- Les terminaux H.323 sont des systèmes multimédia (téléphone, PC) permettant de communiquer en « temps réel ». Ils supportent des communications à deux sens avec d'autres terminaux H.323 et doivent comporter un codec audio. Pour la négociation et l'établissement de sessions, le terminal H.323 doit supporter le protocole H.245 ainsi que le protocole de signalisation H.225, la fonction RAS pour communiquer avec le gatekeeper et le protocole RTP/RTCP pour le séquençement des paquets audio.
- Le gatekeeper gère une zone H.323 qui correspond à une collection logique de périphériques tels que les terminaux H.323, les passerelles et le MCU. Il identifie et traduit les adresses, route et contrôle les appels, l'admission et la bande passante. Le gatekeeper supporte aussi des fonctions optionnelles telles que le contrôle de la signalisation, l'autorisation des appels, la gestion de la bande passante et des appels.
- La passerelle H.323 (*Gateway*) permet d'interfacer le réseau IP avec le réseau téléphonique classique. Elle assure donc la conversion des formats et la conversion de la signalisation H.323 en signalisation RTC ou le contraire. Elle assure en plus la compression/décompression de la voix.
- L'unité de contrôle MCU (*Multipoint Controller Unit*) gère les connexions multipoint (ex. : appels de conférence). Il se décompose en un Multipoint Controller (MC), affecté à la signalisation, et un Multipoint Processor (MP), dédié à la transmission proprement dite.

3.1.2. Architecture protocolaire de H.323

La figure 11 représente les différentes couches constituant l'architecture H.323

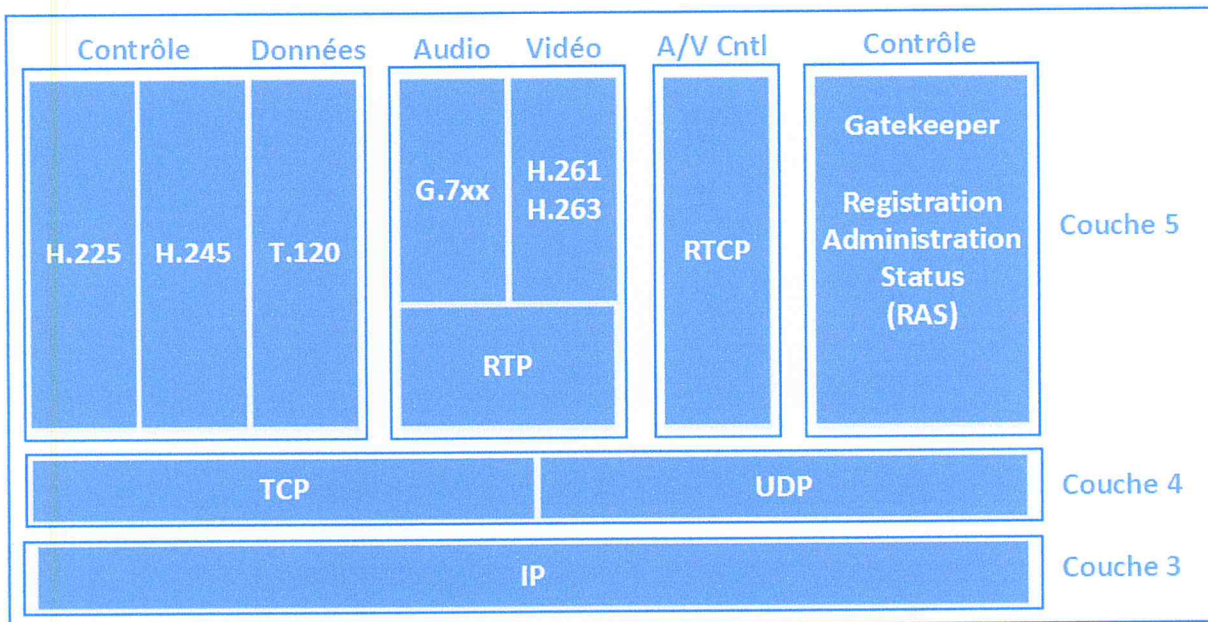


Figure 11 : Architecture protocolaire de H323 [30].

3.1.4. Etablissement d'une connexion H.323

L'établissement d'une connexion H.323 illustré par la figure 12 s'effectue à travers les étapes suivantes :

- Etablissement de la communication.
- Communication initiale et échange des capacités.
- Etablissement de la communication audiovisuelle.
- Services de communication

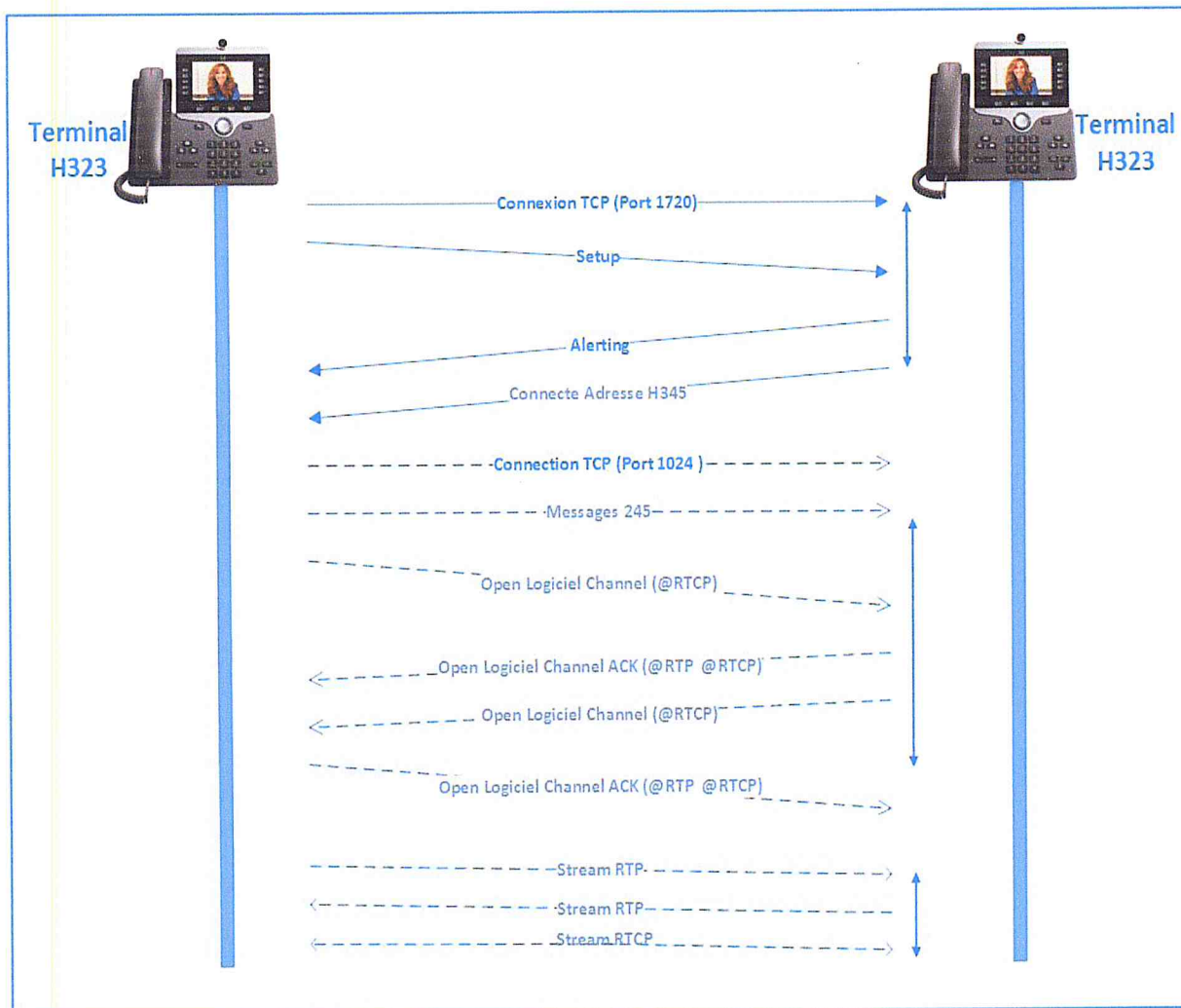


Figure 12 : Etablissement d'une connexion H.323.

Le dialogue commence par l'ouverture d'une session TCP sur le port 1720 pour l'échange des données de signalisation. Durant cet échange, les terminaux conviennent d'un numéro de port TCP supérieur à 1024 qui sera utilisé pour l'échange de contrôle (H245). Les messages H.245 échangés correspondent à la négociation des paramètres (type codec voix...).

Puis une séquence d'initialisation des canaux logique H.323 est échangée. L'échange de RTP et RTCP se fait sur UDP.

3.2. Protocole SIP

SIP est un protocole de contrôle de couche d'application (signalisation) pour créer, modifier et libérer des sessions multimédia de bout en bout, où la session multimédia peut être une conférence multimédia, un appel téléphonique Internet, une application multimédia. Une chose importante à noter est que SIP est un protocole qui gère uniquement la configuration de session, et non un protocole qui exécute les services VoIP en même temps dans une combinaison de plusieurs protocoles, tels que H.323. Cela signifie que SIP est simple et évolutif pour être utilisé avec de nombreux protocoles différents.

3.2.1. Architecture SIP

L'architecture de SIP est basée sur des relations client/serveur. Les composants qui composent SIP sont divisés en agent utilisateur et serveur réseau.

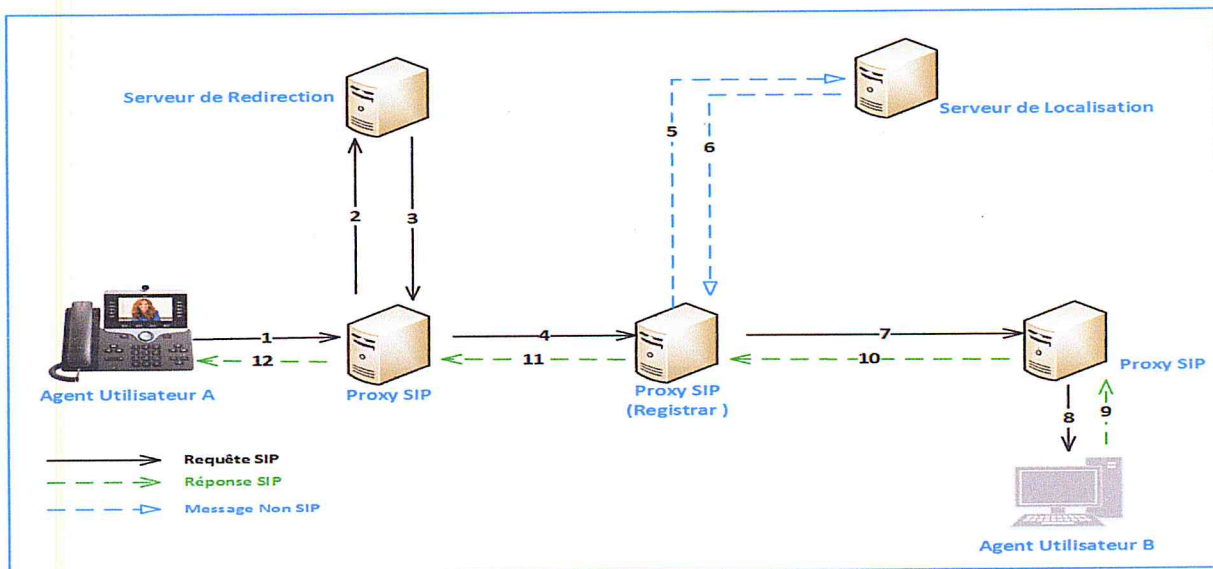


Figure 13: Architecture de SIP [31].

Les terminaux sont considérés comme clients lorsqu'ils effectuent une requête et appelés dans ce cas UAC (*User Agent Client*), et comme des serveurs lorsqu'ils y répondent et alors appelés UAS (*User Agent Server*). Les terminaux peuvent communiquer directement entre eux ou par l'intermédiaire d'autres serveurs.

Enregistrement : est la tâche de l'utilisateur informant le serveur de localisation de ses informations de localisation. Vous pouvez le faire en incluant vos informations dans la méthode REGISTER et en l'envoyant au serveur de localisation. Processus d'enregistrement du PC dans le bureau et du téléphone dans le bureau du serveur de localisation. Chaque périphérique est stocké dans la base de données du serveur de localisation et peut définir la session correcte en utilisant les informations de l'utilisateur stockées dans la base de données lorsque proxy et rediriger.

Proxy : Le serveur de réseau SIP reçoit un message INVITE (demande de connexion de session) provenant de l'UAC et décide s'il doit effectuer un proxy ou une redirection en fonction de la politique de traitement d'appel. Lorsqu'il joue un rôle en tant que serveur proxy, il transmet la demande à d'éventuels utilisateurs (UAS) et transmet la réponse de UAS à UAC à la place, c'est-à-dire, agit en tant que délégué. La figure suivante montre le processus d'opération proxy.

Redirection : Lorsque vous effectuez un rôle en tant que serveur de redirection, il envoie les informations appropriées (par exemple, adresse) sur l'appelé (l'utilisateur demandé) à l'appelant (l'utilisateur demandeur, UAC) afin que l'appelant puisse effectuer la demande INVITE

3.2.2. Architecture protocolaire de SIP

Le schéma suivant donne l'architecture protocolaire de SIP.

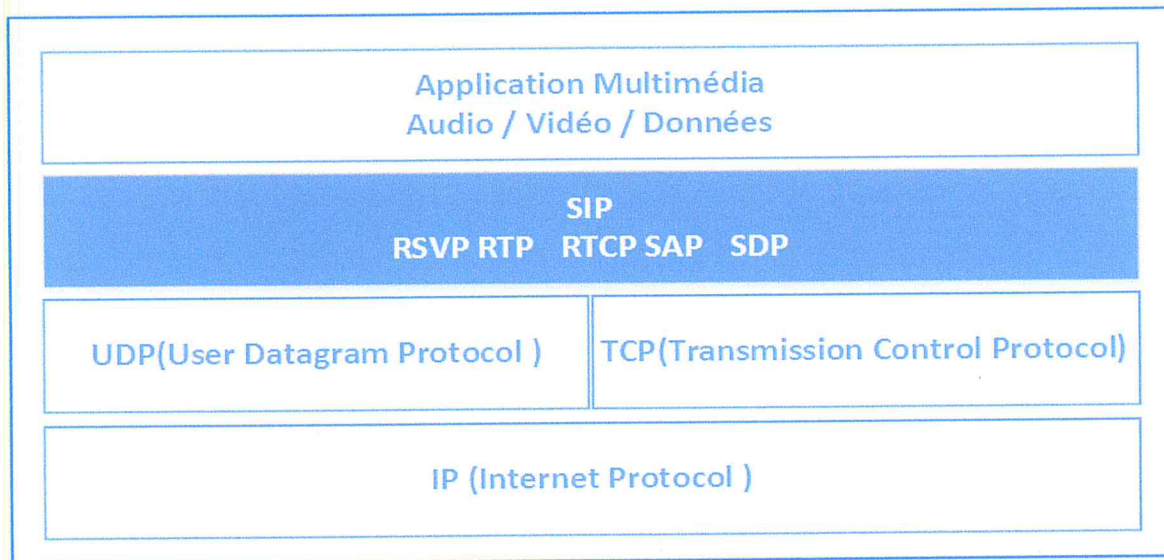


Figure 14: Architecture protocolaire de SIP [31].

Le standard SIP se base sur les protocoles suivants :

- **RSVP (*Ressource Reservation Protocol*)** : il est utilisé pour la réservation des ressources dans le réseau IP.
- **RTP/RTCP.**
- **SAP (*Session Announcement Protocol*)** : qui précise l'état des sessions multimédia ouvertes.
- **SDP (*Session Description Protocol*)**: Le protocole SDP est un protocole qui décrit les sessions audio, vidéo et multimédia. SDP utilise des caractères ASCII et donne les informations nécessaires à l'établissement d'une communication multimédia telle que l'identité de l'initiateur de la session, la bande passante disponible, les codeurs utilisés.

3.2.3. Initiation d'un appel SIP

Le protocole SIP est très simple et ses messages sont inspirés du protocole http. Un exemple d'appel avec serveur Proxy est illustré par la figure 15.

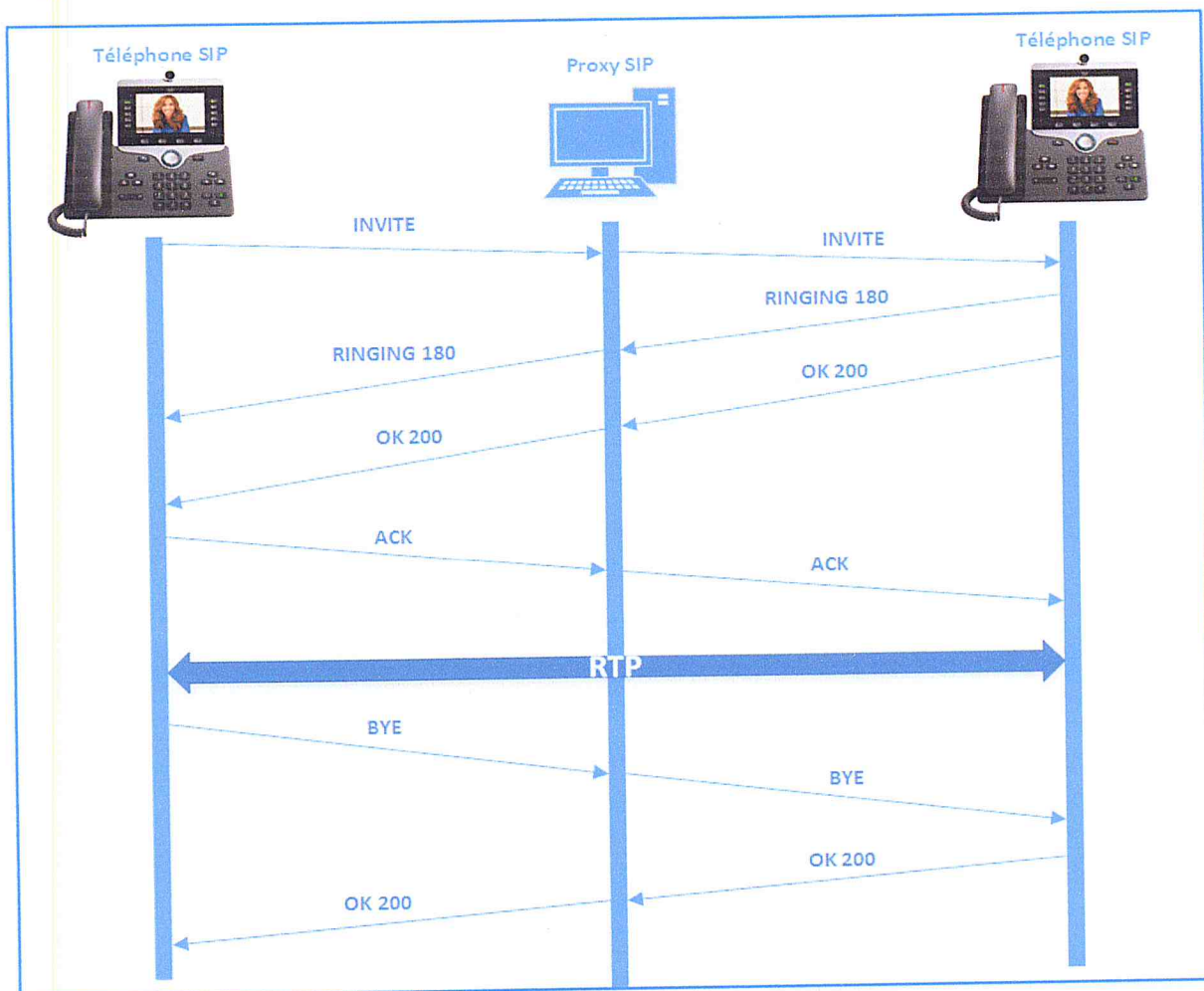


Figure 15: Initiation d'un appel SIP.

La localisation physique d'un usager s'effectue en deux étapes. L'URL SIP permet à l'utilisateur appelant de localiser le SIP Server auquel est rattachée la machine de l'appelé. Celui-ci sera la destination du message « Invite » initial. Soit le serveur connaît l'adresse physique de l'utilisateur appelé et il permettra l'établissement d'une connexion, soit il redirige la requête vers un autre lieu où il sait que l'appelé pourra être joint.

Le fait que l'URL SIP pointe sur un serveur et non sur l'utilisateur terminal donne à ce dernier une plus grande mobilité. Cela permet aussi de soulager le serveur DNS qui n'a qu'à connaître l'adresse du serveur et non de tous les terminaux reliés au serveur.

3.4. Etude comparative entre SIP et H.323

Comparons H.323 et SIP à partir de quatre perspectives.

- La complexité : H.323 a de nombreux en-têtes car elle est créée grâce à l'interopérabilité entre différents protocoles, et il est difficile à déboguer et à développer. SIP, d'autre part, est un protocole de signalisation simple qui est facile à déboguer car il envoie et reçoit des messages textuels contenant seulement quelques en-têtes.
- L'extensibilité du protocole : Pour étendre le protocole dans H.323, il est possible d'ajouter l'information désirée au nonstandardParam. Cependant, les paramètres existants ne peuvent pas être modifiés et il n'y a aucune garantie que des extensions différentes seront appliquées par différents fabricants. SIP, d'autre part, est l'extensibilité parce que c'est un système de messagerie basé sur le texte qui peut être facilement compris et fournit un moyen d'ajouter et de modifier de nouveaux en-têtes, méthodes, paramètres et corps de message.
- L'évolutivité du système: est limitée au LAN sur la base de la conception initiale, de sorte que le concept de la zone et les données traversant la zone n'ont pas encore été clairement définis. En outre, étant donné que le serveur conserve l'état de l'appel pendant qu'un appel est défini, la charge sur le serveur augmente à mesure que le nombre d'utilisateurs augmente. De plus, le contrôleur multipoint (MC) responsable du contrôle d'appel multiparti augmente également la charge de traitement lorsque le nombre d'utilisateurs augmente. D'autre part, comme SIP est lui-même une IP de base et peut utiliser un proxy sans état (un serveur proxy qui ne gère pas les informations d'état d'appel), la charge sur le serveur n'augmente pas drastiquement même s'il y a beaucoup d'utilisateurs, Aucun contrôle requis.
- Le service : H.323 est exécuté par l'interfonctionnement de divers protocoles, les fonctions de chaque protocole peuvent être utilisées. En d'autres termes, il a de nombreux services en soi. Cependant, étant donné que SIP est un protocole de signalisation simple, il n'a pas la capacité de contrôler les sessions et devrait utiliser différents protocoles (par exemple SDP).

SIP		H.323
Structure	Élément	Empiler
Instrument standard	IETF	ITU
Contrôle de conférence	Normalisation en cours	Soutien
Protocole	Centre UDP	TCP centré
Encodage	HTTP Similaire	ASN.1, Q.931
Point	Multimédia, Multicast, Événement	Téléphone

Tableau 3 : Comparaison de caractéristiques entre SIP et H.323

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 permettre à SIP de convaincre les

investisseurs. De plus, ses avancées en matière de sécurité des messages sont un atout important par rapport à ses concurrents.

3.5. Skinny Client Control Protocol

SCCP est un protocole propriétaire de Cisco qui est utilisé pour la communication entre Cisco UCM et points de terminal end points. SCCP est un protocole client-serveur, ce qui signifie tout événement (tel comme raccrochage, décroché ou boutons enfoncés) provoque l'envoi d'un message à Cisco UCM.

Cisco UCM envoie ensuite des instructions spécifiques à l'appareil pour lui dire quoi faire à propos de l'événement. Par conséquent, chaque pression sur un bouton de téléphone provoque le trafic de données entre Cisco UCM et le point de terminaison du terminal. SCCP est largement utilisé avec les téléphones IP Cisco. Le principal L'avantage de SCCP dans les réseaux Cisco UCM est sa nature exclusive, qui vous permet de modifier apporter des rapidement le protocole et ajouter des fonctionnalités.

SCCP est un protocole simplifié utilisé dans les réseaux VoIP. Les téléphones IP Cisco qui utilisent le SCCP peuvent coexister dans un environnement H.323. Lorsqu'il est utilisé avec Cisco Communications Manager, un client SCCP peut interagir avec des terminaux compatibles H.323 [6].

4. Les différents éléments d'un réseau VoIP

- Le PABX-IP : c'est lui qui assure la commutation des appels et leurs autorisations, il peut servir aussi de routeur ou de switch dans certains modèles, ainsi que de serveur DHCP. Il peut posséder des interfaces de type analogiques (*fax*), numériques (*postes*), numériques (*RNIS, QSIG*) ou opérateurs (*RTC-PSTN ou EURO-RNIS*).
- Le serveur de communications : (exemple : Call Manager de Cisco), il gère les autorisations d'appels entre les terminaux IP ou softphones et les différentes signalisations du réseau. Il peut posséder des interfaces réseaux opérateurs (*RTC-PSTN ou RNIS*), sinon les appels externes passeront par la passerelle dédiée à cela.
- La passerelle : c'est un élément de routage équipé de cartes d'interfaces analogiques et/ou numériques pour s'interconnecter avec soit d'autres PABX, soit des opérateurs de télécommunications local, national ou international.
- Le routeur : il assure la commutation des paquets d'un réseau vers un autre réseau.
- Le switch : il assure la distribution et commutation de dizaines de port Ethernet à 10/100 voire 1000 Mbits/s. Suivant les modèles, il peut intégrer la télé alimentation des ports Ethernet à la norme 802.3af pour l'alimentation des IP-phones ou des bornes WIFI en 48V.
- Le gatekeeper : il effectue les translations d'adresses (identifiant H323 et @ IP du référencement du terminal) et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action.

- Le MCU : est un élément optionnel et gère les conférences audio vidéo.
- L'IP-PHONE : c'est un terminal téléphonique ToIP 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.
- Le SOFTPHONE : c'est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP [7].

Conclusion

Dans ce chapitre, nous avons étudié le concept et le système VoIP, ainsi que les protocoles de signalisation importants (SIP, H.323). La voix sur IP devrait connaître une croissance rapide car non seulement elle permet de réaliser des économies, mais elle a aussi l'avantage de créer des services supplémentaires. Et nous avons terminé par cité les différents éléments d'un réseau VoIP

Dans le troisième chapitre, nous présenterons L'architecture réseau du Catering et en réalisera une étude détaillée sur la sécurité dans le monde de la VoIP.

CHAPITRE 3

LES VULNERABILITES DE L'INFRASTRUCTURE ET LES PROTOCOLES VOIP

1. Introduction

Après avoir étudié la théorie de la VoIP, nous passons à l'étape la plus importante et la plus critique, « Etude de l'existant », qui a pour objectif de présenter, d'analyser et de critiquer l'existant de l'entreprise d'air Algérie Catering, afin de répondre, au mieux, aux insuffisances et problèmes soulevés.

2. Présentation de l'existant

Une bonne compréhension de l'environnement du réseau informatique de Catering nous aide à déterminer le contexte et la portée de notre projet. Il est donc important d'avoir des informations précises sur l'infrastructure réseau physique Catering, ainsi que les problèmes qui peuvent influencer son fonctionnement. En effet, ces données affectent une grande partie des décisions que nous allons prendre dans le choix de la solution. La première partie sera dédiée à la présentation du réseau Catering et la seconde à l'analyse de son réseau.

2.1. Présentation du réseau Catering

Afin de faciliter la gestion du réseau, le site du Catering a été divisé en (08) blocs comme l'indique la figure 16.

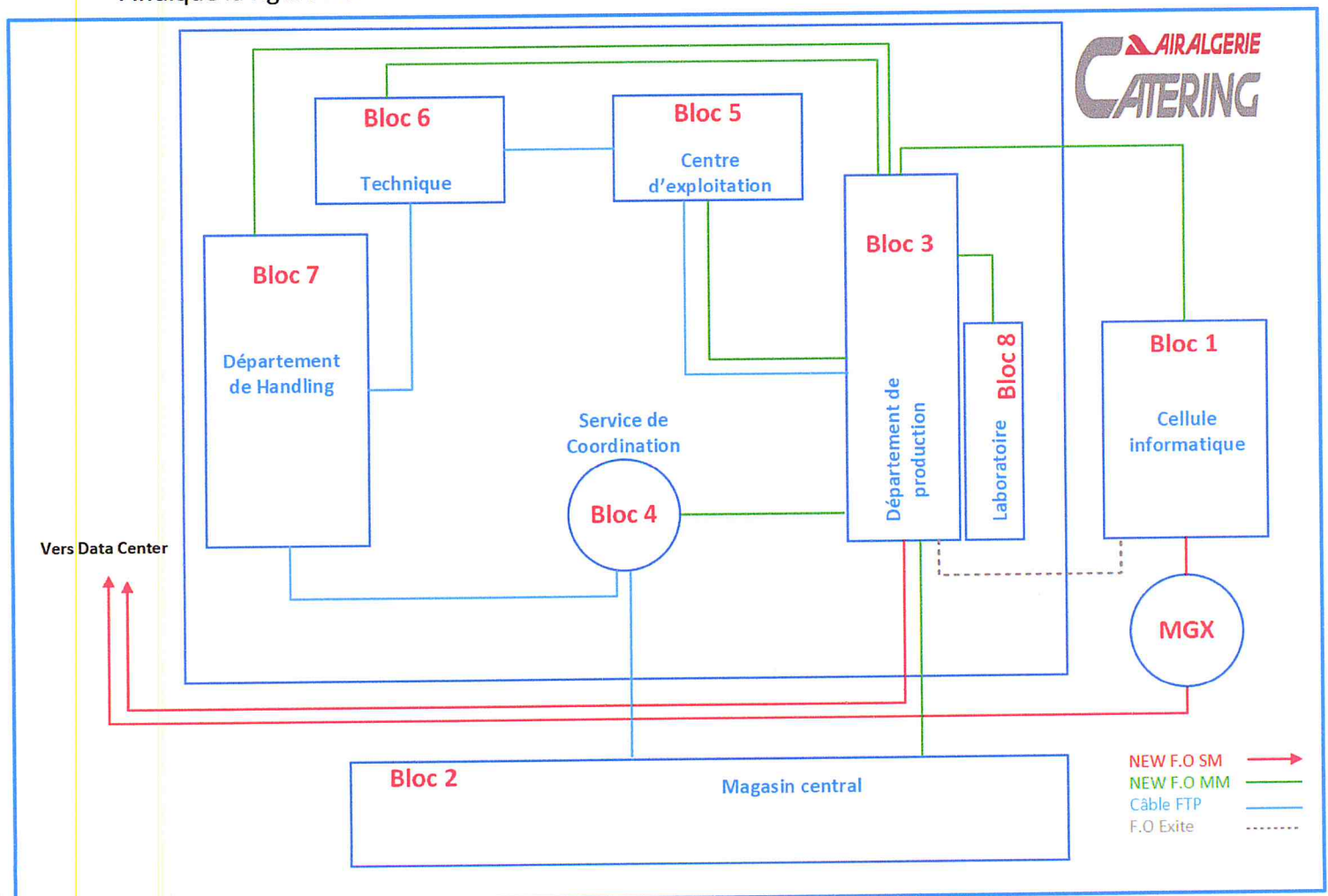


Figure 16 : les blocs du site d'air Algérie Catering.

En vas testes les attaques dans cette architecture non sécurisée et voir tous les vulnérabilités qui peu existé dans une tel situation.

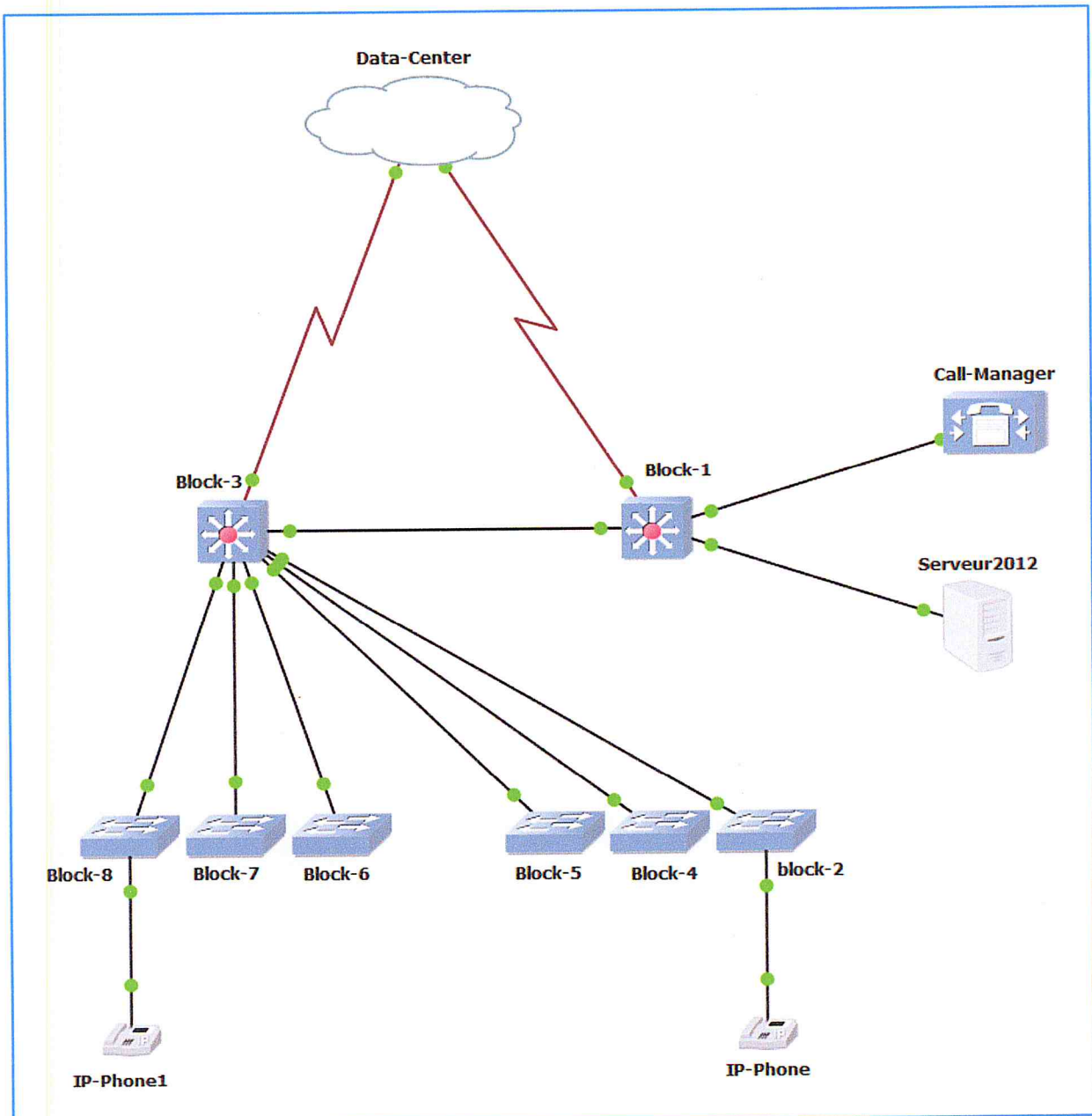


Figure 17 :Architecture réseau existant

2.2. L'inventaire des équipements

Tel que cité précédemment, le Catering est divisé en (08) blocs. Chacun couvre plusieurs entités. Les (08) tableaux ci-dessous résument l'inventaire des équipements réseau.

BLOC N 1 ADMINISTRATION		
Entités	Equipements	Quantité
• Cellule informatique	▪ Switch Cisco Catalyst 2960 ▪ Switch Cisco Catalyst 3750 ▪ Panneaux de brassage 24 ports ▪ Convertisseurs optiques ▪ Tiroir optique ▪ Point d'accès ▪ Onduleur 5000 VA	03 03 02 14 01 18 01

Tableau 4: Bloc n° 1 Cellule informatique.

BLOC N 2 MAGASIN		
Entités	Equipements	Quantité
• MAGASIN CENTRAL	• Switch Cisco Catalyst 2960 • Panneaux de Brassage 24 Ports Cat 6 • Tiroir Optique • Onduleur 1500 VA	01 01 01 01

Tableau 5 : Bloc n° 2 magasin armoire d'étage 22 U.

BLOC N 3 PRODUCTION		
Entités	Equipements	Quantité
• DEPARTEMENT PRODUCTION	• Switch Cisco Catalyst 2960 TCL • Switch Cisco Catalyst 3750X-12 S • Panneaux de Brassage Cat 6 • Tiroir Optique • Point d'accès • Onduleur 5000 VA	01 01 01 01 24 01

Tableau 6: Bloc n° 3 département production armoire principale 42 U.

BLOC N 4 COORDINATION		
Entités	Equipements	Quantité
• SERVICE DE COORDINATION	• Switch Cisco Catalyst 2960 TCL • Panneaux de Brassage 24 ports Cat 6 • Tiroirs Optique • Bandeau d'Alimentation électrique • Point d'Accès	01 01 01 01 08

Tableau 7 : Bloc n° 4 service de coordination armoire d'étage 15 U.

BLOC N 5 EXPLOITATION		
Entités	Equipements	Quantité
• CENTRE D'EXPLOITATION	• Switch Cisco Catalyst 2960 TCL	01
	• Panneaux de Brassage 24 ports Cat 6	01
	• Onduleur 1500VA	01
	• Bandeau d'Alimentation	01
	• Point d'accès	16

Tableau 8: Bloc n° 5 Centre d'exploitation armoire d'étage 32 U.

BLOC N 6 TECHNIQUE		
Entités	Equipements	Quantité
• BLOC TECHNIQUE	• Switch Cisco Catalyst 2960 TCL	01
	• Panneaux de Brassage 24 ports Cat 6	01
	• Onduleur 1500VA	01
	• Bandeau d'Alimentation	01
	• Point d'accès	09

Tableau 9 : Bloc n° 6 Technique Armoire d'étage 22 U.

BLOC N 7 PRODUCTION HANDLING		
Entités	Equipements	Quantité
• DEPARTEMENT HANDLING	• Switch Cisco Catalyst 2950	01
	• Panneaux de Brassage 24 ports Cat 6	01
	• Onduleur 2KVA	01
	• Tiroir Optique	01
	• Bandeau d'Alimentation Electrique	09
	• Point d'accès	26

Tableau 10 : Bloc n° 7 département handling armoire d'étage 16 U.

BLOC N 8 LABORATOIRE		
Entités	Equipements	Quantité
• DEPARTEMENT HANDLING	• Switch Cisco Catalyst 2960 TCL	01
	• Panneaux de Brassage 24 ports Cat 6	01
	• Onduleur 1500VA	01
	• Tiroir Optique	01
	• Bandeau d'Alimentation Electrique	09
	• Point d'accès	16

Tableau 11 : Bloc n° 8 laboratoire armoire d'étage 15 U.

3. Conception de l'infrastructure

Cisco définit des directives de conception pour créer des infrastructures solides, parmi lesquelles nous avons l'architecture à trois niveaux.

Être ingénieur réseau peut être très difficile, en particulier lorsqu'on conçoit de nouveaux réseaux. En général, on doit créer des solutions techniques répondant aux besoins réels du monde des affaires. Cependant, nous allons faire face à des contraintes strictes telles que des budgets serrés. Bien sûr, nous voulons offrir la meilleure solution possible pour un prix donné. Pour ce faire, nous devons comprendre quelles sont les options offertes par le marché et comment nous pouvons les utiliser dans ce contexte.

Mais connaître les technologies disponibles n'est pas suffisant. Nous devons sélectionner l'un par rapport à l'autre, identifier ceux qui sont obligatoires pour notre déploiement. La mise en œuvre de fonctionnalités inutiles ne fera que nuire au budget, sans pour autant apporter d'amélioration appréciable. Pour éviter cela, nous devons évaluer les exigences clairement. Nous pouvons le faire en évaluant les indicateurs décrits ci-dessous

3.1. Indicateurs clés de performance du réseau

Avant que nous puissions mettre en œuvre, nous devons évaluer la qualité de notre réseau pour ce faire, nous pouvons mesurer trois éléments clés: **l'évolutivité**, **la résilience** et la **gérabilité**. Nous nous ne tenons pas compte de ces éléments tels que les indicateurs en noir et blanc, mais en tant que zone de mesure. Chaque indicateur a sa propre échelle et nous devons identifier le niveau de mise en œuvre de chaque indicateur [8].

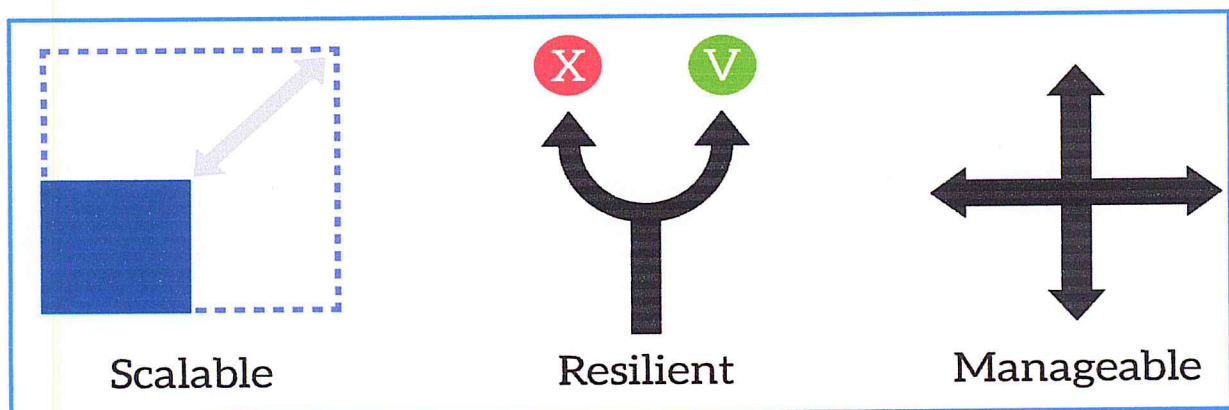


Figure 18 :Indicateurs de performance du réseau [8].

Chaque réseau doit répondre à ces trois exigences au moins dans une certaine mesure. Si nous comprenons ce que sont ces exigences, nous pouvons alors définir un design qui les implémente le mieux possible.

- **L'évolutivité (*Scalable*)** est la capacité du réseau à s'adapter à la croissance future. Dans un réseau évolutif, vous pouvez ajouter d'autres commutateurs pour prendre en charge un plus grand nombre d'utilisateurs sans avoir à modifier la conception entière. Souvent, cela se traduit par la possibilité d'ajouter des composants sans interruption de service sur les périphériques déjà en place.

- **Un réseau résilient (*Resilient*)** peut tolérer les défauts des périphériques et continuer à fonctionner même en cas de défaillance d'un composant principal. Cela est possible en utilisant des périphériques secondaires capables de prendre en charge la charge en cas de défaillance. Plus le réseau peut tolérer de fautes, meilleure est la résilience. En outre, considérons qu'avant que le périphérique secondaire puisse prendre le relais, il pourrait y avoir un certain retard. Encore une fois, moins ce retard est important, meilleure est la résilience.
- **La facilité de gestion (*Manageable*)** est assez explicite. C'est la facilité que vous avez lors de la gestion du réseau. Vous devriez être en mesure de mettre à niveau le matériel et les logiciels, de remplacer les composants avec seulement des pannes limitées. En plus de cela, votre réseau devrait être facile à dépanner et à travailler. Vous devez savoir de manière déterministe ce qui se passe et pourquoi cela se produit. Dans l'ensemble, cette fonctionnalité reflète la clarté de la solution.

3.2. Présentation de l'architecture à trois niveaux

Avant de pouvoir identifier un bon réseau, nous devons identifier un mauvais réseau. Souvent, les petites et moyennes entreprises sous-estiment l'importance d'un réseau sain. Par conséquent, ils n'embauchent pas de spécialiste réseau pour leur réseau. Cela ne peut signifier qu'un réseau qui ne répondant pas aux trois exigences définies ci-dessus, Voici un exemple.

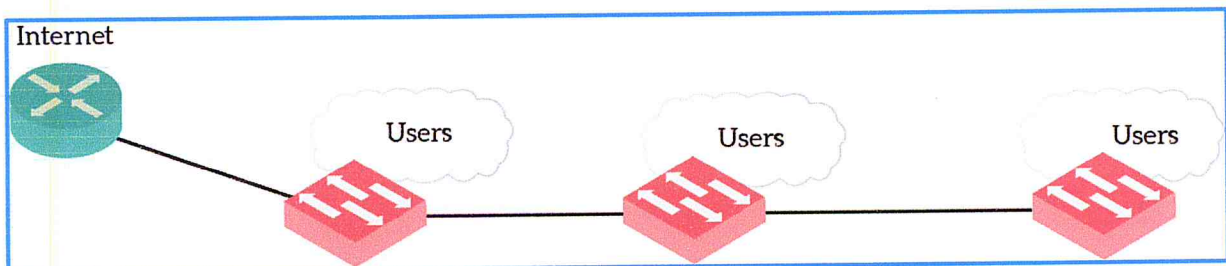


Figure 19 :Exemple d'une mauvaise conception réseau.

Aussi connu sous le nom de modèle hiérarchique à trois couches, il s'agit de la conception phare de Cisco pour les réseaux de campus. Ses concepts, cependant, peuvent être appliqués à n'importe quel réseau, y compris les centres de données. Cette architecture à trois niveaux est la solution la plus évolutive et la plus résiliente. Son design clair et simple le rend également très facile à gérer. La combinaison de ces caractéristiques fait de cette conception la meilleure pour les grandes entreprises, où vous devez connecter des milliers d'appareils sur un grand campus, même dans plusieurs bâtiments [9].

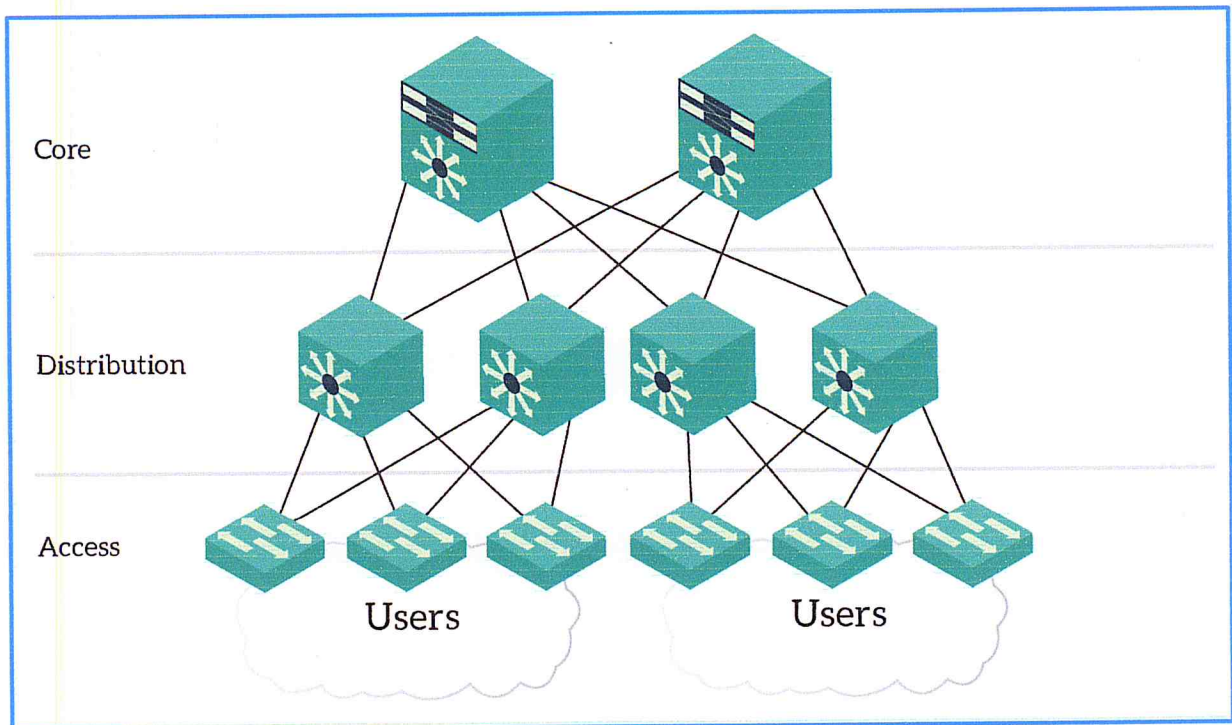


Figure 20 :Architecture à trois niveaux selon Cisco [8].

Cette approche définit trois couches: **Core, Distribution et Access**. Chaque couche à son objectif spécifique, donc ce que nous implémentons dans la couche d'accès ne sera pas implémenté sur la distribution et ainsi de suite.

❖ **Couche d'accès**

À cette couche, nous appliquons des politiques d'accès au réseau. Ce sont les politiques de sécurité que nous voulons appliquer afin de permettre l'accès au réseau. Par exemple, nous pouvons configurer **la sécurité des ports** ou **le contrôle d'accès** au réseau pour garantir que seul le PC de notre société puisse avoir accès au réseau. Les commutateurs d'accès propagent les domaines de diffusion de couche 2 aux utilisateurs, nous devons donc implémenter des **VLAN** à cet endroit. De plus, puisque nous parlons de la couche 2, **Spanning-Tree** fonctionne comme un mécanisme de prévention de boucle.

La couche d'accès remplit un certain nombre de fonctions, notamment Commutation de couche 2 :

- La haute disponibilité
- Sécurité portuaire
- Classification QoS et marquage et limites de confiance
- Inspection du protocole de résolution d'adresse (ARP)
- Listes de contrôle d'accès virtuel (VACL)
- Spanning Tree
- Power over Ethernet (PoE) et VLAN auxiliaires pour VoIP

❖ Couche de distribution

La couche Distribution relie les utilisateurs à la couche principale. Il sert de colonne vertébrale majeure pour tous les utilisateurs dans une zone, de sorte qu'il connecte plusieurs commutateurs d'accès. Dans la plupart des déploiements, les passerelles par défaut pour tous les VLAN résident sur la couche Distribution.

La couche de distribution peut fournir :

- Agrégation de liens LAN ou WAN.
- Sécurité basée sur des règles sous la forme de listes de contrôle d'accès (ACL) et de filtrage.
- Services de routage entre LAN et VLAN et entre domaines de routage (par exemple, EIGRP à OSPF).
- Redondance et équilibrage de charge.
- Une limite pour l'agrégation d'itinéraires et le résumé configurés sur les interfaces vers la couche de base.
- Contrôle de domaine de diffusion, car les routeurs ou les commutateurs multicouches ne transmettent pas émissions. L'appareil sert de point de démarcation entre les domaines de diffusion.

À cette couche, nous devons utiliser des commutateurs multicouches

❖ Couche noyau

La couche noyau est celui qui coordonne tout. Il n'a qu'un seul but « connecter toutes les couches de distribution ensemble ». Dans les grandes entreprises, où nous avons plusieurs commutateurs de distribution, la couche principale est également appelée *Backbone*.

Les considérations sur la couche noyau comprennent :

- Fournir une commutation à haute vitesse (c'est-à-dire un transport rapide)
- Assurer la fiabilité et la tolérance aux pannes
- Mise à l'échelle en utilisant un équipement plus rapide et pas plus
- Éviter les manipulations de paquets gourmandes en ressources CPU causées par la sécurité, à l'inspection de la qualité de service (QoS), ou d'autres processus

3.3. Conception hiérarchique à deux niveaux

L'architecture à trois niveaux est une excellente solution pour les grandes entreprises. Cependant, cela peut être très coûteux et son coût ne sera pas justifié dans un environnement plus petit. Pas de soucis, Cisco a conçu une solution plus petite qui offre encore un certain degré d'évolutivité, de résilience et de facilité de gestion. Nous parlons de l'architecture de base collapsée, une version sous-alimentée de l'architecture à trois niveaux [9].

Avec cette conception, nous fusionnons la couche de base et la couche de distribution en une seule couche appelée noyau effondré. En conséquence, cette conception a deux couches au lieu de trois, comme dans l'image ci-dessous.

Nous avons opté pour cette architecture comme base pour créer une nouvelle conception du réseau catering.

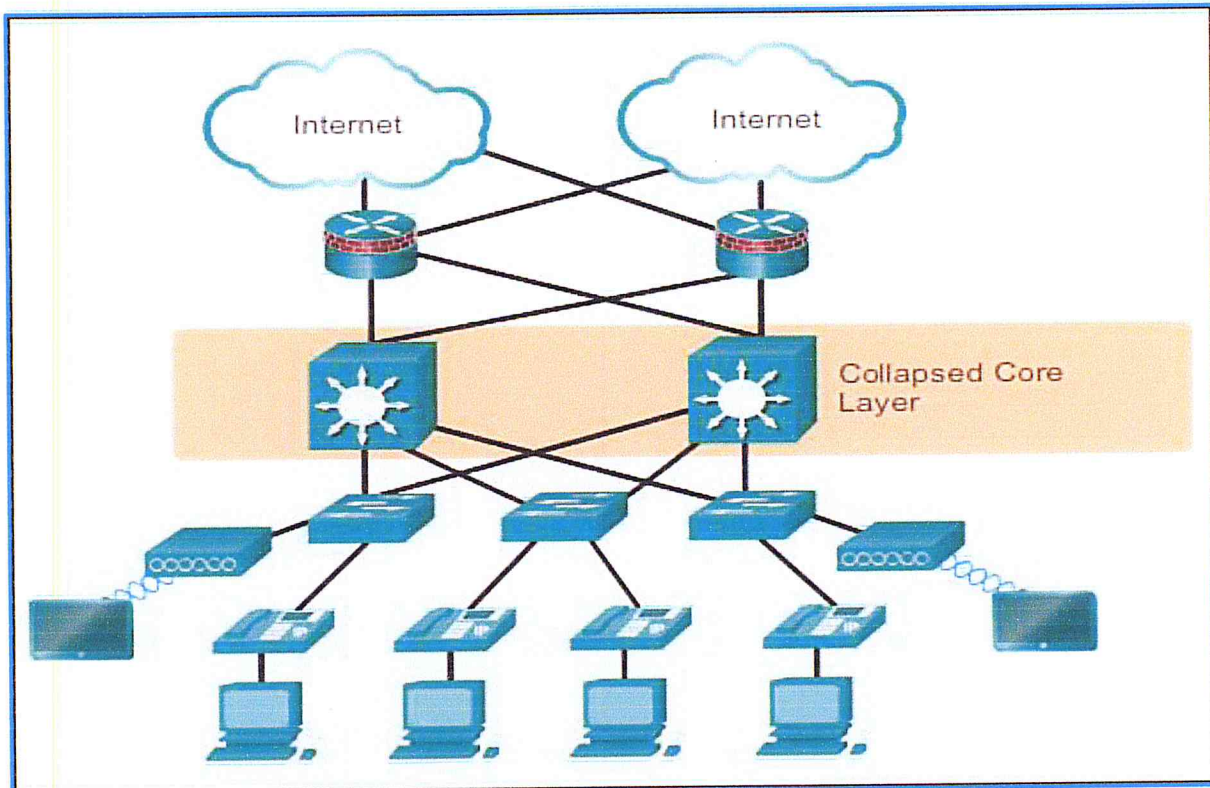


Figure 21 : Conception hiérarchique à deux niveaux [9].

4. Vulnérabilités de l'infrastructure

Au fur et à mesure que la technologie VoIP évolue, de plus en plus de départements informatiques ont fait le saut pour intégrer la VoIP dans leurs systèmes de communication d'entreprise. Mais avant qu'une organisation ne s'engage pleinement dans cette technologie, elle doit évaluer les risques et surveiller les mesures de sécurité nécessaires. Réseaux vocaux basés sur IP.

Pour les systèmes téléphoniques où l'accès contrôlé dans toute l'infrastructure de communication n'est pas nécessaire, les services qui exploitent les machines sur l'Internet public pourraient être un choix rentable. Cependant, pour les systèmes où le contrôle de réseau sécurisé est essentiel, les réseaux VoIP basés sur des infrastructures d'entreprise privées doivent être pris en compte. Nous nous concentrons sur les mesures de sécurité associées aux réseaux VoIP basés sur l'entreprise privée. Certaines mesures étendent les pratiques de sécurité réseau traditionnelles. D'autres mesures corrigent des vulnérabilités spécifiques propres au domaine VoIP [10].

4.1. Faiblesse du softphone

Les softphones, une autre attraction majeure de la technologie VoIP, sont des solutions logicielles qui fonctionnent sur des PC standard pour faire en sorte que ces PC agissent comme un téléphone IP.

Semblable aux problèmes rencontrés par les téléphones IP câblés et les pare-feu basés sur le réseau, une opération softphone peut ne pas être compatible avec les pare-feu logiciels traditionnels s'exécutant sur le même hôte. De plus, comme les contrôleurs VoIP et les passerelles, les softphones sont des applications logicielles qui résident sur un hôte PC et sont donc sujettes aux mêmes vulnérabilités que cet hôte. Cependant, un problème supplémentaire rencontré par les softphones est la difficulté de séparer le trafic vocal du softphone du trafic de données. Avec un softphone, le réseau vocal doit partager le même sous-réseau que le trafic de données.

En conséquence, toute attaque sur le réseau vocal peut potentiellement provoquer des perturbations sur le réseau de données et vice versa.

4.2. Latence sur la VoIP

TLS et IPSec varie en fonction de l'algorithme exact utilisé. Cependant, la latence ou la gigue ne peuvent pas être évitées car le dispositif cryptographique effectue les opérations mathématiques requises pour manipuler le flux de données. Étant donné qu'un retard de 150 millisecondes est perceptible et donc inacceptable, les administrateurs doivent s'assurer que les crypto dispositifs sur le réseau peuvent fonctionner dans ces limites de temps à la charge maximale.

4.3. Cryptage des protocoles de signalisation

Le cryptage de bout en bout des protocoles de signalisation empêche les pare-feu d'apprendre des ports dynamiques. Les firewalls doivent comprendre les protocoles de signalisation VoIP. Pour ce faire, ils doivent analyser et interpréter le trafic de signalisation. Si ce trafic est chiffré, alors ils ne connaîtront pas les ports autorisés. Notez que la capacité de fonctionnement du pare-feu n'est pas affectée par le chiffrement de bout en bout du flux de données vocales.

4.4. Faiblesses de configuration des dispositifs VoIP

Plusieurs dispositifs de la VoIP, dans leur configuration par défaut, peuvent avoir une variété de Ports TCP et UDP ouverts. Les services fonctionnant sur ces ports peuvent être vulnérables aux attaques DoS ou buffer overflow. Plusieurs dispositifs de la VoIP exécutent également un serveur WEB pour la gestion à distance qui peut être vulnérable aux attaques buffer overflow et à la divulgation d'informations. Si les services accessibles ne sont pas configurés avec un mot de passe, un attaquant peut acquérir un ces accès non autorisés à ce dispositif.

Les services SNMP (*Simple Network Management Protocol*) offerts par ces dispositifs peuvent être vulnérables aux attaques de reconnaissance ou attaques d'overflow.

Plusieurs dispositifs de la VoIP sont configurés pour télécharger périodiquement un fichier de configuration depuis un serveur par TFTP ou d'autres mécanismes.

Un attaquant peut potentiellement détourner la connexion et tromper le dispositif qui va télécharger un fichier de configuration malveillant à la place du véritable fichier.

5. Sécurité des protocoles de signalisation

Toute technologie, y compris la VoIP, a des problèmes de sécurité qui visent ses protocoles de communication ou ses services. La réalité est que, avec une motivation suffisante, tout problème de sécurité peut être exposé et exploité. En se basant sur l'objectif d'une personne malveillante, les attaques VoIP peuvent être classées en trois catégories : les attaques contre la signalisation, les attaques contre le transfert média et les attaques contre les services support. Dans cette partie, nous détaillons les principales attaques de sécurité contre les protocoles fondamentaux d'une infrastructure VoIP (voir figure 22) [11].

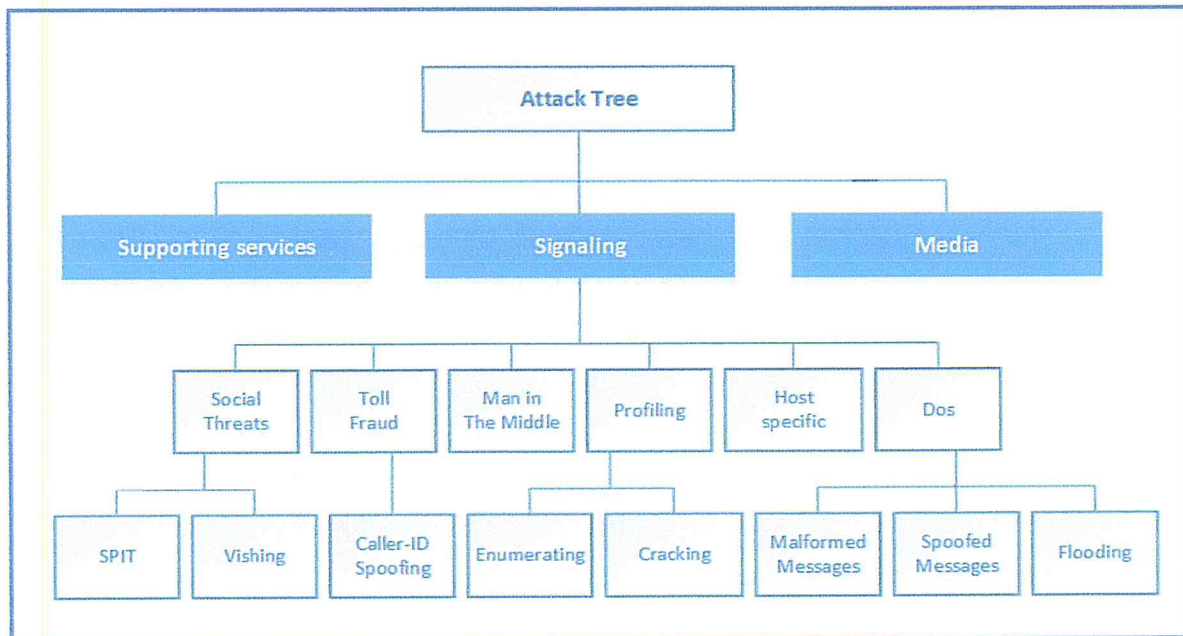


Figure 22 :Classification des attaques par protocole cible [12].

5.1. Attaques de sécurité sur le protocole SIP

Nous allons nous concentrer sur les attaques VoIP sur les appareils utilisant SIP pour l'installation de la session. Nous allons couvrir les attaques les plus connues dans les classes d'attaque critiques, à savoir :

- Nom d'utilisateur
- Cracking mot de passe SIP (attaque par dictionnaire)
- Attaque de l'homme dans le milieu
- Piratage d'enregistrement
- Usurpation des bureaux d'enregistrement et des serveurs proxy
- Dénier de service, y compris
 - ✓ BYE
 - ✓ REGISTER

5.2. Enumération

L'énumération est la clé de tout test de pénétration réussi car elle fournit les détails nécessaires et une vue d'ensemble de l'installation, la VoIP n'est pas différente. Dans le réseau VoIP, les informations utiles à nos attaquants sont les passerelles, serveurs VoIP, les systèmes IP-PBX, les logiciels clients (softphones), téléphones VoIP et les extensions utilisateur. Jetons un coup d'œil à quelques-uns des outils largement utilisés pour l'énumération et les empreintes digitales, supposons que nous connaissons les adresses IP des dispositifs déjà lus.

❖ Nmap (Périphériques)

Les analyseurs de port réseau peuvent être utilisés pour énumérer les agents utilisateurs SIP, les bureaux d'enregistrement, les serveurs proxy et d'autres systèmes compatibles SIP. Il écoute généralement sur le port TCP ou UDP 5060. Nous saisissons la commande **Nmap** suivante sur la ligne de commande / Shell pour énumérer les agents utilisateurs SIP et les autres périphériques intermédiaires [13].

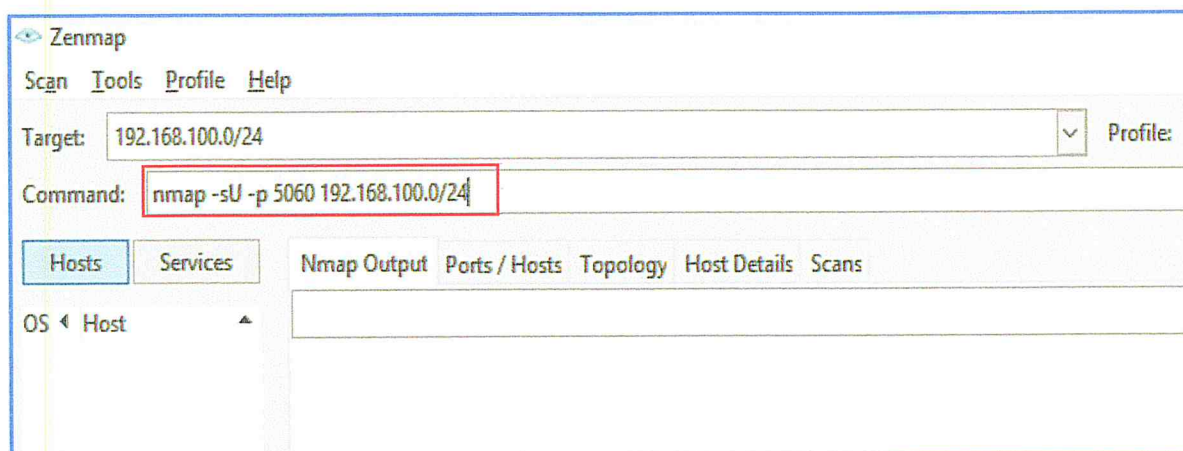


Figure 23 :Enumération des équipements sip sur le réseau.

❖ Swar (Extension)

Au cours de l'énumération VoIP, l'énumération d'extension est importante pour identifier les extensions SIP en direct. Swar vi aide à numériser une gamme complète d'adresses IP. La figure 25 montre une analyse pour les extensions utilisateur de 200 à 300. Le résultat est des extensions utilisateur qui ont été enregistrées avec le serveur IP-PBX.

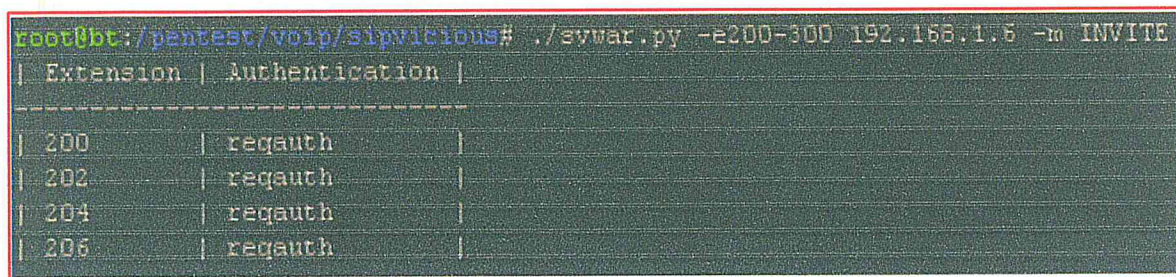
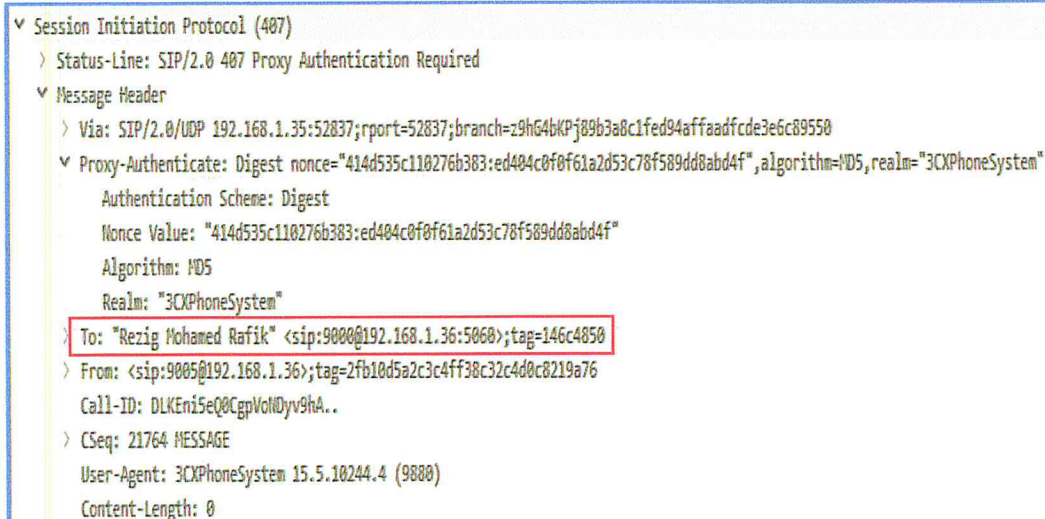


Figure 24 :Enumération d'extension avec Swar.

❖ Wireshark (Nom d'utilisateur)

La figure 25 montre un exemple d'un nom d'utilisateur reniflé sur le réseau en utilisant Wireshark. Pour voir le nom d'utilisateur SIP dans Wireshark, il faudrait accéder simplement à la section SIP du paquet, développer l'en-tête de message section, Ces champs montrent le nom d'utilisateur de l'agent en clair.



```
Session Initiation Protocol (407)
  Status-Line: SIP/2.0 407 Proxy Authentication Required
  Message Header
    Via: SIP/2.0/UDP 192.168.1.35:52837;rport=52837;branch=z9hG4bKPj89b3a8c1fed94affadfcde3e6c89550
    Proxy-Authenticate: Digest nonce="414d535c110276b383:ed404c0f0f61a2d53c78f589dd8abd4f",algorithm=MD5,realm="3CXPhoneSystem"
      Authentication Scheme: Digest
      Nonce Value: "414d535c110276b383:ed404c0f0f61a2d53c78f589dd8abd4f"
      Algorithm: MD5
      Realm: "3CXPhoneSystem"
    To: "Rezig Mohamed Rafik" <sip:9000@192.168.1.36:5060>;tag=146c4850
    From: <sip:9005@192.168.1.36>;tag=2fb10d5a2c3c4ff38c32c4d0c8219a76
    Call-ID: DLKEi5eQ0CgpVolDyv9hA..
    CSeq: 21764 MESSAGE
    User-Agent: 3CXPhoneSystem 15.5.10244.4 (9880)
    Content-Length: 0
```

Figure 25 :nom d'utilisateur SIP dans Wireshark.

5.3. Récupération du mot de passe

Le processus d'authentification de SIP utilise l'authentification Digest. Ce modèle garantit que le mot de passe n'est pas envoyé en clair. Cependant, le modèle n'est pas immunisé contre les attaques de base de dictionnaire hors ligne.

L'agent utilisateur SIP utilise les équations suivantes pour créer la valeur de réponse MD5 utilisée pour authentifier le point de terminaison sur le serveur. Notez que le seul élément qui n'est pas exposé à une machine anonyme passive sur le réseau est le mot de passe, ce qui signifie qu'il est vulnérable à une attaque de dictionnaire hors ligne. Elle consiste à soumettre un dictionnaire de mots par rapport à un algorithme de hachage donné pour en déduire le mot de passe correct :

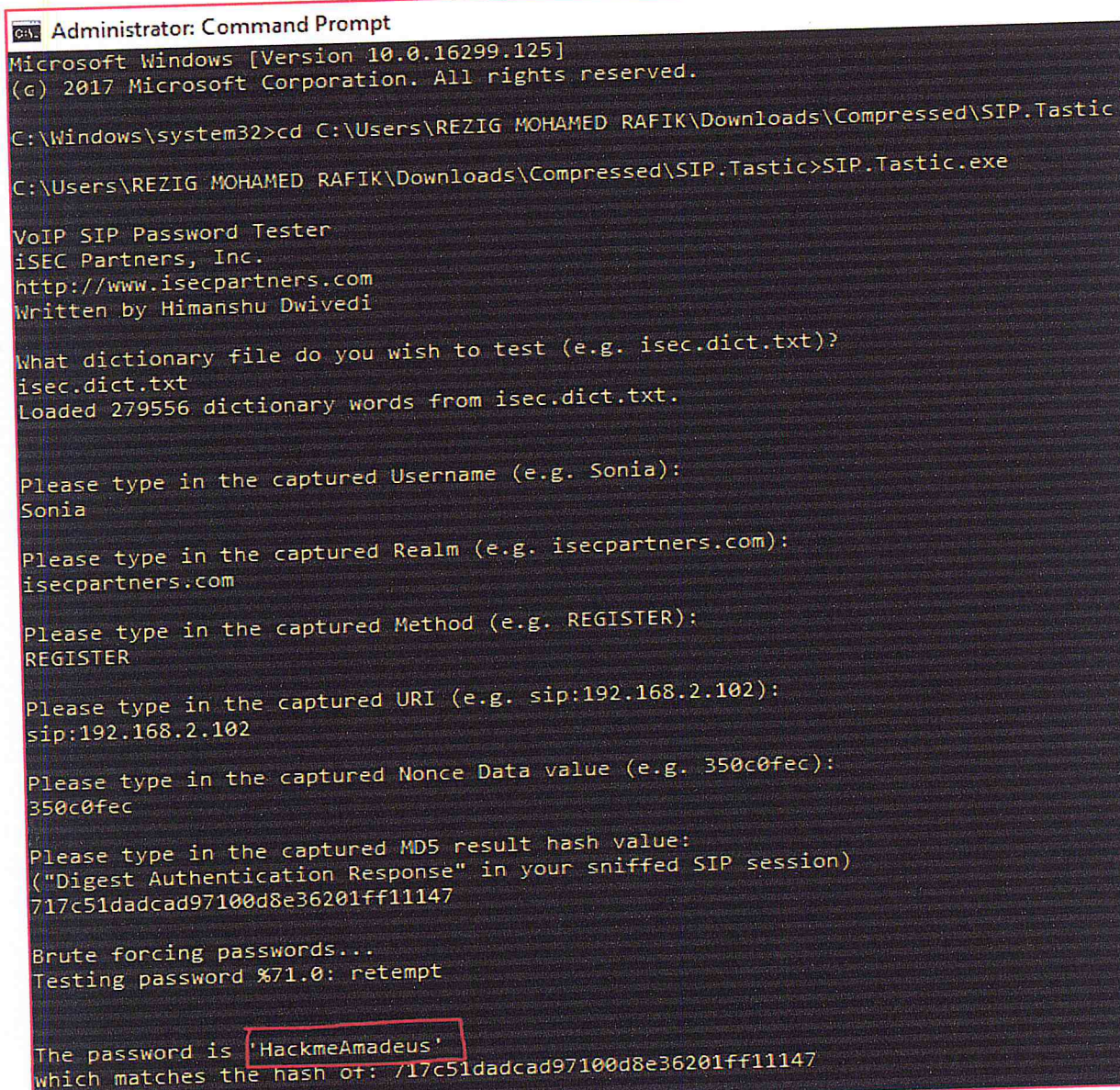
- ❖ MD5-1 = MD5 (Username: Realm: Password)
- ❖ MD5-2 = MD5 (Method: URI)
- ❖ Réponse MD5 valeur MD5 (MD51: Nonce:MD52)

Pour effectuer une attaque de dictionnaire hors ligne, l'attaquant doit d'abord ignorer le nom d'utilisateur, le domaine, la méthode, l'URI, le nonce et le hachage de réponse MD5 sur le réseau (en utilisant une attaque de type man-in-the-middle). Qui sont tous disponibles en clair. Une fois cette information obtenue, l'attaquant prend une liste de mots de passe dans le dictionnaire et insère chacun dans l'équation ci-dessus, ainsi que tous les autres éléments qui ont déjà été capturés. Une fois que cela se produit, l'attaquant aura toutes les informations pour effectuer l'attaque du dictionnaire hors ligne.

5.4. Collecte de données pour les attaques d'authentification SIP

Les informations nécessaires pour effectuer une attaque de dictionnaire hors ligne sont disponibles pour un attaquant passif à partir de deux paquets en sniffant le réseau, y compris le paquet de challenge provenant du serveur SIP et le paquet de réponse envoyé par l'agent utilisateur. Le paquet envoyé depuis le serveur SIP contient le défi et le domaine en clair. Le paquet de l'agent utilisateur contient le nom d'utilisateur, la méthode et l'URI en clair.

Cette attaque amplifie l'importance d'un mot de passe fort, celui qui ne peut pas être brutalement forcé lors de l'utilisation de l'authentification Digest. Un outil qui peut effectuer cet exercice. L'outil prend une liste de mots de passe qu'un utilisateur final souhaite tester, les concatène avec les informations requises sur le réseau (provenant de Wireshark) et détermine si la valeur de hachage MD5 résultante correspond à la valeur de hachage qui a également été détectée sur le réseau. L'outil s'appelle « **SIP.Tastic** ».



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\REZIG MOHAMED RAFIK\Downloads\Compressed\SIP.Tastic
C:\Users\REZIG MOHAMED RAFIK\Downloads\Compressed\SIP.Tastic>SIP.Tastic.exe

VoIP SIP Password Tester
iSEC Partners, Inc.
http://www.isecpartners.com
Written by Himanshu Dwivedi

What dictionary file do you wish to test (e.g. isec.dict.txt)?
isec.dict.txt
Loaded 279556 dictionary words from isec.dict.txt.

Please type in the captured Username (e.g. Sonia):
Sonia

Please type in the captured Realm (e.g. isecpartners.com):
isecpartners.com

Please type in the captured Method (e.g. REGISTER):
REGISTER

Please type in the captured URI (e.g. sip:192.168.2.102):
sip:192.168.2.102

Please type in the captured Nonce Data value (e.g. 350c0fec):
350c0fec

Please type in the captured MD5 result hash value:
("Digest Authentication Response" in your sniffed SIP session)
717c51dadcad97100d8e36201ff11147

Brute forcing passwords...
Testing password %71.0: retempt

The password is 'HackmeAmadeus'
which matches the hash of: 717c51dadcad97100d8e36201ff11147
```

Figure 26 :teste du mot de passe SIP.

6. Attaque de l'homme au milieu

En plus d'une attaque de dictionnaire hors ligne, SIP est également vulnérable à une attaque de type man-in-the-middle, comme le montre la figure. Cette attaque utilise des techniques d'empoisonnement du cache ARP ou d'usurpation DNS pour permettre à l'attaquant de passer d'un serveur SIP à l'agent utilisateur SIP légitime. Une fois que l'attaquant achemine le trafic entre les deux entités légitimes, il peut effectuer une attaque de type man-in-the-middle et s'authentifier auprès du serveur SIP sans connaître un nom d'utilisateur et un mot de passe valides. L'authentification auprès du serveur SIP augmente considérablement la surface d'attaque d'une implémentation SIP [11].

Au cours de l'attaque, comme illustré à la figure, l'attaquant surveille le réseau pour identifier quand les agents utilisateurs SIP envoient des demandes d'authentification au serveur SIP. Lorsque la demande d'authentification se produit (étape 1), il intercepte les paquets et les empêche d'atteindre le serveur SIP réel. Il envoie ensuite sa propre demande d'authentification au serveur SIP (étape 2). Utilisation de la méthode challenge / réponse pour l'authentification, le serveur SIP envoie un nonce à l'attaquant (étape 3). L'attaquant reçoit le nonce et envoie ensuite le même nonce à l'agent utilisateur légitime, qui tentait d'authentifier à l'origine (étape 4). L'agent utilisateur légitime envoie ensuite à l'attaquant une valeur de hachage MD5 valide qui est dérivé du mot de passe réel et le nonce du serveur SIP (étape 5), pensant que l'attaquant est le serveur SIP réel. Une fois que l'attaquant a la valeur de hachage MD5 digeste valide de l'agent utilisateur légitime, il envoie le hachage en son nom au serveur SIP et s'authentifie avec succès (étape 6). Une fois que l'attaquant a la valeur de hachage MD5 digeste valide de l'agent utilisateur légitime, il envoie le hachage en son nom au serveur SIP et s'authentifie avec succès (étape 7).

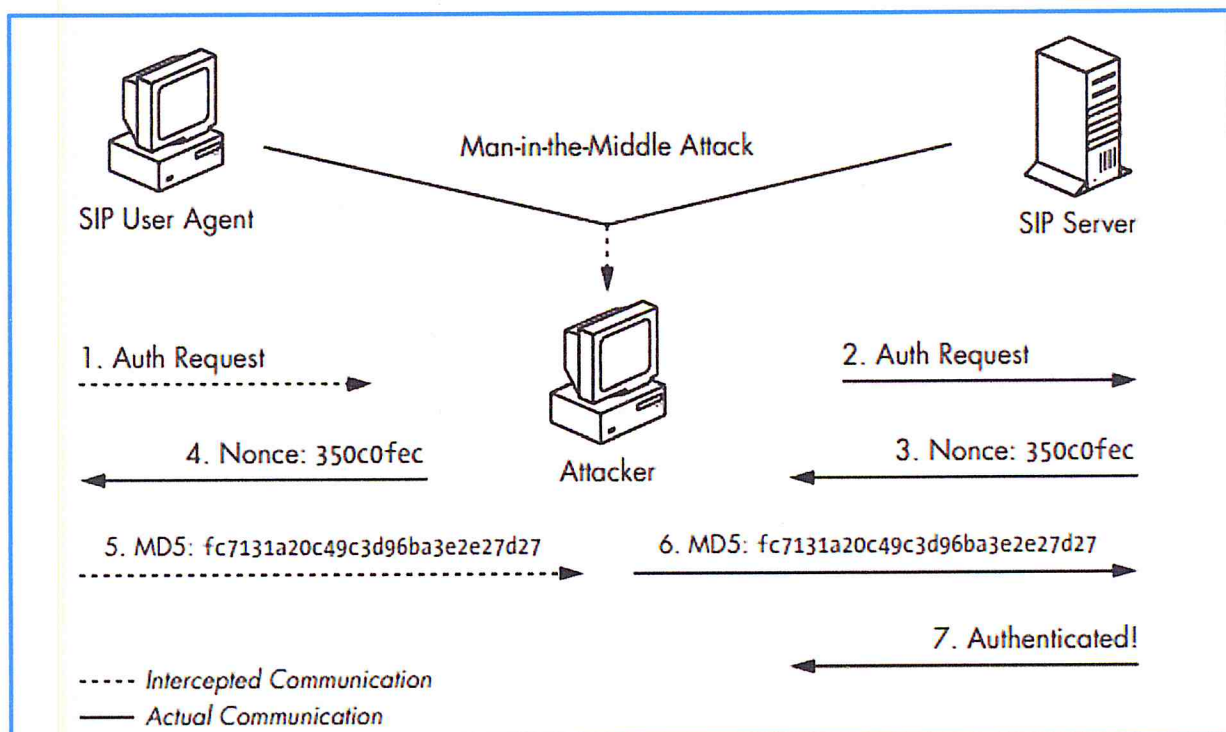


Figure 27 : attaque homme au milieu avec l'authentification SIP [11].

7. Enregistrement Hijacking

Le piratage d'enregistrement utilise une classe d'attaque datée mais fonctionne toujours dans de nombreuses nouvelles technologies telles que la VoIP. L'attaque tire parti de la capacité d'un agent utilisateur à modifier le champ « **Contact** » dans l'en-tête SIP.

Lorsqu'un agent utilisateur s'enregistre auprès d'un bureau d'enregistrement SIP, beaucoup de choses sont enregistrées, y compris les coordonnées de l'agent utilisateur. Les informations sur le point de contact, répertoriées dans le champ Contact de l'en-tête SIP, contiennent l'adresse IP de l'agent utilisateur. Elles permettent aux serveurs proxy SIP de transmettre les demandes INVITE au bon téléphone IP ou logiciel via l'adresse IP.

Afin de détourner l'enregistrement d'un agent utilisateur SIP, un attaquant peut soumettre le même paquet de demande d'enregistrement mais modifier le champ Contact dans l'en-tête SIP et insérer sa propre adresse IP. Par exemple, si un attaquant nommé **Neo** voulait pirater l'enregistrement d'un utilisateur **Alice**, il remplacerait le champ Contact, qui contient l'adresse IP de 192.168.1.5 d'**Alice**, avec le sien, qui est 192.168.1.3 **Neo** serait alors usurper La requête **REGISTER** avec son adresse IP au lieu de celle d'**Alice**, comme indiqué dans la figure 28

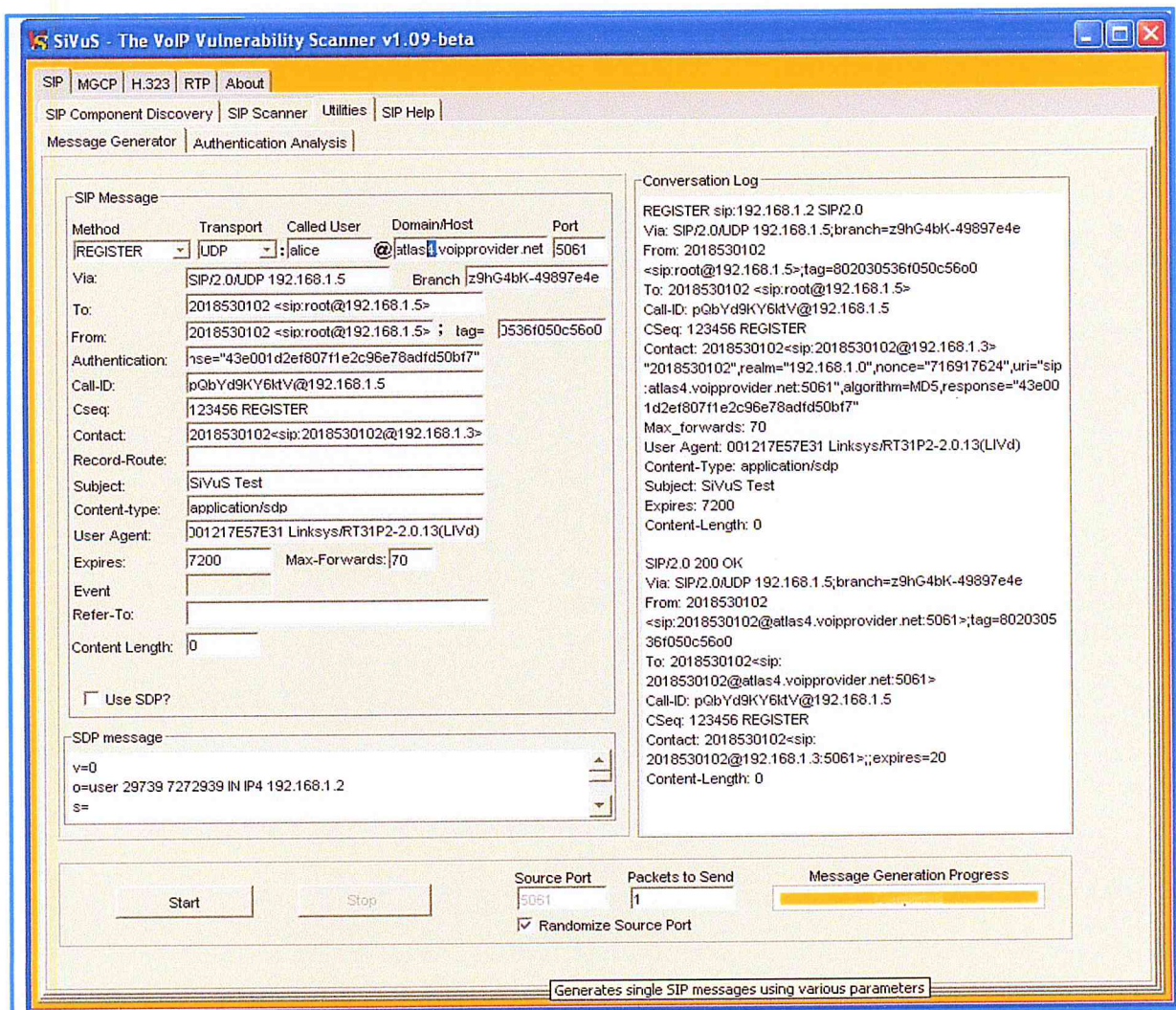


Figure 28 :Usurpation d'enregistrement SIP avec SiVuS.

8. Déni de service

Similaire aux protocoles de signalisation H.323 et SIP est également vulnérable à de nombreux Déni de service (DoS) attaques.

❖ Via un message BYE

La première attaque DoS à discuter consiste simplement à usurper le message BYE d'un agent utilisateur à un autre. Un message BYE est envoyé d'un utilisateur à un autre pour indiquer que l'utilisateur souhaite mettre fin à l'appel et ainsi mettre fin à la session. Dans des circonstances normales, un agent utilisateur envoie un message BYE une fois l'appel terminé. Cependant, un attaquant peut usurper un message BYE d'un utilisateur à un autre et mettre fin à tout appel en cours [14].

Avant que cette attaque puisse avoir lieu, un attaquant doit renifler quelques éléments d'une conversation existante entre deux parties (à partir d'un message INVITE ou similaire), en particulier l'identifiant d'appel et les valeurs d'étiquette. Une fois que l'attaquant a capturé ces entités sur le réseau, il peut créer un message BYE, en forgeant le champ « From » comme un côté de la conversation et en ajoutant la victime dans le champ « To ». Une fois que le champ « From » (qui est l'adresse source usurpée de l'attaquant), le champ « To » (qui est la victime), la valeur Call-ID et les valeurs de tag sont exactes pour l'appel, l'attaquant peut envoyer le paquet et l'appel sera terminé immédiatement.

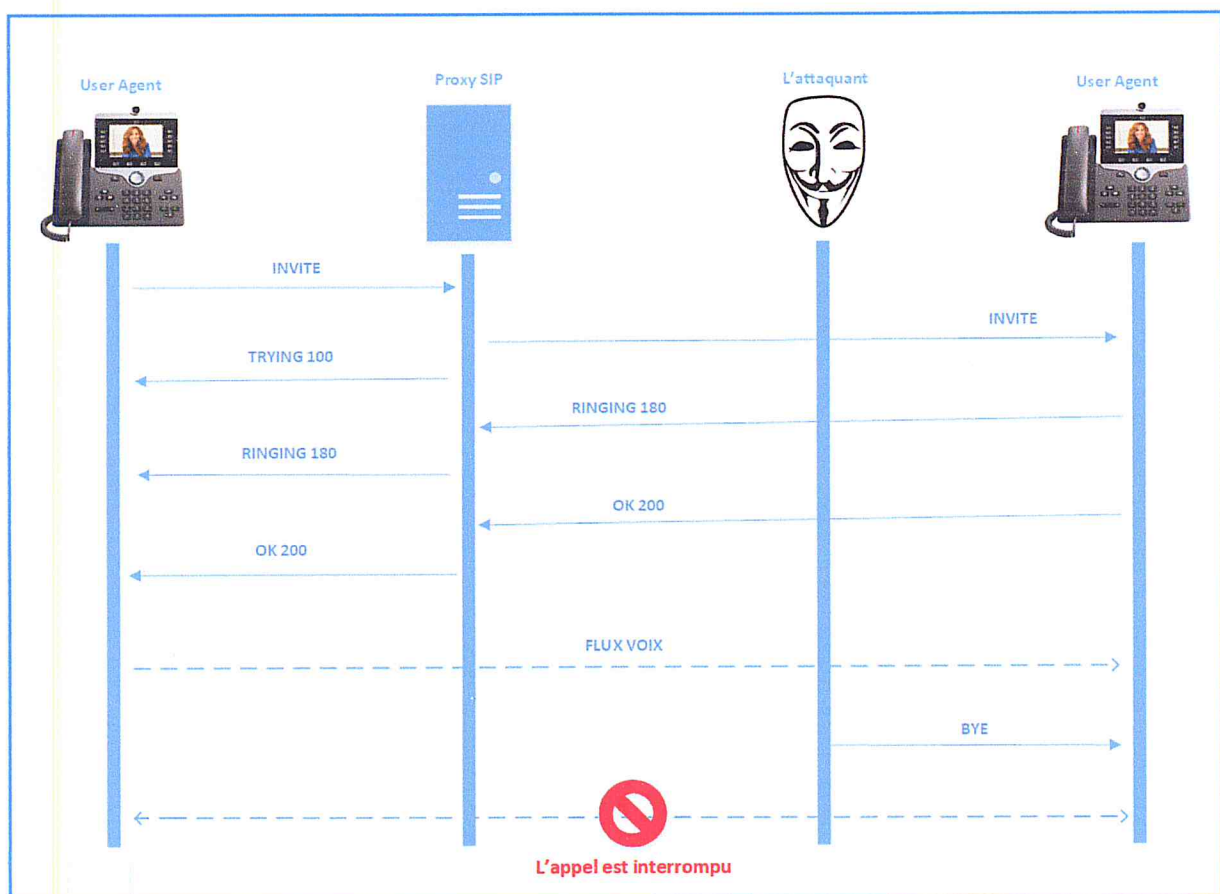


Figure 29 : Attaque par le BYE.

❖ Via REGISTER

Semblable à l'attaque par détournement d'enregistrement, un attaquant peut effectuer une attaque par déni de service en associant un agent utilisateur légitime à une adresse IP fausse ou inexistante. Lorsque les appels sont redirigés vers l'adresse IP inexistante, il n'y aura pas de réponse et l'appel échouera [14].

Pour effectuer une attaque par déni de service via un paquet REGISTER, un attaquant peut soumettre le même paquet de demande d'enregistrement mais modifier le champ Contact dans l'en-tête SIP et insérer une adresse IP fausse / inexistante.

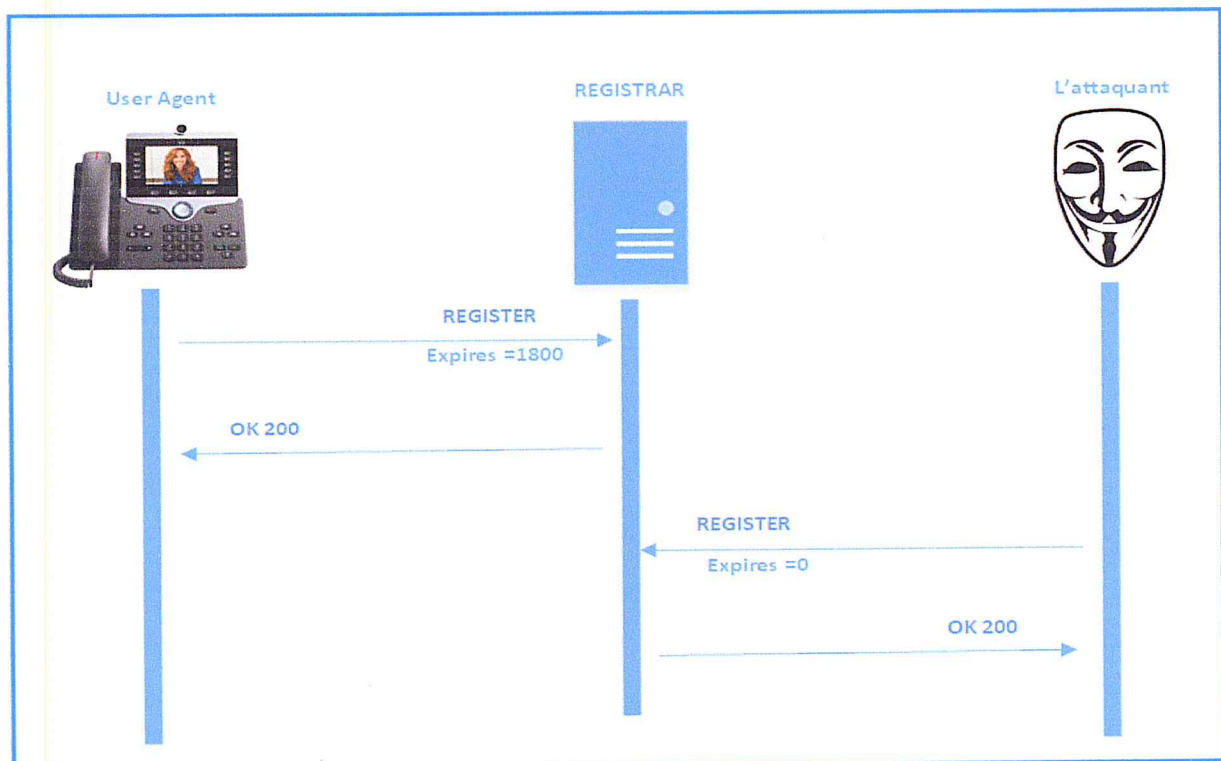


Figure 30 : Attaque sur le REGISTER.

9. SIP Fuzzing

Fuzzing est le processus consistant à soumettre des données aléatoires à un protocole ou une application afin d'en provoquer l'échec. Si le programme échoue (se bloque), des problèmes de sécurité peuvent être identifiés aux points de défaillance dans le protocole ou l'application. Le protocole SIP peut être fuzzed pour tester la robustesse de l'implémentation SIP d'un fournisseur. Par exemple, si le protocole ne peut pas se défendre contre les techniques communes de Fuzzing, la disponibilité du réseau VoIP pourrait être affectée.

10. Attaques de sécurité sur le protocole RTP

Les attaques de sécurité sur VoIP sont généralement axées sur la capture de média (audio), ce qui implique le protocole RTP. L'absence de cryptage et / ou de confidentialité permet plusieurs types d'attaques provenant d'utilisateurs non autorisés, y compris des utilisateurs anonymes non authentifiés.

RTP est vulnérable à de nombreux types d'attaques, y compris les attaques classiques, telles que l'usurpation d'identité, le piratage, le déni de service et la manipulation du trafic, ainsi que les plus récentes telles que l'écoute clandestine et l'injection vocale. Dans les sections suivantes, nous allons nous concentrer sur les attaques les plus dangereuses et les plus sévères sur RTP, Comprenant :

- Écoute passive
- Écoute active
- Déni de service

10.1. Écoute passive

Les paquets en clair de RTP peuvent être sniffés sur le réseau comme avec Telnet, FTP et HTTP. Cependant, contrairement à une telle attaque sur Telnet, la simple capture de quelques paquets RTP sur le réseau ne fournira pas à un attaquant toutes les informations sensibles qu'il souhaite. En effet, RTP transfère des flux de paquets audio, ce qui signifie qu'un attaquant doit capturer un flux entier afin de capturer une conversation. Capturer un seul paquet RTP équivaldrait à capturer la lettre S de cette phrase - vous n'auriez qu'une seule lettre et aucune information réelle. Bien que cela rende RTP espionné un peu plus fort que d'intercepter un trafic plus simple, la possibilité de capturer des flux audio RTP est toujours très possible.

➤ Utilisation de Cain et Abel pour les attaques de l'homme dans le milieu

Notre exemple utilisera Cain & Abel écrit par (*Massimiliano Montoro*) pour capturer les paquets RTP, les réassembler et les décoder en fichiers .wav. Nous commencerons par utiliser Cain & Abel pour effectuer une attaque man-in-the-middle sur l'ensemble du sous-réseau, puis utiliser son sniffer RTP pour capturer tous les paquets RTP et écouter l'audio capturé. Voici les instructions étape par étape:

1. Sélectionnez l'icône verte dans le coin supérieur gauche qui ressemble à carte d'interface réseau, comme illustré à la figure
2. La fenêtre MAC Address Scanner apparaît et énumère toutes les adresses MAC du sous-réseau local. Cliquez sur OK.

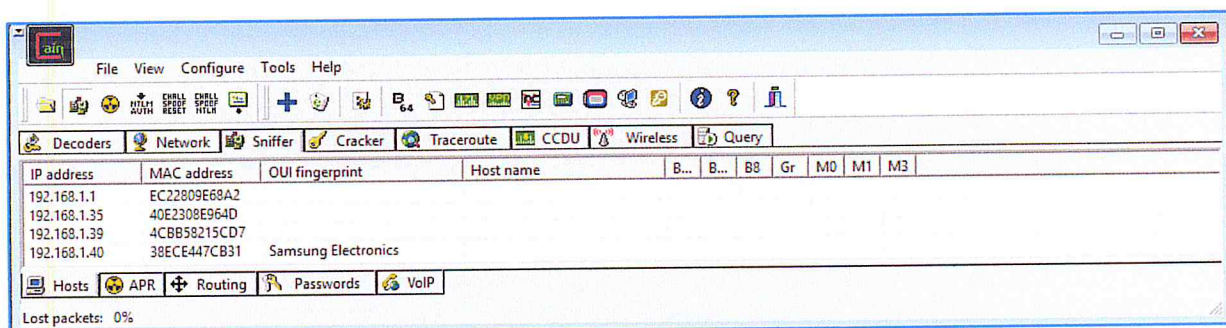


Figure 31 : résultats des Adresses MAC scanner.

3. Dans le menu ARP Poison Routing, nous choisissons la cible de notre attaque man-in-the-middle à partir de la liste des adresses IP et de leurs adresses MAC

correspondantes. La cible la plus probable sera la passerelle par défaut de votre sous-réseau. Va passer par vous d'abord avant qu'ils atteignent la passerelle réelle du sous-réseau.

- Une fois que nous avez sélectionné notre cible, qui est 192.168.1.1 dans notre exemple, nous sélectionnons les points de terminaison VoIP à partir desquels vous voulez intercepter le trafic. Nous pouvons choisir tous les points de terminaison VoIP dans le sous-réseau ou un particulier.

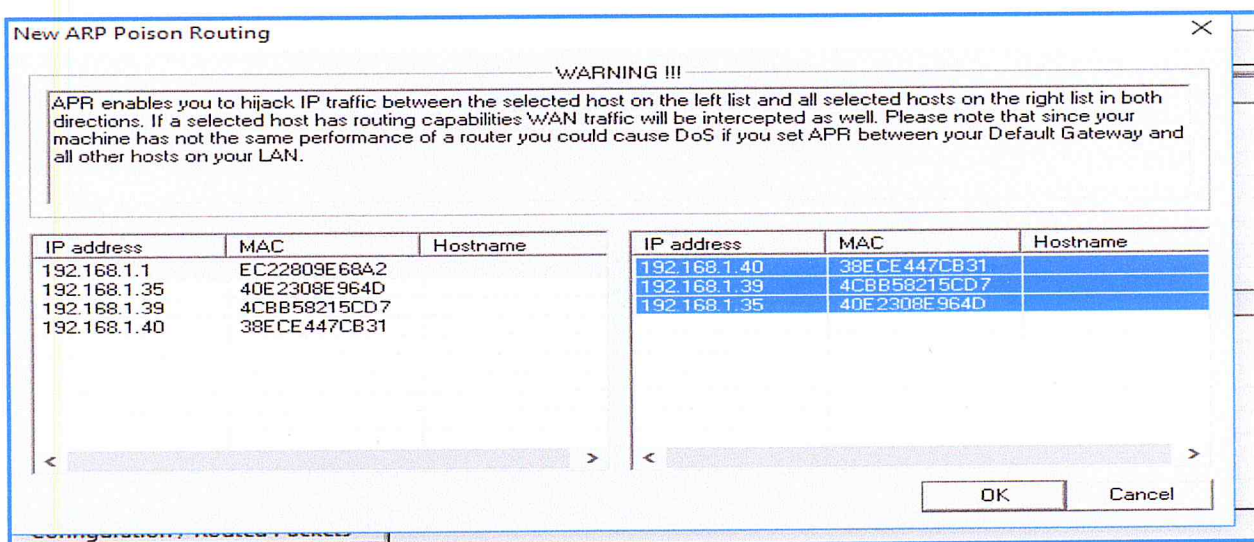


Figure 32 : les victimes de l'attaque (*Man-In-The-Middle*).

- Lorsque nous sommes revenus à l'écran principal, nous cliquons sur l'icône jaune-et-noire pour lancer l'attaque de l'homme-dans-le-milieu. Cela permettra à la tierce partie non fiable de commencer à envoyer des réponses ARP.

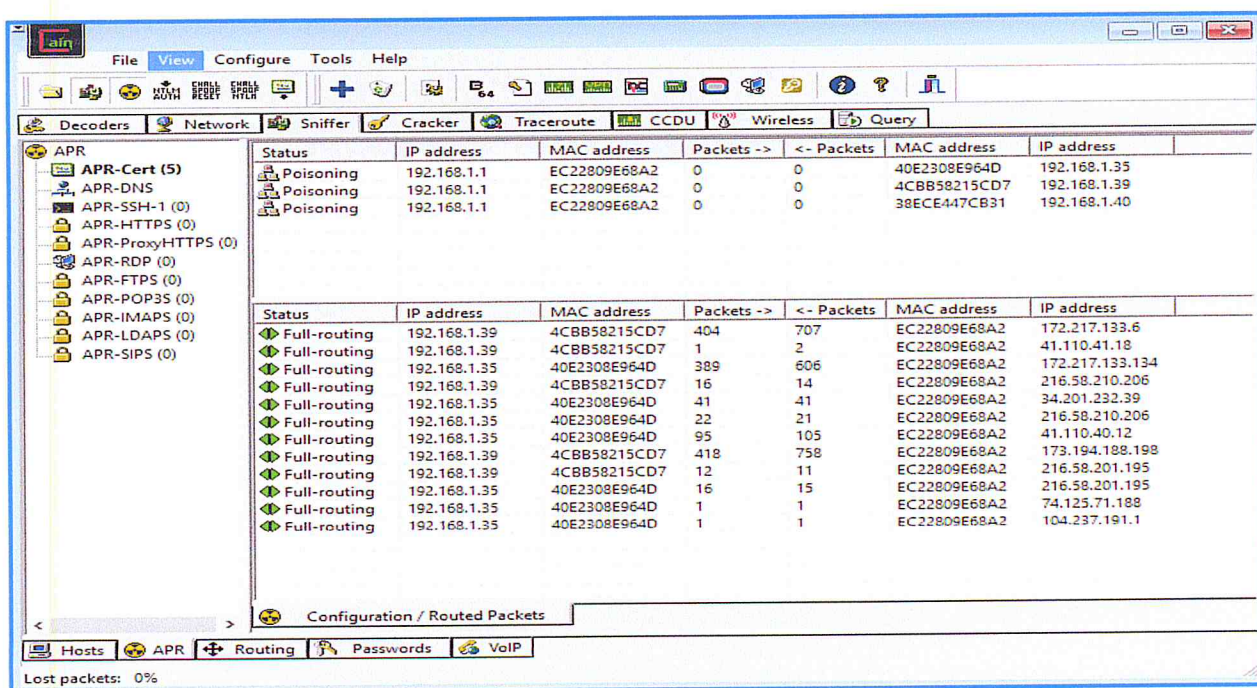


Figure 33 : lancement d'empoisonnement ARP.

6. À ce stade, tout le trafic du point d'extrémité A au point d'extrémité B passe d'abord par le tiers non approuvé, puis sur son itinéraire approprié. La tierce partie non fiable peut maintenant utiliser Cain & Abel, Wireshark ou un programme similaire pour capturer les paquets RTP et les réassembler dans un format audio commun.
7. Nous avons sélectionné VoIP à partir des onglets en bas, comme indiqué dans la figure. Si une communication VoIP a eu lieu sur le réseau à l'aide des flux multimédia RTP, Cain & Abel sauvegarde automatiquement les paquets RTP, les réassemble et les enregistre au format .wav. Comme le montre la figure, Cain & Abel a capturé quelques conversations téléphoniques sur le réseau.

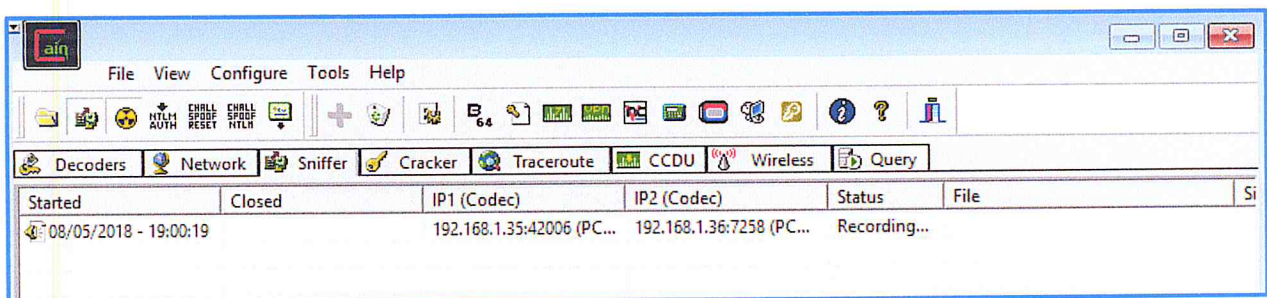


Figure 34 : capture de communication VoIP via RTP.

8. À ce stade, tout le trafic du point de terminaison A vers le point de terminaison B passe d'abord par le tiers non approuvé, puis sur son itinéraire approprié. La tierce partie non fiable peut maintenant utiliser Cain & Abel, Wireshark ou un programme similaire pour capturer les paquets RTP et les réassembler dans un format audio commun.
9. Utiliser Wireshark pour réassembler les paquets RTP et les enregistrer dans un fichier .wav, pour l'attaque man-in-the-middle

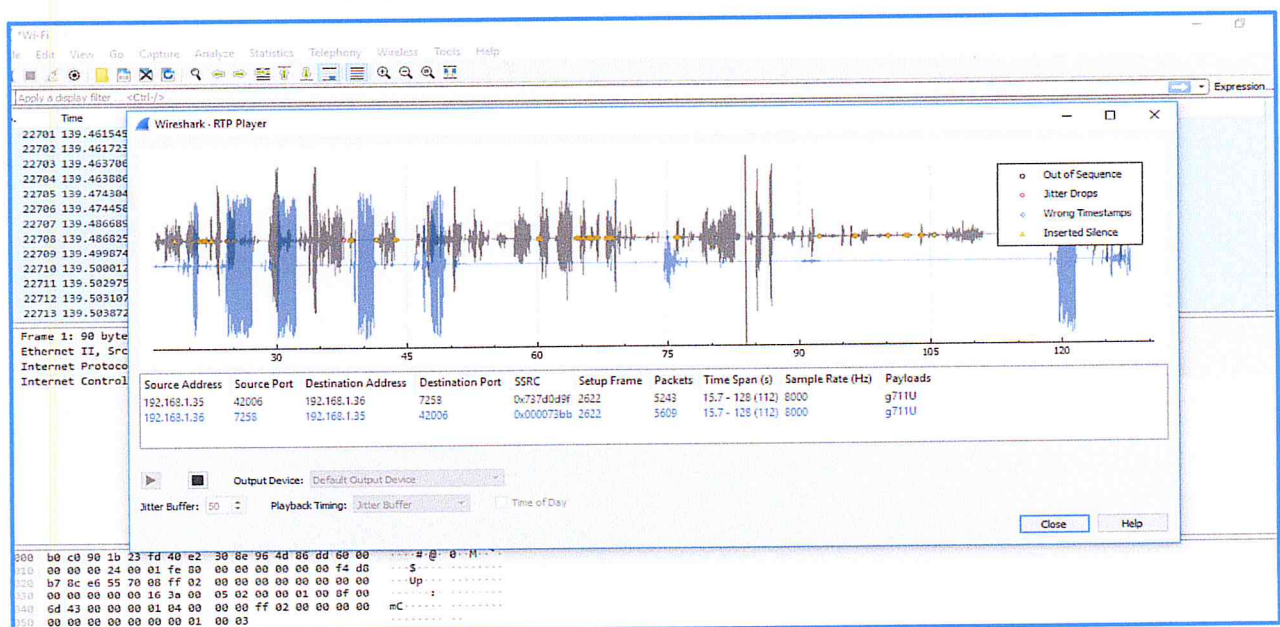


Figure 35 : Communication VoIP capturée par des paquets RTP via Wireshark.

11. Vulnérabilité spécifique au fournisseur de Téléphones IP

Les téléphones VoIP **Cisco**, **Avaya** et **Polycom** sont probablement les téléphones les plus populaires dans les réseaux d'entreprise. Peu importe le fournisseur, cependant, n'importe quel type de téléphone est livré avec des problèmes de sécurité. Par exemple, un attaquant peut compromettre le fichier de configuration du téléphone ou en télécharger un malveillant. Heureusement, les informations sur le nom d'utilisateur et le mot de passe ne sont généralement pas stockées dans le fichier de configuration du téléphone, ce qui peut avoir un impact sur le piratage si le fichier est compromis.

Est quelque peu atténué. Au lieu de cela, les risques de vulnérabilités d'un téléphone IP sont des attaques d'énumération générales et des attaques par déni de service (DoS). Les sections suivantes traitent de ces vulnérabilités du téléphone fixe VoIP:

- Compromettre le fichier de configuration du téléphone
- Téléchargement d'un fichier de configuration illicite
- Exploiter les faiblesses de SNMP

11.1. Compromettre le fichier de configuration du téléphone

La plupart des téléphones IP reçoivent des fichiers importants, tels que des images de démarrage ou des fichiers de configuration, sur le réseau. Les appareils VoIP, y compris ceux de **Cisco** et d'**Avaya**, transfèrent souvent ces fichiers en utilisant le protocole TFTP, mais certains utilisent également le protocole HTTP. De toute façon, un attaquant peut obtenir des copies de ces fichiers assez facilement.

TFTP et HTTP sont des protocoles en clair qui sont souvent utilisés sans aucune authentification. Un attaquant qui a obtenu de tels fichiers à accès aux paramètres et aux options du téléphone [11].

Pour obtenir le fichier de configuration d'un téléphone, un attaquant devrait effectuer ces étapes:

1. Connectez-vous au réseau VoIP.
2. Localisez le serveur TFTP utilisé pour télécharger des images / fichiers de configuration sur des téléphones fixes.
3. Recherchez le serveur TFTP en sniffant le réseau pour l'adresse source à partir de laquelle les connexions TFTP arrivent. Une recherche rapide du fichier 46xxsettings.txt aidera à localiser les paquets avec le serveur TFTP source sur un réseau **Avaya**. Pour cet exemple, un attaquant devrait supposer.
4. Entrez ce qui suit à l'invite de commande Windows: « **TFTP 172.16.1.88 GET 46xxsettings.txt** ».

Le Tableau 12 répertorie les services non sécurisés couramment utilisés, les recommandations d'atténuation de la vulnérabilité et le meilleur outil open source pour tester le problème.



services	Recommandation	outil
FTP	Désactiver les protocoles de gestion de texte en clair en faveur d'une communication cryptée avec authentification à deux facteurs	Nmap Nessus
telnet	Implémenter SSH avec authentification à deux facteurs	Nmap Nessus
OpenSSH obsolète	Assurez-vous que tous les serveurs SSH sont à jour et entièrement patchés	Nmap Nessus
OpenSSL obsolète	Assurez-vous que les bibliothèques SSL sont à jour et entièrement patchées	Nmap, Nessus, Nikto
Version Apache obsolète	Assurez-vous que tous les serveurs Web sont à jour et entièrement patchés	Nmap, Nessus, Nikto
Certificats	Tous les certificats SSL doivent être à jour. Assurez-vous que la certification SSL n'est pas auto-signée et concerne l'hôte correct (n'utilisez pas le certificat par défaut sur tous les points de terminaison VoIP)	Nmap, Nessus, Nikto
SNMP	Activer SNMPv3 avec des chaînes de communauté complexes et uniques	GetIf, Nessus
Logging	Activer les options de journalisation sur les passerelles média	N/A

Tableau 12 :Recommandations d'atténuation et outils de test.

Conclusion

La sécurité dans un réseau VoIP est essentielle en raison des vulnérabilités spécifiques à l'infrastructure réseau et de l'architecture de l'application. Bien que de simples extensions de la sécurité du réseau de données puissent contribuer à atténuer ces vulnérabilités.

Dans ce chapitre, nous avons présentés l'architecture réseau du Catering, ensuite en a mis le point sur les vulnérabilités les plus importantes, dans les protocoles les services médias, et les service support.

En va voir comment procéder pour faire faces a ces vulnérabilités, tout en préconisant un certain nombre de mesures de sécurités qui doit être prises en compte, dans le but de garantir la qualité de service du réseau ainsi que sa sécurité.

CHAPITRE 4

DEPLOIEMENT ET MECANISME DE SECURITE

1. Introduction

L'objectif du présent chapitre est d'illustrer au mieux les différentes vulnérabilités d'un réseau VoIP/SIP à l'intérieur de l'entreprise. Nous commençons nos tests avec une plateforme SIP non sécurisée, basée sur le serveur de téléphonie CUCM (*Cisco Unified Communications Manager*). Vu que l'infrastructure sera non sécurisée, cela va nous permettre de réaliser les attaques décrites dans le chapitre précédent. Et par la suite, le but est de sécuriser le réseau afin de démontrer la fiabilité des mécanismes de défenses qui ont été mis en place.

2. Environnement de travail

Dans cette section, nous présentons l'environnement matériel et logiciel utiles pour la conception et la mise en place de notre architecture.

2.1. Environnement Matériel

Machine 1: HP ElitBook 8570p, Processeur Intel® Core™ i7 CPU @2.20GHz avec 16Go de RAM.

Machine 2: Lenovo, Processeur Intel® Core™ i3 CPU @2.0GHz, avec 4Go de RAM.

2.2. Environnement logiciel

Le tableau, présente les principaux logiciels utilisés pour la réalisation du notre projet :

Nom de logiciel	Description
 GNS3	GNS3 est un logiciel utilisé pour simuler différents périphériques virtuels et les dispositifs réels comme les routeurs, commutateurs. Il utilise Dynamips qui est un logiciel d'émulation pour simuler des périphériques virtuels. L'interface est graphique, elle est simple et agréable d'utilisation [15].
 VMware	VMware Workstation est un logiciel de machine virtuelle utilisé par les ordinateurs x86 et x86-64 pour exécuter plusieurs systèmes d'exploitation sur un seul ordinateur hôte physique. Chaque machine virtuelle peut exécuter une seule instance de n'importe quel système d'exploitation (Microsoft, Linux, etc.) simultanément [16].
 Cisco IP Communicator	Cisco IP Communicator est une application de logiciel de téléphonie sur PC Windows qui vous permet d'utiliser votre ordinateur personnel pour effectuer des appels vocaux et vidéo de qualité supérieure. Offrant les dernières technologies de communication IP, il est facile à acquérir, déployer et utiliser [17].
 Wireshark	Wireshark, dans son sens le plus fondamental, est un outil pour comprendre les données que vous capturez à partir d'un réseau. Les données capturées sont interprétées et présentées sous forme de paquet individuel pour l'analyse, le tout dans Wireshark, les paquets sont les morceaux de données en streaming sur un réseau [18].
 NMAP	Abréviation de Network Mapper, un utilitaire open source permettant d'explorer des réseaux ou de faire un audit de sécurité. Il est disponible gratuitement et a été développé pour scanner rapidement de grands réseaux. Il fonctionne bien dans cet environnement ainsi qu'avec des hôtes uniques [19].
 Call Manager	Cisco Unified Communications (UC) est un système de communication basé sur IP intégrant des produits et des applications voix, vidéo, données et mobilité. Il permet des communications plus efficaces et sécurisées et peut transformer la façon dont nous communiquons [20].

Tableau 13 :Les Logiciels utilisés pour la simulation.

3. Architecture Réseau Déployée

La première étape dans cette partie du projet est de mettre en place le réseau de test SIP/VoIP.

Notre architecture réseau réalisée avec GNS3, comporte le serveur de téléphonie Cisco Unified Communications Manager, un attaquant, des Softphone Cisco IP Communicator et un contrôleur du domaine Windows Server 2012R2. Nous avons utilisé des routeurs et des commutateurs Cisco, L'architecture est présentée dans la figure suivante:

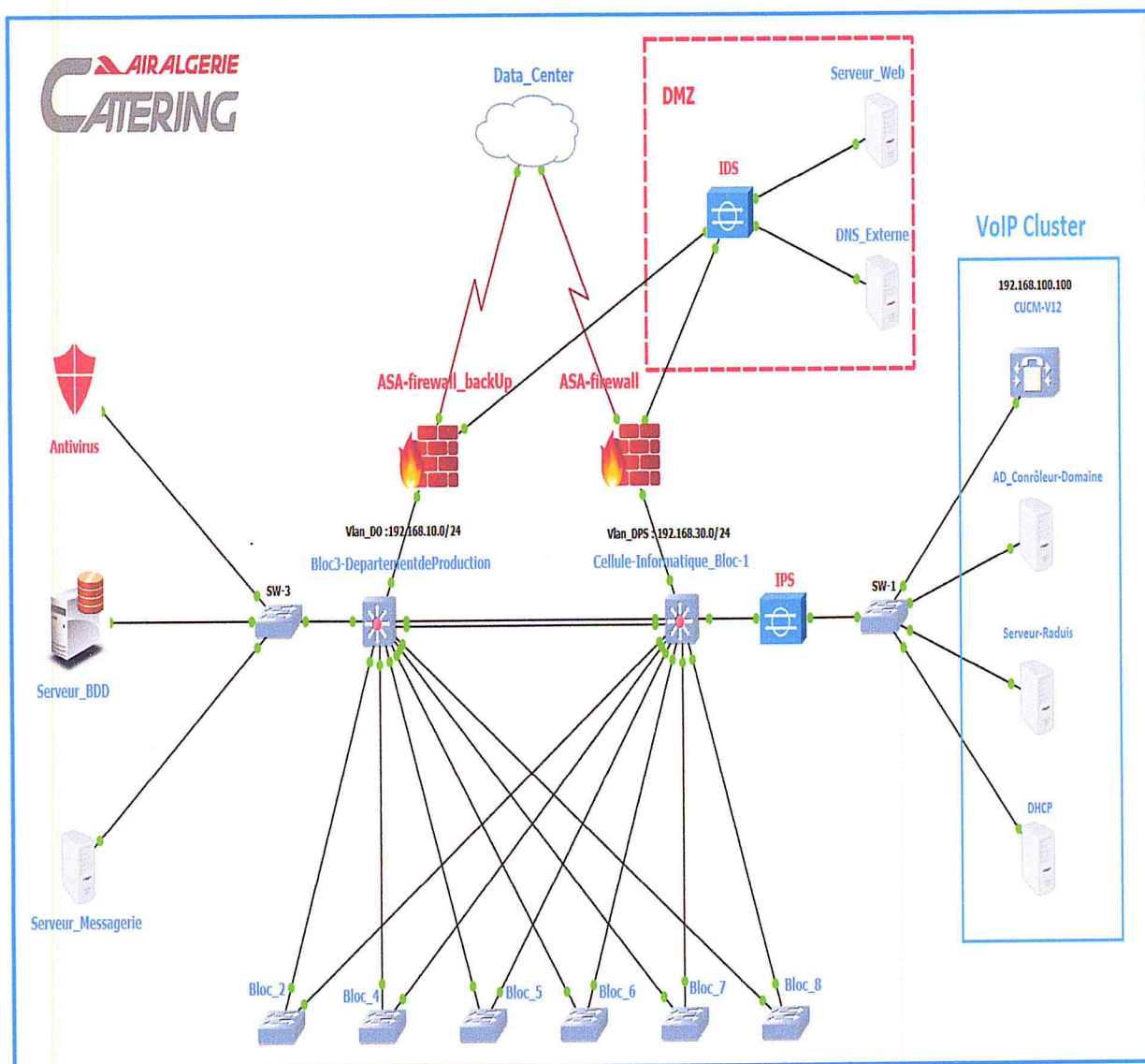


Figure 36 :Architecture Réseaux VoIP Déployer.

3.1. Adressage et réseaux virtuels

Le réseau d'air Algérie Catering est segmenté en plusieurs réseaux virtuels et ce afin de minimiser les broadcasts diffusés dans le réseau et de bénéficier de la bande passante maximale Pour assurer la qualité de service de la voix sur IP. Le tableau 14 et la figure 37 liste les différents réseaux virtuels et leurs adresses constituant le réseau global.

Les VLANs Existants	Les Adresses
Vlan_DC	192.168.20.0/24
Vlan_DPS	192.168.30.0/24
Vlan_DO	192.168.10.0/24
Vlan_DRH	192.168.40.0/24
Vlan_DFC	192.168.50.0/24
Vlan_CM	192.168.60.0/24
Vlan_VoIP	192.168.100.0/24

Tableau 14 :Liste des VLANs.

```
SW-BLOC3#vlan database
SW-BLOC3(vlan)#vlan 10 name DR-OPERATION
VLAN 10 added:
    Name: DR-OPERATION
SW-BLOC3(vlan)#
SW-BLOC3(vlan)#vlan 20 name DR-COMMERCIALE
VLAN 20 added:
    Name: DR-COMMERCIALE
SW-BLOC3(vlan)#
SW-BLOC3(vlan)#vlan 30 name DR-PLANIFICATION&STRATIGIE
VLAN 30 added:
    Name: DR-PLANIFICATION&STRATIGIE
SW-BLOC3(vlan)#
SW-BLOC3(vlan)#vlan 40 name DR-RESSOURCE-HUMMAINES
VLAN 40 added:
    Name: DR-RESSOURCE-HUMMAINES
SW-BLOC3(vlan)#
SW-BLOC3(vlan)#vlan 50 name CELLULE-MANAGEMENT
VLAN 50 added:
    Name: CELLULE-MANAGEMENT
SW-BLOC3(vlan)#
SW-BLOC3(vlan)#vlan 60 name DR-FINANCES-COMPTABILITE
VLAN 60 added:
    Name: DR-FINANCES-COMPTABILITE
SW-BLOC3(vlan)#
SW-BLOC3(vlan)#vlan 100 name VOICE
VLAN 100 added:
    Name: VOICE
SW-BLOC3(vlan)#
```

Figure 37: Création des Vlan

3.2. Configuration des équipements

La configuration des équipements réseau sont données respectivement dans les figures 38, 39, 40 et 41.

La sécurité des ports est le moyen par lequel nous pouvons empêcher les périphériques réseau d'utiliser un port sur notre commutateur. Au niveau du port, nous pouvons spécifier certaines adresses MAC.

La sécurité du port est activée avec la commande switchport port-security. Cette commande peut être configurée uniquement sur une interface qui a été définie comme un switchport.

```
SW1-LAB(config)#int gi 0/1
SW1-LAB(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

SW1-LAB(config-if)#switchport access vlan 5
SW1-LAB(config-if)#switchport port-security max 5
SW1-LAB(config-if)#switchport port-security aging type inactivity
SW1-LAB(config-if)#switchport port-security aging time 5
SW1-LAB(config-if)#switchport port-security violation restrict
SW1-LAB(config-if)#switchport port-security
SW1-LAB(config-if)#ip verify source
SW1-LAB(config-if)#spanning-tree portfast
SW1-LAB(config-if)#exit
SW1-LAB(config)#
```

Figure 38 :Activation de la sécurité des ports.

Le DHCP Snooping est une technologie à implémenter sur un commutateur et qui permet d'empêcher de brancher un serveur DHCP indésirable sur un réseau, Voici la procédure à suivre pour activer la technologie DHCP Snooping sur un commutateur Cisco [21].

```
SW1-LAB(config-if)#
SW1-LAB(config-if)#exit
SW1-LAB(config)#ip dhcp snooping vlan 5
SW1-LAB(config)#int gi 0/3
SW1-LAB(config-if)#ip dhcp snooping trust
SW1-LAB(config-if)#exit
SW1-LAB(config)#
SW1-LAB(config)#int gi0/1
SW1-LAB(config-if)#ip dhcp snooping limit rate 10
SW1-LAB(config-if)#
SW1-LAB(config-if)#
```

Figure 39 :Mécanisme de prévention contre les serveurs DHCP indésirable.

Si la configuration montre un port à activer, mais que le logiciel sur le commutateur détecte une situation d'erreur sur le port, le logiciel arrête ce port. En d'autres termes, le port est automatiquement désactivé par le logiciel de système d'exploitation du commutateur en raison d'une condition d'erreur qui est produite sur le port [22].


```

SW1-LAB(config)#
SW1-LAB(config)#errdisable recovery cause psecure-violation
SW1-LAB(config)#! recover from port-security violation error
SW1-LAB(config)#errdisable recovery cause security-violation
SW1-LAB(config)#! recover from 802.1x violation error
SW1-LAB(config)#errdisable recovery interval 120
SW1-LAB(config)#

```

Figure 40 :Port désactivé par erreur.

Nous devons installer le serveur SIP/VoIP, nous choisissons le serveur de téléphonie propriétaire Cisco, le « Cisco Unified Communications Manager v12 » qui s'exécute sur une machine RedHat Enterprise Linux 5. « CUCM » est un serveur de téléphonie compatible avec la plupart des protocoles de signalisation (H.323, SIP, SCCP, etc.), il propose une interface web très évoluée pour le paramétrage du système et il rassemble plusieurs services téléphoniques.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

Cisco Unified CM Administration

Username
Mezaourou-Billel

Password
.....

Login Reset

Copyright © 1999 - 2017 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Figure 41 :Interface Web de CUCM.

Après avoir installé CUCM, nous devons établir une communication VoIP. Maintenant, nous installons le Softphone CIPC sur les stations Windows et procédons à les configurer. Comme le montre la figure 42.

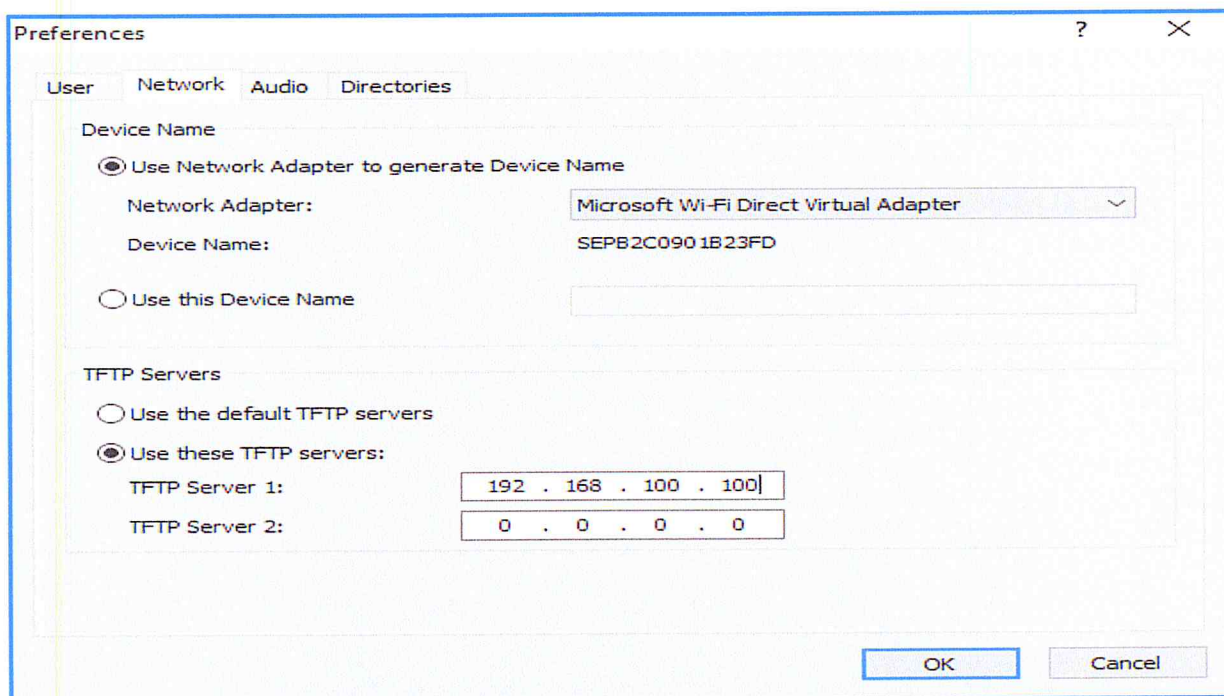


Figure 42 :Paramétrage du CIPC.

Après l'ajout des deux CIPC et leurs configurations, nous allons les redémarrer, pour qu'ils s'enregistrent au près du notre serveur Cisco Unified CM. L'enregistrement est fait, comme est Indiqué dans la figure 43.

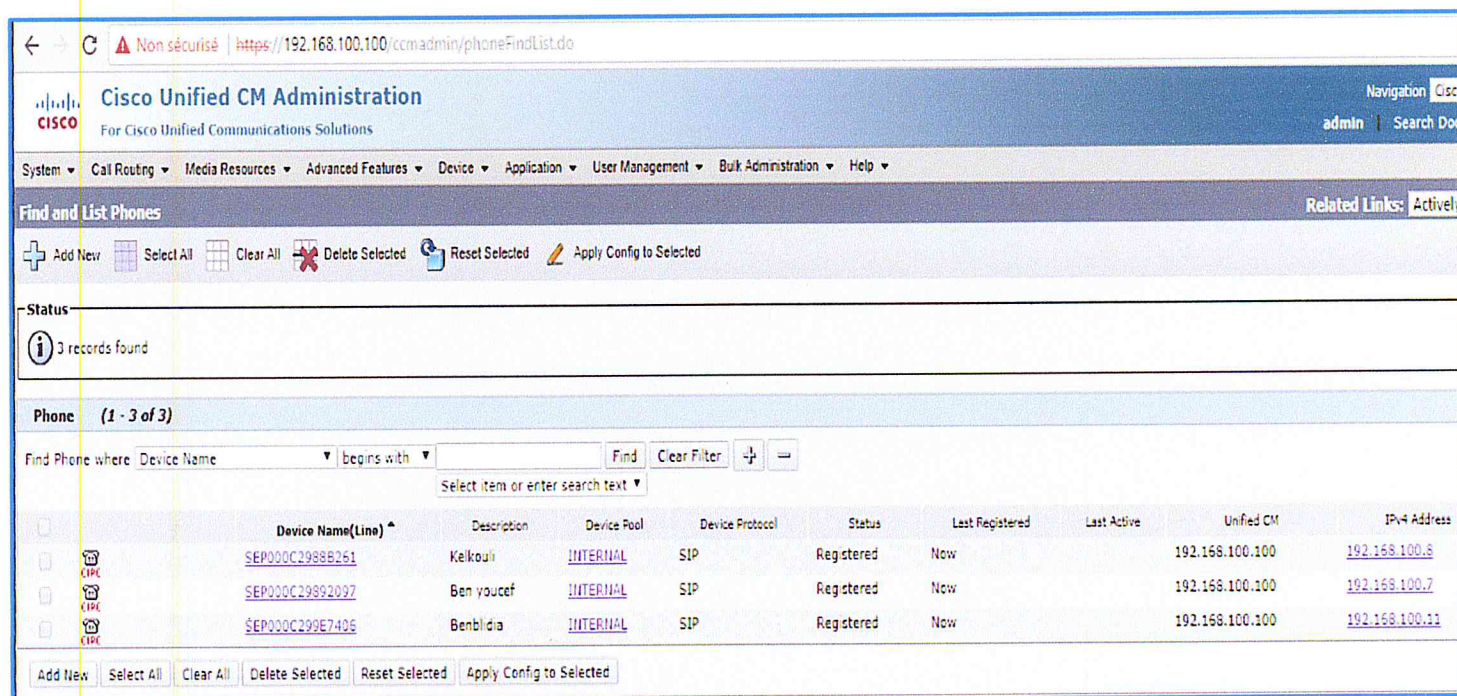


Figure 43 :Enregistrement des CIPCs.

Maintenant, nous pouvons établir une communication téléphonique entre CIPC1 et CIPC2



Figure 44 :Etablissement d'une conversation entre les CIPCs.

4. Sécurité de call manager

Le call manager, présente un grand nombre de vulnérabilités qui peuvent être exploitées par un attaquant pour nuire à la sécurité de notre système VoIP, telle que la configuration par défaut des téléphones IP qui est à la base des attaques ARP Spoofing, attaque Google, écoute clandestine, etc. Alors, nous devons modifier les configurations relatives aux téléphones IP et au CUCM afin de les rendre moins vulnérables côté sécurité.

4.1. Utilisation du protocole TLS pour la signalisation

Puisque le protocole SIP présente une importante faille de sécurité, très exploitée par les attaquants, est que les messages transitent entre le téléphone IP et le CUCM en texte clair.

Nous devons alors agir sur la configuration du téléphone IP pour qu'il utilise le protocole TLS à la place du protocole SIP, voir la figure 45.

Phone Security Profile Information	
Product Type:	Cisco IP Communicator
Device Protocol:	SIP
Name*	Cisco IP Communicator - Standard SIP Secure Profile
Description	Cisco IP Communicator - Standard SIP Secure Profile
Nonce Validity Time*	600
Device Security Mode	Encrypted
Transport Type*	TLS
☒ Enable Digest Authentication	
☒ TFTP Encrypted Config	
☐ Exclude Digest Credentials in Configuration File	

Figure 45 :Configuration du TLS dans le Profil de Sécurité du CIPC.

4.2. Implémentation du protocole SRTP

L'attaque d'écoute clandestine n'aura jamais eu lieu, si le trafic média transitant entre les deux User-agents était chiffré. Pour sécuriser le trafic RTP, nous devons utiliser le Secure RTP, qui chiffrera la conversation et ainsi devient difficile à l'attaquant de convertir la communication et de l'écouter.

4.3. Configuration des paramètres des téléphones IP

La configuration par défaut du téléphone IP, le laisse accepter directement les paquets GARP qui sont à l'origine de l'attaque ARP Spoofing, et cette même configuration permet l'accès Web au téléphone IP ce qui est à la base de l'attaque de reconnaissance passive.

Pour remédier à :

- ARP Spoofing : Nous devons désactiver l'acceptation implicite des paquets GARP par les téléphones Cisco IP Communicator,
- Attaque Google : Nous devons désactiver l'accès Web aux téléphones IP.

Nous configurons les paramètres des téléphones IP, d'une manière sécurisée afin de rendre un peu plus difficile à l'attaquant de s'introduire dans notre système VoIP. La nouvelle configuration des téléphones Cisco IP Communicator est donnée dans la figure 46.

RTCP*	Enabled
Advertise G.722 and iSAC Codecs*	Use System Default
Video Calling*	Enabled
Wifi*	Disabled
PC Port *	Disabled
Span to PC Port*	Disabled
PC Voice VLAN Access*	Disabled
PC Port Remote Configuration*	Disabled
Switch Port Remote Configuration*	Disabled
802.1x Authentication*	User Controlled
FIPS Mode*	Disabled
80-bit SRTP*	Enabled

Figure 46 :La nouvelle Configuration des CIPCs.

5. Les éléments de sécurité de l'infrastructure

L'infrastructure doit bien sûr elle-même se protéger ce qui renforce la sécurité globale et la disponibilité du système. Chaque équipement, doit être sécurisé pour éviter une prise de contrôle malveillante. Ceci est assuré par la protection des accès aux équipements en mode administrateur (mots de passe forts, liste restreinte d'adresses autorisées, chiffrement SSL des connexions, authentification RADIUS des utilisateurs).

L'infrastructure réseau apporte également un certain nombre de fonctions qui doivent être activées par configuration pour renforcer la sécurité des communications:

Les fonctionnalités de pare-feu ou de routeur filtrant, de détection et de prévention d'intrusion doivent être réparties sur le réseau. On propose d'ajouter des équipements de type ASA (*Adaptive Security Appliance*) [23].

5.1. Gestion de l'accès à l'infrastructure

Nous cherchons ici à construire une infrastructure qui permet d'assurer une séparation des flux tout en mutualisant cette dernière.

L'isolation des flux voix et données sur la même infrastructure grâce aux VLANs (réseaux locaux) ou aux technologies de virtualisation de l'infrastructure (réseaux locaux et étendus).

Nous apportons donc le support du Vlan Voix avec plusieurs mécanismes de contrôle d'accès :

- Les protocoles LLDP-MED et CDP permettent de réaliser l'auto-configuration mais également de contrôler l'entrée d'un périphérique dans le Vlan Voix, ainsi le commutateur n'autorisera l'entrée dans le Vlan Voix qu'à condition qu'un terminal voix de type « IP Phone » soit reconnu sur le port.
- La gestion d'accès au réseau par des technologies d'authentification répondant au standard IEEE 802.1x, à la fois pour les téléphones mais aussi pour les postes informatiques connectés sur ces téléphones (qui hébergent un micro-commutateur).

5.1.1 Fonction dans les commutateurs

La mise en place des mécanismes permettant de parer des attaques de type :

- Saturation de la table d'adresses MAC d'un commutateur visant à le transformer en un simple répéteur (hub) de façon à récupérer des flux sur des interfaces où ils ne sont théoriquement pas attendus. Appelée « MAC Flooding », cette attaque est parée par l'activation de la fonctionnalité de « port Security ».
- Ecoute et capture de trafic basé sur le vol d'adresses IP obtenues par émission de trames GARP (gratuitous ARP). Appelées « ARP Spoofing », ces attaques sont contrées par deux techniques au choix :
 - ✓ L'activation de la fonction DAI (Dynamic ARP Inspection) sur les commutateurs.
 - ✓ L'activation de rejet des trames GARP sur les téléphones.
- Déni de service sur les serveurs DHCP soit par introduction d'un second serveur DHCP dans le réseau ou par saturation des plages d'adresses par inondation de requêtes factices. On se protège contre ces attaques grâce à deux techniques au choix :
 - ✓ Activation de la fonction « DHCP Snooping » sur les commutateurs.
 - ✓ Limitation (rate limiting) du nombre de requêtes par seconde émises vers un port du commutateur.
- Fonction de renforcement d'accès au réseau : Support de 802.1X sur le Vlan Voix ou Données
- Port Security permettant de limiter le nombre d'adresses MAC par port détectées.

5.1.2. Serveurs de traitement des communications (CUCM)

Les serveurs de traitement des communications (CUCM) offrent une panoplie de services permettant de déployer un environnement de communications unifiées sécurisé. On utilise :

- Chiffrement et authentification de la signalisation (SIP/TLS ou IPSEC).
- Distribution dynamique des clés de chiffrement et authentification pour que les terminaux et les serveurs puissent générer un flux Média chiffré (SRTP)
- Intégration dans la PKI de l'entreprise avec des fonctionnalités d'automatisation de distribution des certificats aux terminaux.
- Mécanismes de classes de restrictions d'appels (voix/vidéo) permettant d'éviter les usages abusifs du système de communications.
- Administration multi-niveaux et délégation avec gestion des droits et stockage des mots de passe avec mécanismes de sécurité forts.
- Télédistribution des mises à jour de microcodes signées et chiffrées
- Télédistribution des fichiers de configuration signés et chiffrés
- Administration sécurisée : SSH / SFTP / SNMPv3 / HTTPS

5.1.3. Flux signalisation et média chiffrés

Dans le cadre d'une communication entre deux équipements VoIP, la partie confidentialité avec l'encryption de la signalisation et des flux RTP (SRTP) est souvent un challenge pour les équipements de filtrage.

Cela implique une très forte intégration entre l'ASA et les CUCM avec entre autre une intégration dans la CTL (*Certificat Trusted List*) de l'ASA.

L'ASA ouvrira dynamiquement les ports RTP en fonction de ce qui sera négocié par la signalisation, cela évite ainsi d'autoriser statiquement un range de port RTP.

Cette fonction permettra aussi d'appliquer des fonctions de translation (NAT) et bien sur une analyse et un filtrage approfondie des messages de la signalisation.

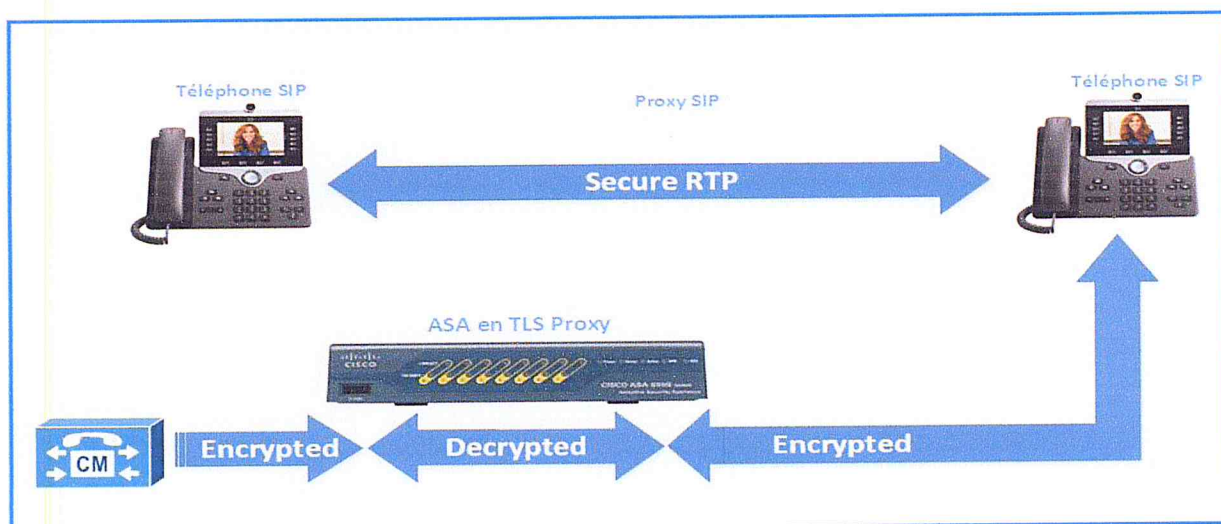


Figure 47 :Filtrage de La Voix encryptée.

5.1.4. Implémentation du Cisco ASA Firewall

L'ASA relève ces défis en faisant évoluer la technologie pare-feu éprouvée du PIX, tout en intégrant des fonctions de pare-feu à inspection applicative avancée (plus de 30 protocoles supportés), ainsi que des fonctions de sécurisation des communications unifiées uniques. Flexibilité de déploiement, haute disponibilité, haute performance [24].

En ce qui concerne la fonction de pare-feu hébergée par l'ASA elle supporte :

- L'inspection des protocoles de signalisation : SIP et H.323
- L'écoulement du trafic inspecté sans ralentissement
- La qualité de service (QoS)
- La mise en œuvre d'un système redondant
- Joue le rôle d'un IDS

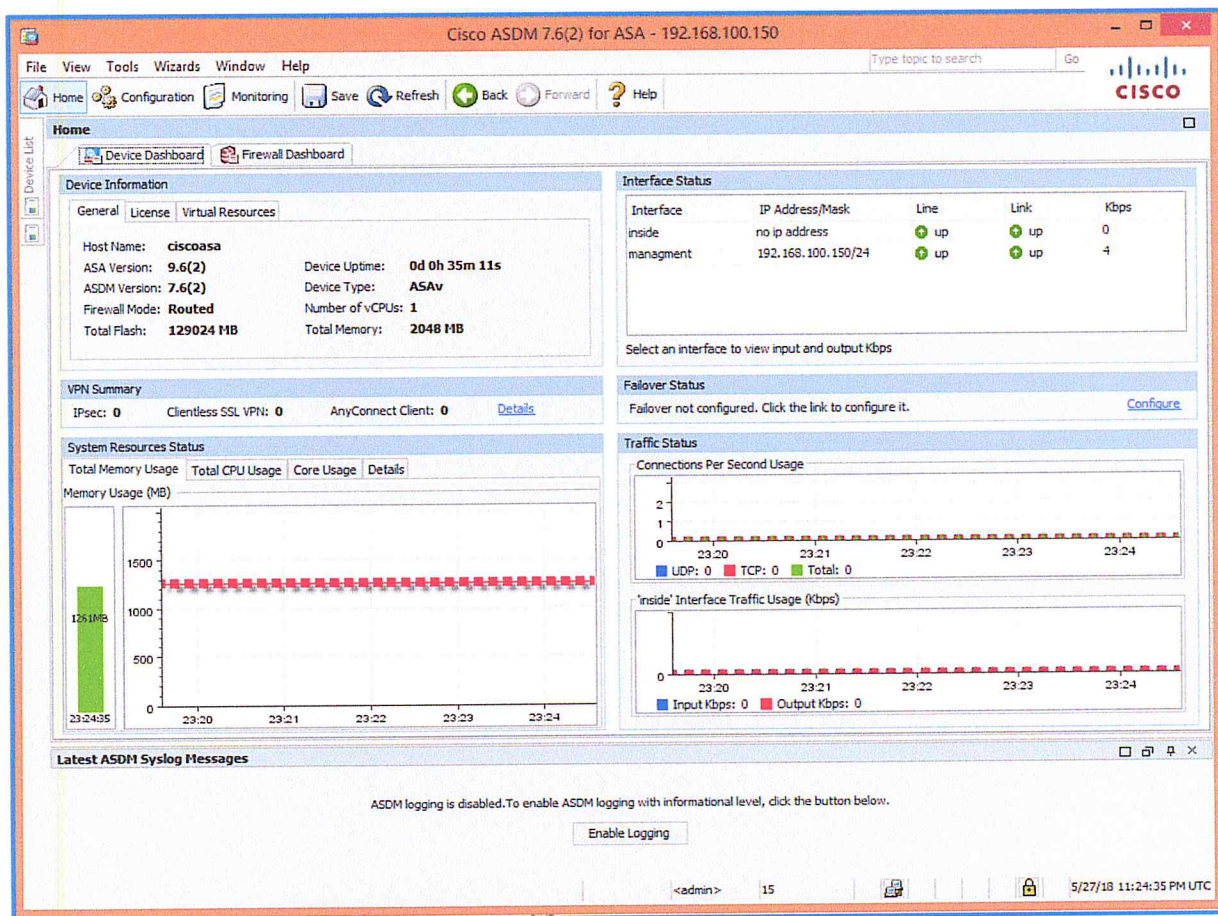


Figure 48 : Interface Web de Firewall ASA.

```
ciscoasa# show ip
System IP Addresses:
Interface      Name      IP address      Subnet mask      Method
GigabitEthernet0/0    inside    192.168.200.200  255.255.255.0    manual
GigabitEthernet0/2    outside  10.1.1.1        255.255.255.0    manual
Management0/0        managment 192.168.100.150  255.255.255.0    CONFIG
```

Figure 49 : Commande "Show ip" dans Firewall ASA.

Comme nous avons dit dans des sections précédentes, que si nous voulons sécuriser notre Infrastructure réseau, nous devons mettre en place un système de supervision tel qu'un serveur Syslog ou un système de détection d'intrusion (IDS).

Le point fort du Cisco ASA est qu'il peut jouer le rôle d'un IDS, pour ce faire nous devons le Configurer pour qu'il nous alerte en cas d'une attaque ou même pour un niveau de notification Informationnel, il suffira juste de taper les commandes suivantes (voir figure 50) :

```
ciscoasa(config)#ip audit info action alarm
ciscoasa(config)#ip audit attack action alarm
```

Figure 50 :Configuration L'IDS dans ASA

5. Surveillance de la qualité de service

Grâce à la surveillance de la qualité de service (QoS), les performances des lignes de données sont surveillées à l'aide de paramètres tels que la **latence**, la **perte de paquets** et la **gigue**. La surveillance de la qualité de service peut se faire en interne, c'est-à-dire à l'intérieur d'un grand bâtiment (la société LAN).

```
CATERING-SW3650(config)#int range gil/0/23-24
CATERING-SW3650(config-if-range)#auto qos voip cisco-phone
CATERING-SW3650(config-if-range)#do sh run int gil/0/23
Building configuration...

Current configuration : 278 bytes
!
interface GigabitEthernet1/0/23
 switchport access vlan 20
 switchport voice vlan 100
 trust device cisco-phone
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

Figure 51 : Paramétrage de la qualité de service

Même avec les mesure de sécurité implémenté les tests montre que la voix bénéficie d'une bande passante suffisante pour des appels de très bonne qualité.

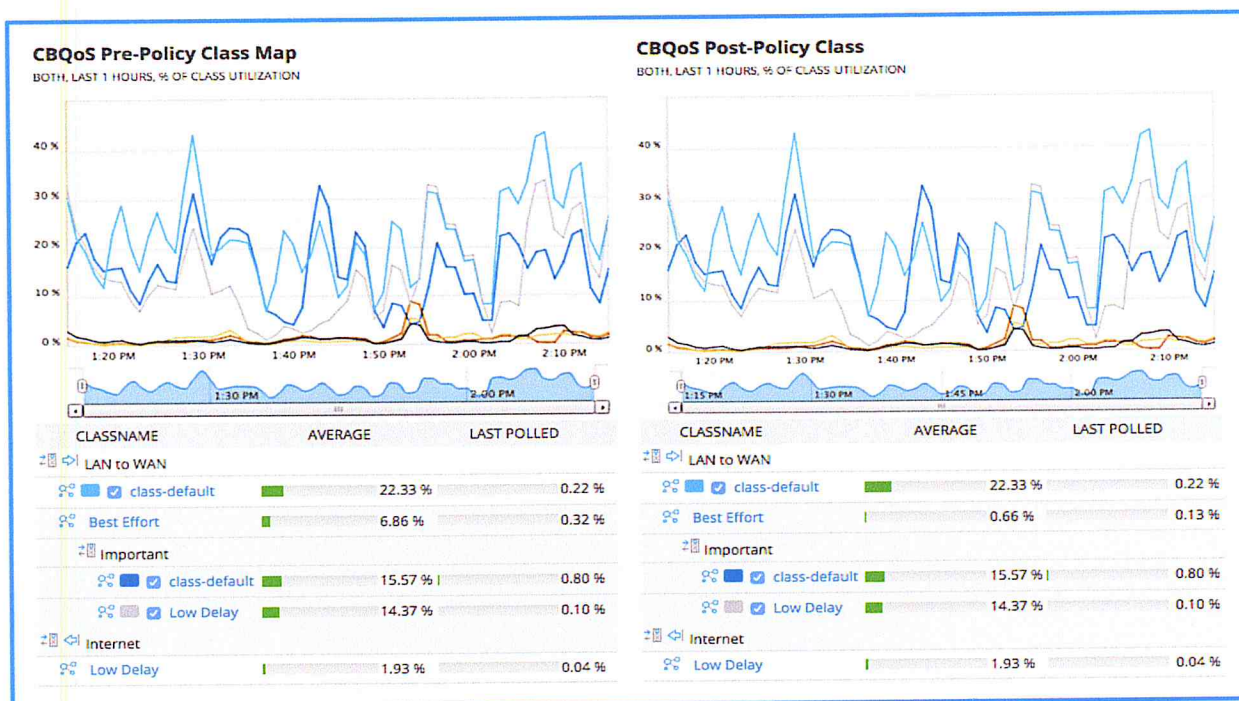


Figure 52 :Test de la qualité de service

6. Sécurisation protocolaire

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

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 [25].

6.1. Secure RTP (SRTP)

SRTP est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPSec, dont le mécanisme d'échanges de clés est trop lourd. Il aussi est bâti sur le protocole RTP. Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles de signalisation tel que SIP, ainsi que le protocole RTSP. Mais, surtout, il s'adjoit les services du protocole de gestion de clé MIKEY.

6.1.1. Service de sécurités offertes par SRTP

Les principaux services offerts par SRTP sont :

- Rendre confidentielles les données RTP, que ce soit l'en-tête et la charge utile ou seulement la charge utile.
- Authentifier et vérifier l'intégrité des paquets RTP. L'émetteur calcule une empreinte du message à envoyer, puis l'envoie avec le message même.

- La protection contre le rejeu des paquets. Chaque récepteur tient à jour une liste de tous les indices des paquets reçus et bien authentifiés.

6.1.2. 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 suivante présente le format d'un paquet SRTP

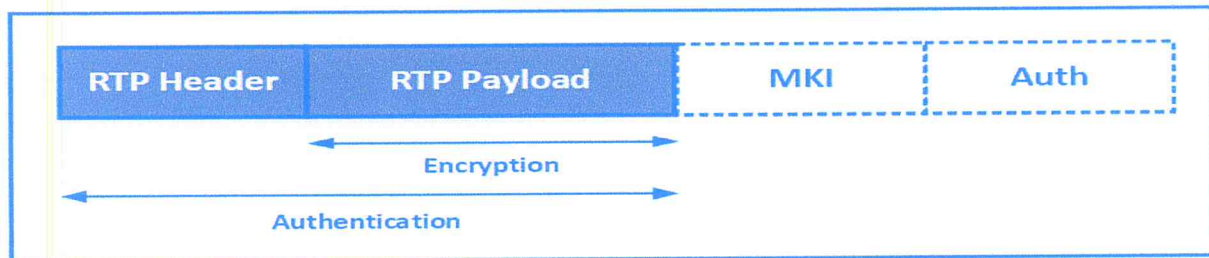


Figure 53 :Format d'un Paquet SRTP [25].

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

- SRTP MKI (SRTP Master Key identifier) : sert à ré-identifier 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.
- Authentication 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 rejeu de paquets en authentifiant le numéro de séquence.

6.2. Sécurité du protocole SIP

Le RFC de SIP prévoit un certain nombre de mécanismes de sécurité pour assurer la confidentialité, l'intégrité, l'anonymat et l'authentification au travers de la signalisation.

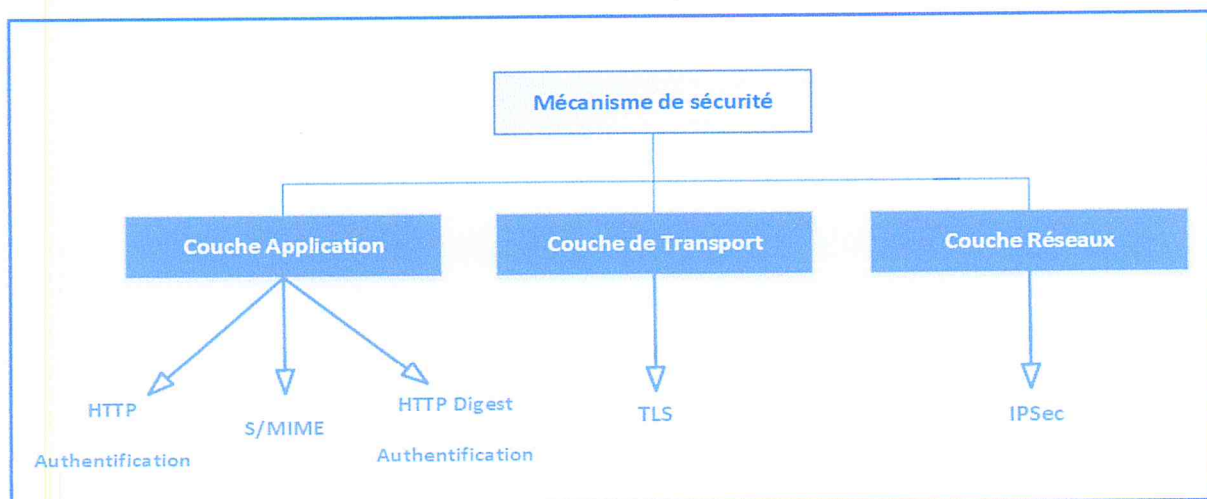


Figure 54 :Mécanismes des Sécurités SIP [27].

D'autres mécanismes de sécurité existent comme SRTP pour protéger la voix. La figure 53 présente leur position dans la pile protocolaire SIP. Bien que les solutions de sécurité existent, il n'y a pas d'obligation à les utiliser. Cette situation conduit généralement à dire que la sécurité n'est pas le point fort de SIP qui reporte cette problématique au niveau des couches sous-jacentes.

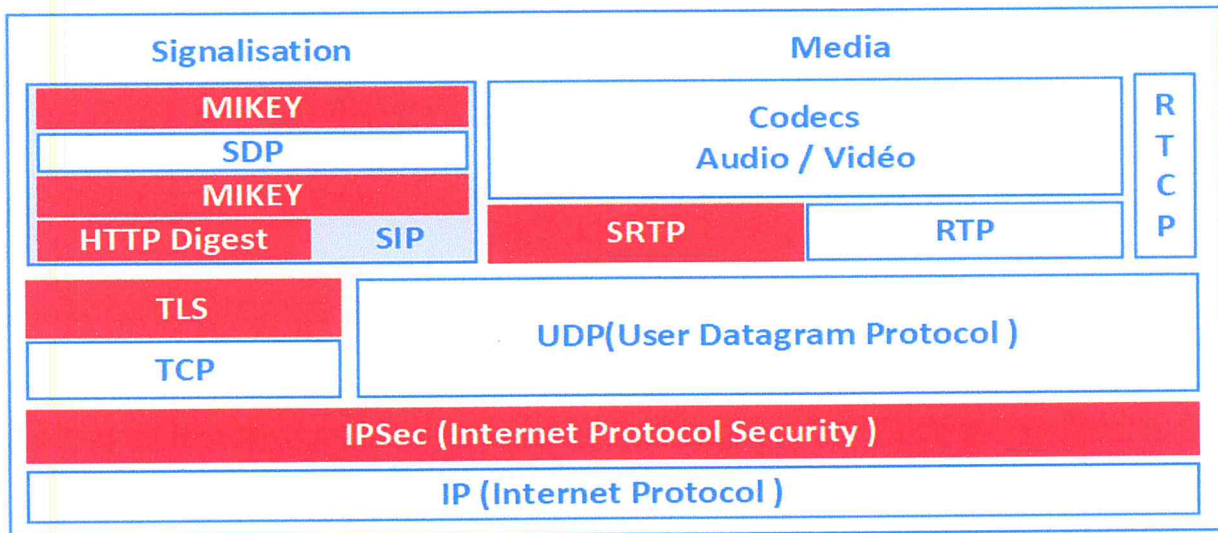


Figure 55 : Pile protocolaire SIP avec les éléments de sécurité [27].

La sécurité peut s'envisager de deux manières :

- Soit de proche-en-proche entre un usager et un serveur ou entre serveurs. Les propriétés de sécurité ne sont alors définies qu'entre deux entités seulement.
- Soit de bout-en-bout entre les deux usagers.

6.3.1. TLS et SIPS

SIP prévoit la sécurisation des échanges au niveau de la couche Transport avec Transport Layer Security (TLS). TLS, anciennement nommé Secure Sockets Layer (SSL), est un protocole de sécurisation des échanges sur Internet. TLS 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. Ainsi il ne s'occupe pas de fiabilité de couche Transport ni du maintien de la connexion. Les services offerts sont : l'authentification, l'intégrité et la confidentialité. Son implémentation native dans de nombreux navigateurs a fait de TLS le standard de sécurisation des applications Web, HTTPS correspondant à l'association d'HTTP avec TLS [28].

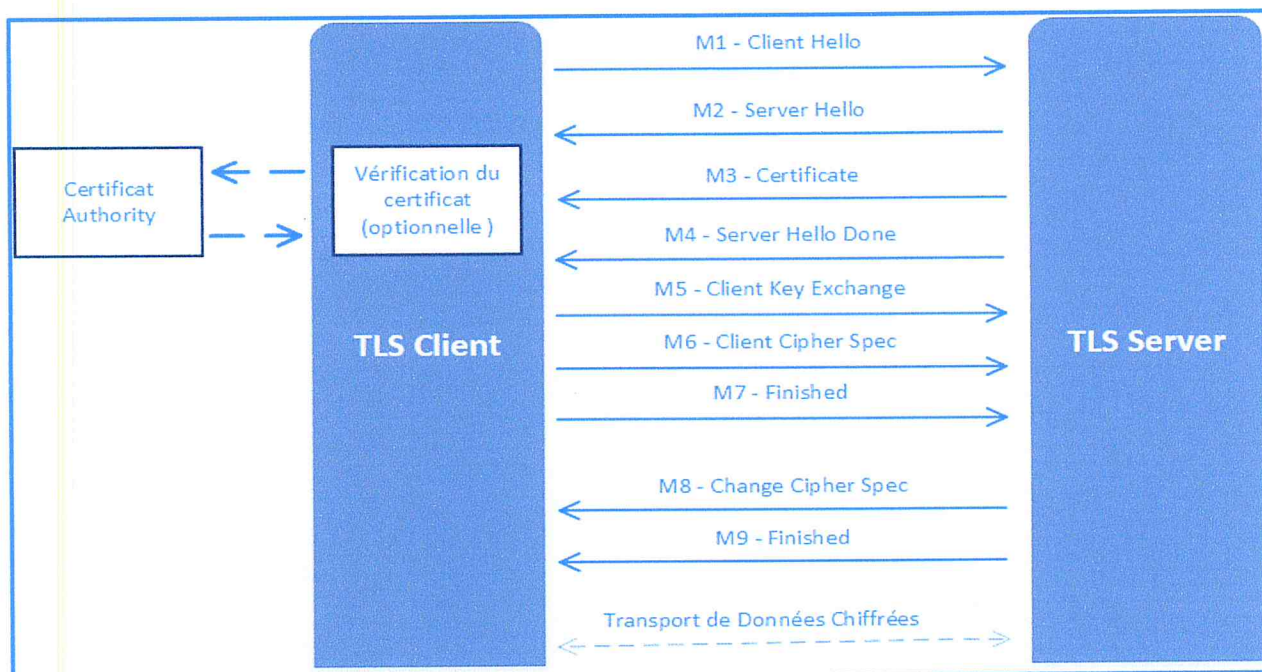


Figure 56 :Échange des Messages TLS.

TLS spécifie les fonctions suivantes :

- L'échange de messages d'ouverture de session, incluant la proposition des algorithmes et la méthode de négociation des clés de session.
- L'authentification du serveur voire du client.
- L'élaboration d'une clé « maître ».
- La dérivation des clés de session à partir de la clé « maître ».
- La transmission des paramètres des algorithmes de chiffrement et des aléas.
- La vérification des paramètres.

Pour réaliser la mise en œuvre de cette solution, un IPBX 3CX qui supporte TLS été installé sur un PC. Il a permis d'observer au travers des trames la solution TLS appliquée à SIP. La figure 57 présente la phase d'authentification, d'envoi de certificat et l'élaboration de la clé « maître ».

137.194.192.243	137.194.192.240	TCP	49638 > sip-tls [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2
137.194.192.240	137.194.192.243	TCP	sip-tls > 49638 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 WS=0
137.194.192.243	137.194.192.240	TCP	49638 > sip-tls [ACK] Seq=1 Ack=1 win=65700 [TCP CHECKSUM INCORRECT] Len=0
137.194.192.243	137.194.192.240	SSL	Client Hello
137.194.192.240	137.194.192.243	TLSv1	Server Hello, Certificate, Server Hello Done
137.194.192.243	137.194.192.240	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
137.194.192.240	137.194.192.243	TLSv1	Change Cipher Spec, Encrypted Handshake Message
137.194.192.243	137.194.192.240	TLSv1	Application Data, Application Data
137.194.192.240	137.194.192.243	TCP	sip-tls > 49638 [ACK] Seq=927 Ack=981 win=64555 Len=0
137.194.192.240	137.194.192.243	TLSv1	Application Data, Application Data
137.194.192.243	137.194.192.240	TCP	49638 > sip-tls [ACK] Seq=981 Ack=1529 win=65700 [TCP CHECKSUM INCORRECT] Len=0
137.194.192.243	137.194.192.240	TLSv1	Application Data, Application Data

Figure 57 :Exemple d'échanges TLS pour SIP.

6.3.2. IPSec

Pour protéger les échanges dans les réseaux, une des solutions usuelles consiste à utiliser le protocole IPSec (IP security), la version sécurisée d'IP. De même que SIP prévoit la sécurisation des échanges au niveau de la couche Transport, il envisage une protection au niveau Réseau avec IPSec. Ce protocole permet en effet d'authentifier l'origine de paquets IP, de garantir l'intégrité voire la confidentialité. IPSec permet donc de protéger des communications et la signalisation entre deux entités. Deux modes sont possibles : le mode transport ou le mode tunnel. Quel que soit le mode, le serveur SIP peut modifier les en-têtes SIP et permettre l'établissement de l'appel. D'une manière générale, les clients SIP n'implémentent pas cette solution. IPSec est donc principalement utilisé pour protéger le trafic entre deux domaines.

Deux protocoles sont définis pour l'encapsulation, AH (Authentication Header) et ESP (*Encapsulating Security Payload*). AH fournit le service d'authentification et l'antirejeu. ESP par rapport à AH fournit en plus la confidentialité.

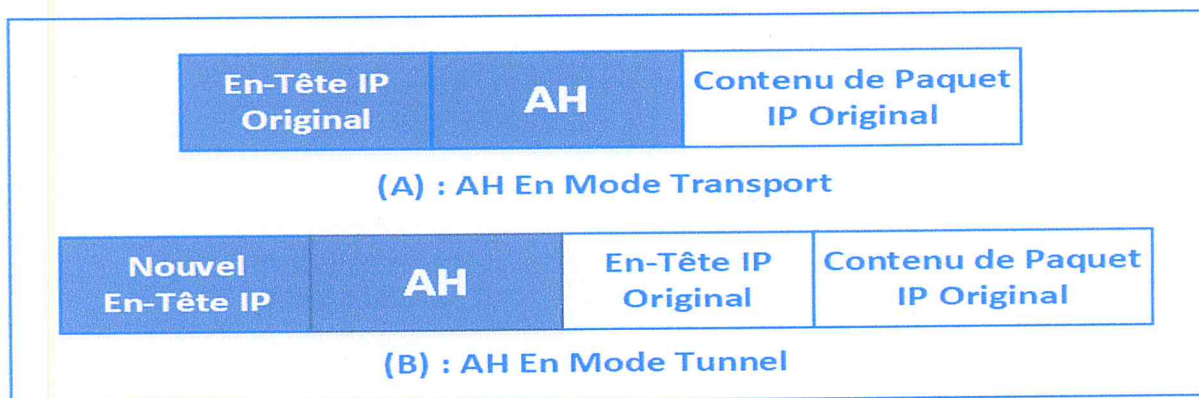


Figure 58 :IPSec en mode AH.

Les modes AH et ESP peuvent être utilisés en mode transport ou en mode tunnel. Le mode transport est utile pour sécuriser des communications de bout en bout (par exemple, de PC à PC). Le mode tunnel est principalement utilisé pour sécuriser les échanges transitant entre passerelles de sécurité. Ce dernier mode est utilisé pour la construction des VPN IPSec. Pour la gestion des clés, IPSec utilise IKE (*Internet Key Exchange*).

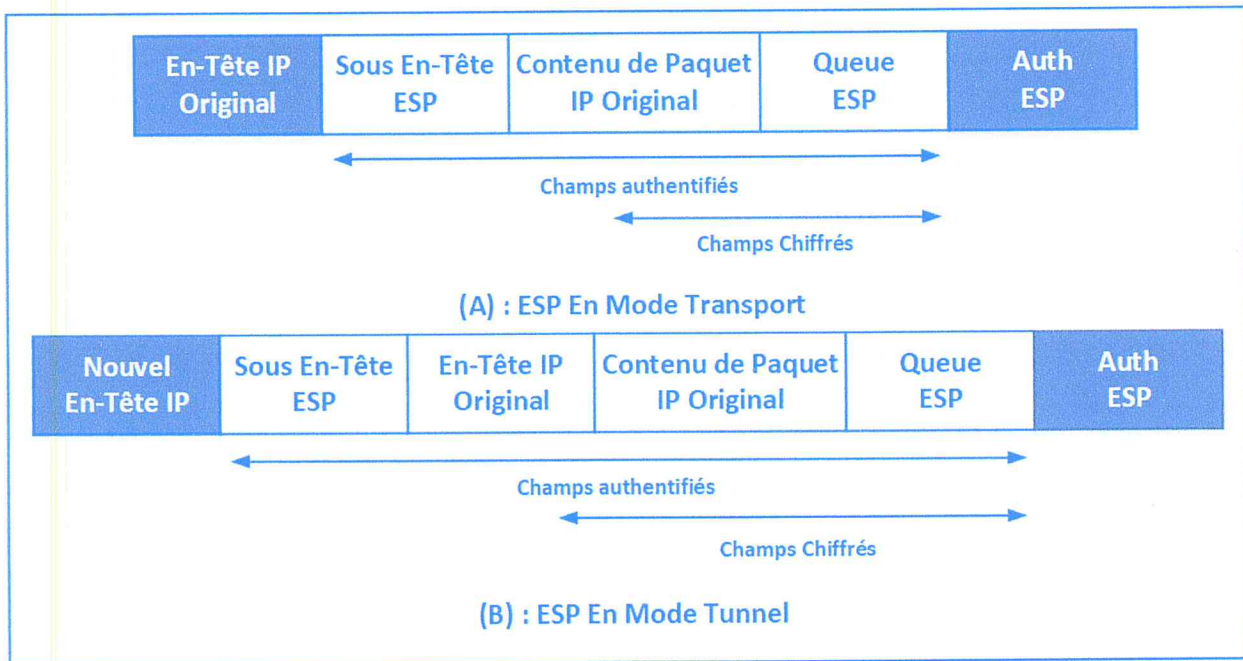


Figure 59 :IPSec en mode ESP.

7. Système de Contrôle d'accès AAA

Le contrôle d'accès est la manière dont nous contrôlons qui est autorisé à accéder au serveur réseau et quels services ils sont autorisés à utiliser une fois qu'ils ont accès. Les services de sécurité réseau d'authentification, d'autorisation et traçabilité (AAA) fournissent le cadre principal à travers lequel nous configurons le contrôle d'accès sur notre commutateur et service d'accès.

Lors de la phase d'authentification et pour communiquer avec le client ou sa machine, le serveur AAA fait appel à un ensemble des normes et de protocoles. Ce sont principalement : 802.1X, EAP et RADIUS.

❖ 802.1x

802.1X définit l'authentification basée sur le port 802.1X comme un protocole d'authentification et de contrôle d'accès client-serveur qui empêche les clients non autorisés de se connecter à un réseau local via des ports accessibles au public. Un serveur d'authentification valide chaque demandeur (client) connecté à un port d'authentification (commutateur d'accès au réseau) avant de rendre disponibles les services offerts par le commutateur ou le réseau local.

La prise en charge 802.1X requiert un serveur d'authentification configuré pour le service d'accès distant à l'authentification à distance (RADIUS). L'authentification 802.1X ne fonctionne que si le commutateur d'accès réseau peut router les paquets vers le serveur RADIUS d'authentification configuré. Pour vérifier que le commutateur peut router les paquets.

❖ EAP

Le protocole EAP (Extensible Authentication Protocol) est mieux considéré comme un cadre pour le transport de protocoles d'authentification, plutôt que comme un protocole d'authentification lui-même. EAP peut être utilisé pour authentifier les connexions d'accès à distance et VPN, ainsi que les ports LAN en conjonction avec IEEE 802.1X

❖ RADIUS

RADIUS est un protocole de réseau largement utilisé parfois appelé protocole client / serveur, qui fournit un mécanisme centralisé d'administration des informations de compte utilisateur. Ceux-ci peuvent être des noms d'utilisateur, des mots de passe et des niveaux de privilèges pour chaque compte.

Nous avons configuré le service d'authentification Radius sur la station « Contrôleur du domaine » vu qu'elle est d'OS (Windows Server 2012R2) et le serveur Radius est intégré implicitement dans toutes les versions Server du Windows. Les principales étapes de configuration du Radius sont illustrées dans les figures 60-61-62-63-64.

The screenshot shows the 'New RADIUS Client' dialog box. The 'Settings' tab is active. The 'Enable this RADIUS client' checkbox is checked. Below it is a dropdown menu for 'Select an existing template:'. The 'Name and Address' section has 'Friendly name' set to 'rezig' and 'Address (IP or DNS)' set to '192.168.100.7' with a 'Verify...' button. The 'Shared Secret' section has a dropdown for 'Select an existing Shared Secrets template:' set to 'None'. A text block explains that to manually type a shared secret, the 'Manual' radio button should be selected, and to automatically generate one, the 'Generate' radio button should be selected. The 'Manual' radio button is selected. Below it are two text boxes for 'Shared secret:' and 'Confirm shared secret:', both containing masked characters (dots). At the bottom are 'OK' and 'Cancel' buttons.

Figure 60 :Ajout d'un client Radius Standard.

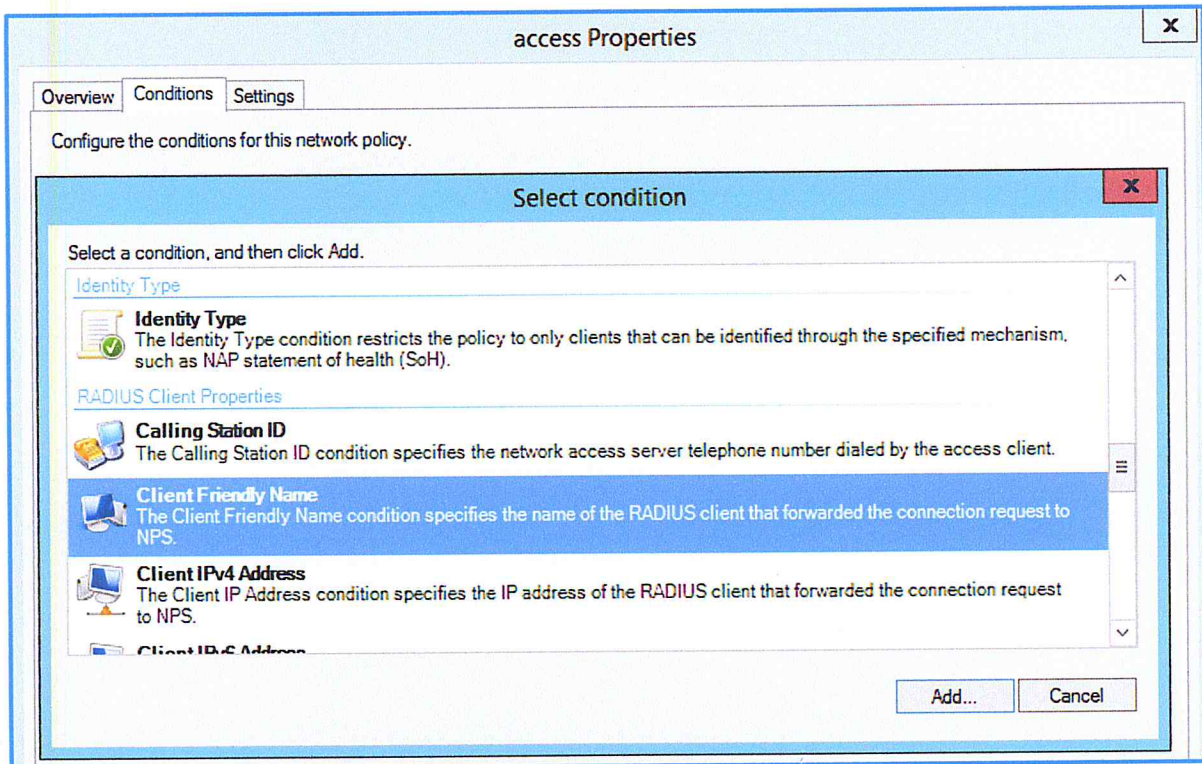


Figure 61 :Stratégie d'authentification selon le nom du Client Radius.

Pour qu'un équipement s'authentifie, il doit satisfaire les conditions de notre stratégie d'authentification (*client friendly Name*).

Pour notre cas, nous avons la stratégie suivante (Voir figure 61)

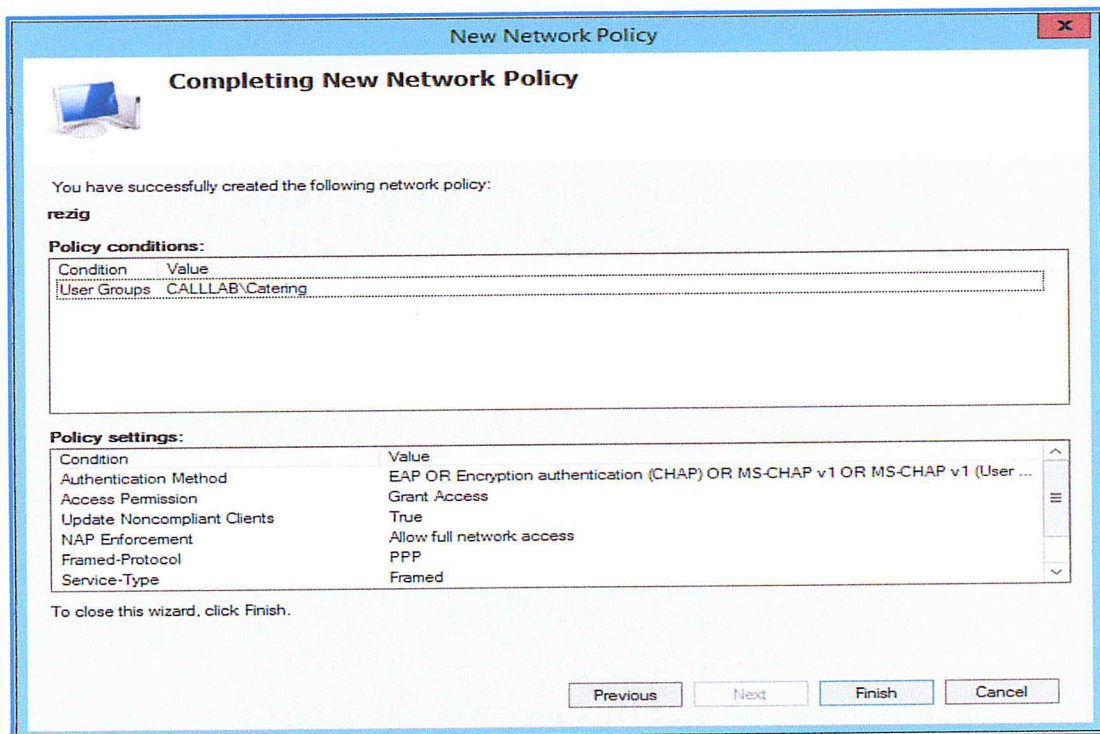


Figure 62 :Condition de notre stratégie d'authentification.

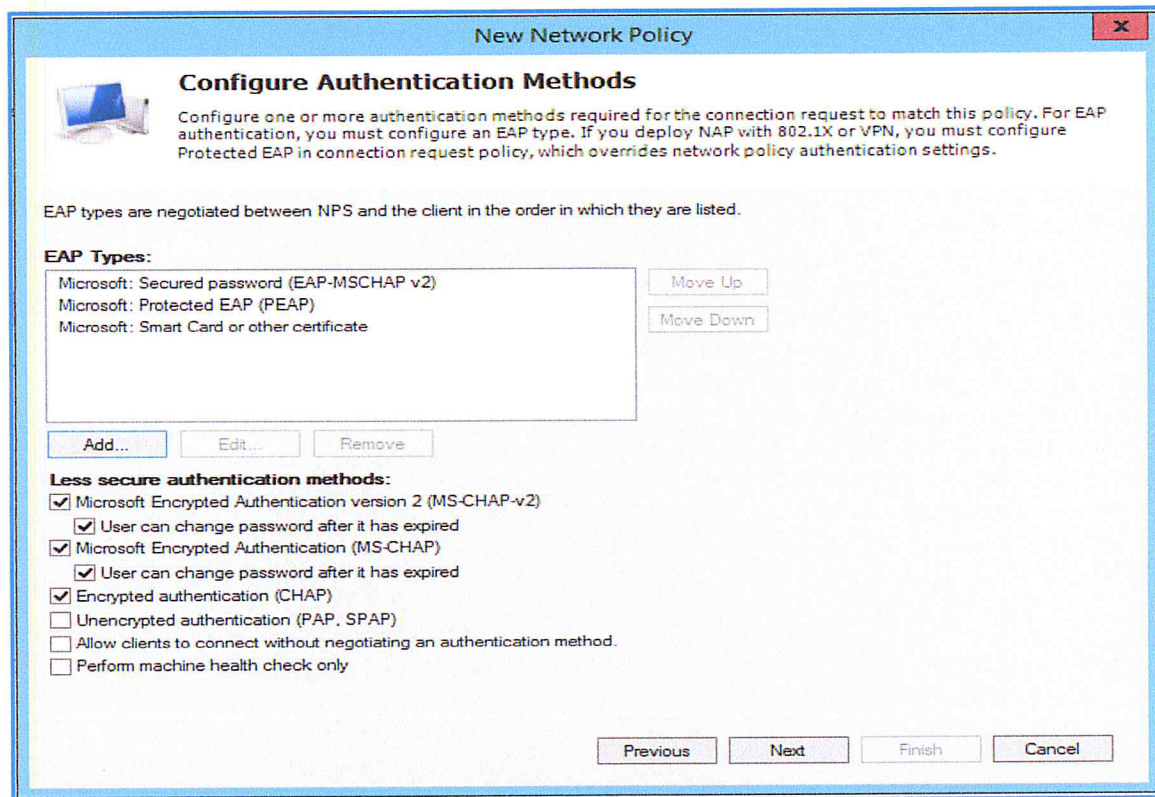


Figure 63 :Mécanisme d'authentification selon le standard 802.1x.

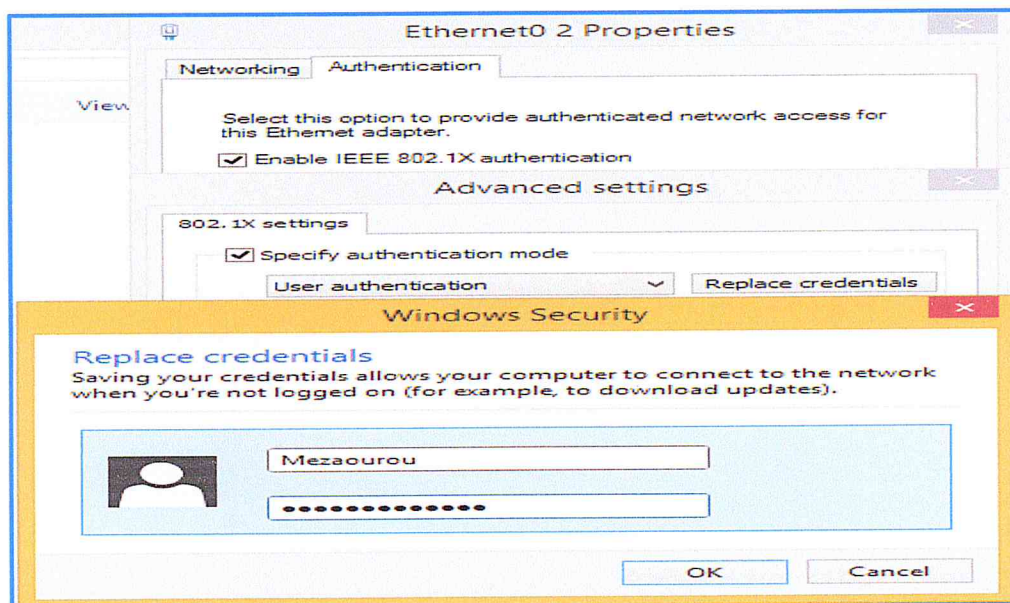


Figure 64 :Phase d'authentification de l'utilisateur.

Cette configuration est côté serveur, maintenant nous allons configurer nos commutateurs pour qu'ils utilisent ce serveur Radius pour l'authentification des utilisateurs et des équipements. Prenons l'exemple de la configuration du commutateur SW1-LAB, les commandes de la figure 65 permettent au SW1-LAB d'interagir avec le serveur Radius lors de demande d'authentification d'un équipement :


```

SW1-LAB(config)#
SW1-LAB(config)#aaa new-model
SW1-LAB(config)#radius server RADIUS-SERVER
SW1-LAB(config-radius-server)#100.101 auth-port 1645 acct-port 1646
SW1-LAB(config-radius-server)#key P@$$w0rd
SW1-LAB(config-radius-server)#aaa authentication login AUTH-VOIP group radius $

```

Figure 65 :Configuration AAA dans Le Commutateur .

7.1. Filtrage du Trafic sur les routeurs Avec des ACLs

Nous allons maintenant utiliser les possibilités de filtrage offertes par le routeur Cisco, nous n'allons utiliser qu'une petite partie de ces capacités, en se limitant au filtrage de niveau réseau. Cette fonctionnalité est appelée Access Control List.

- **Stratégie 1:** Nous allons interdire le trafic http entrant, pour bloquer l'accès aux configurations des téléphones IP à travers le Web. Nous allons définir une Access-List dans comme suit dans la figure 66

```

R1(config)#
R1(config)#ip access-list extended BLOCK-HTTP/HTTPS
R1(config-ext-nacl)# deny tcp any host 192.168.100.7 eq www 443
R1(config-ext-nacl)# deny tcp any host 192.168.100.8 eq www 443
R1(config-ext-nacl)# deny tcp any host 192.168.100.11 eq www 443
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)#
R1(config-ext-nacl)#exit
R1(config)#int serial2/0
R1(config-if)#ip access-group BLOCK-HTTP/HTTPS in

```

Figure 66 :ACL Interdisant le Trafic Http et Https entrant.

- **Stratégie 2:** Nous allons définir une ACL spécifique à nos besoins, nous autoriser le trafic SIP entrant à notre serveur de téléphonie CUCM qu'à partir des trois CIPCs

```

R1(config)#
R1(config)#ip access-list extended ALLOW-SIP
R1(config-ext-nacl)#192.168.100.11 0.0.0.0 eq 5060 host 192.168.100.100
R1(config-ext-nacl)#192.168.100.8 0.0.0.0 eq 5060 host 192.168.100.100
R1(config-ext-nacl)#192.168.100.7 0.0.0.0 eq 5060 host 192.168.100.100
R1(config-ext-nacl)#exit
R1(config)#int s2/0
R1(config-if)#ip access-group ALLOW-SIP in

```

Figure 67 :ACL Autorisant le Trafic SIP des CIPCs uniquement vers le CUCM.

En utilisant le Pare-feu et les Access-List, nous pouvons diminuer l'accès aux équipements critiques de notre infrastructure tel que le Call Manager et ainsi nous évitons des dizaines d'intrusion qui peuvent amener à des grands ravages.

Conclusion

A la fin de ce chapitre, nous avons pu mettre en place des politiques de sécurité qui diminueront l'impact des vulnérabilités et offrant un environnement plus protégé pour les clients SIP. Mais il faut savoir qu'il est impossible d'avoir une sécurité parfaite au niveau du réseau VoIP et généralement sur tous les réseaux.

Conclusion générale

Le système de téléphonie sur IP est confronté à des contraintes liées essentiellement à la sécurité qui nuisent le bon fonctionnement de ses services. En termes de sécurité, le système de téléphonie sur IP est ouvert à une variété d'attaques allant de déni de service jusqu'à le vol d'identité. Plusieurs solutions et outils de sécurité existent tels que les Firewalls, les IPS et d'autres mécanismes assurant la défense contre ces vulnérabilités. L'enjeu serait de savoir bien combiner ces mécanismes ensemble afin de dégager une politique de sécurité assez robuste et fiable.

De ce fait, Le but initial du mémoire était l'élaboration et la conception d'une solution VoIP sécurisée. Pour atteindre cet objectif, l'étude de la VoIP et ces architectures, surtout, le protocole de signalisation SIP a été primordial. La description du fonctionnement et des mécanismes de ces entités a été présentée dans les deux premières parties de ce document. Cela a permis d'avoir de bonnes bases et une bonne compréhension du domaine étudié.

Ensuite, dans la troisième partie présentée dans ce document, la compréhension des vulnérabilités et l'élaboration d'attaques ont pu être faites. Ces différentes attaques ont été expliquées en détail et présentées dans cette troisième partie. Suite à cette élaboration, la conception et la réalisation de certaines attaques ont été exécutées. La structure des implémentations, les configurations nécessaires, ainsi que l'utilisation du programme réalisé ont été expliquées de manière à pouvoir exécuter les attaques sur un réseau réel et pouvoir les tester avec de vrais téléphones VoIP.

Pour terminer on a déployé un environnement de simulation où nous avons pu apporter des améliorations de sécurité au niveau de l'architecture, application et protocole sur Les composants SIP, que ce soit des serveurs ou des terminaux, cela nous a permis d'utiliser un maximum de mécanismes de sécurité disponibles, que ce soit l'authentification, le chiffrement des messages ou bien l'utilisation d'autres outils. De plus, nous avons vu que RTP s'occupait du transfert du flux audio et pouvait, lui aussi, utiliser certains mécanismes de sécurité.

Finalement, la question n'est donc pas de savoir si la sécurité est nécessaire, mais comment se mettra en place une solution robuste et interopérable avec les infrastructures existantes. Chaque jour, la cybercriminalité nous rappelle que la sécurité n'est plus une option mais une obligation. La téléphonie reste encore préservée des attaques mais la convergence des réseaux vers le tout IP va nécessairement faire augmenter les problèmes de sécurité. Ce sujet de recherche reste donc un thème d'actualité. Nos futurs travaux compléteront la définition de l'architecture de téléphonie sur IP sécurisée en définissant les échanges de sécurité sur le canal média et en précisant le rôle de l'infrastructure support de sécurité.

Références Bibliographiques

- [1] O. Dembélé. Avantages et inconvénients des réseaux RNIS ET ADSL. Mémoire d'Ingénieur des Techniques Informatiques, Université de Lyon, 2008
- [2] Centile Telecom. Regards d'experts sur l'arrêt du RTC, CDRT, 2017
- [3] Jean-Louis Mélin. Qualité de service sur IP, Edition Eyrolle, 2000
- [4] Cisco systems. Cisco IOS Voice Video and Fax Configuration, 2001
- [5] Etude réalisée par le cabinet Ovum. L'évolution du coeur de réseau des opérateurs fixes, 2006
- [6] K. Wallace. Authorized Self-Study Guide Cisco Voice over IP (CVOICE), Third Edition, 2009
- [7] <http://www.frameip.com>. Consulter le 25/02/2018
- [8] <https://www.ictshore.com/free-ccna-course/three-tier-architecture>. Consulter le 25/02/2018
- [9] Connecting Networks Companion Guide: Hierarchical Network Design Cisco Networking Academy 2014
- [10] W. Chou. VoIP network security Strategies to Keep Your VoIP Network Secure, 2007
- [11] H. Dwivedi. Hacking VoIP protocols attacks and countermeasures, No Starch Press, 2009
- [12] O. Dabbebi. Gestion des risques dans les infrastructures VoIP. PhD thèse, Université de Lorraine, 2013.
- [13] M. Nassar. VoIP Networks Monitoring and Intrusion Detection. PhD thèse, Université de Lorraine, 2009.
- [14] T. Guillet. Sécurité de la téléphonie sur IP. PhD thèse, TELECOM Paris Tech, 2010.
- [15] <https://www.supinfo.com/articles/single/3031-tutoriel-gns3>. Consulter le 17-04-2018
- [16] <https://www.techopedia.com/definition/25690/vmware-workstation>. Consulter le 17-04-2018
- [17] <https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-communicator/index.html>. Consulter le 17-04-2018
- [18] J. Wiley. Wireshark for Security Professionals, Using Wireshark and the Metasploit Framework, 2015
- [19] <http://www.yourdictionary.com/nmap>. Consulter le 17-04-2018
- [20] A. Behl, B. Gardiner, J. Finke .Implementing Cisco Unified Communications Manager, 2017

- [21] <https://www.supinfo.com/articles/single/1950-mise-place-technologie-dhcp-snooping>. Consulter le 03/05/2018
- [22] <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>. Consulter le 03/05/2018
- [23] F. Medat. White Paper La sécurité des communications unifiées et la collaboration, Cisco Systems, 2009
- [24] T. Moegli. Cisco ASA HES Télécommunications-Réseaux et Sécurité IT, 2015
- [25] R. Bouzaida. Etude et Mise en Place d'une Solution VoIP Sécurisée. Master Professionnel, Université de Brest, 2011
- [26] N. Anderson. QoS on the Cisco ASA Configuration, 2014
- [27] A. Handoura. Création et sécurisation des Services Télécoms Fixes et Mobiles Sur IP. PhD thèse, Université de Bretagne Sud, 2009
- [28] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and S. Gritzalis, SIP Security Mechanisms: A State-of-the-art Review , In the Proceedings of the Fifth International Network Conference (INC 2005), Samos, Grèce, juillet 2005
- [29] <http://www.blog.saeed.com/2011/03/architecture-et-mode-access-de-la-telephonie-sur-ip/> Consulter le 07/03/2018
- [30] https://commons.wikimedia.org/wiki/File:H323_diagram.jpg Consulter le 07/03/2018
- [31] http://wapiti.enic.fr/Commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2005tt_nfa2006/butin-sutter/description_protocoles/description_protocoles.htm Consulter le 07/03/2018

